Teacher, enforcer, soothsayer, scapegoat: the purpose of the CISO in commercial organisations

Submitted by

Joseph Da Silva

for the degree of Doctor of Philosophy

of the

Royal Holloway, University of London

2022

Declaration

I, Joseph Da Silva, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed . . . . (Joseph Da Silva)
Date:

To my parents.

Abstract

The employment of a Chief Information Security Officer (CISO) is common in commercial businesses. However, the purpose of the CISO role is not well understood. This thesis provides in-depth perspectives on the CISO role, and, in so doing, brings to the fore a nuanced understanding of its purpose and surfaces the experiences of those performing it.

The thesis is grounded in an in-depth study of 18 UK-based but predominantly multinational organisations. It utilises semi-structured interviews with 15 CISOs and six senior organisational leaders, as well as an analysis of each organisation's annual report.

Through the application of empirically-grounded sociological theories to an interpretation of the findings, the thesis makes theoretical, practical, methodological, and empirical contributions. These include employing broader security scholarship related to ontological security and sociological notions of identity work to determine that cyber security plays an important role in business identity, being both threat to, and constituent of, that identity. It shows that the CISO's own identity is conflicted and contradictory and proposes a metaphor of soothsaying that provides further insight. By applying analytical lenses of risk management and governance, it shows that the CISO represents an attempt to control cyber-security uncertainty, and highlights paradoxes relating to the role that the CISO plays in risk management. Further, it introduces the concept of recreancy to cyber-security practice.

Cyber security is also explored in wider societal contexts, with the work of Thomas Hobbes used as an analytical lens. This indicates that cyber-security practices within businesses are beneficial to the state and shows that cyber-security threats are survival-level concerns feared by both states and businesses. Reflexivity in relation to the complex and enmeshed nature of cyber-security practice within broader society is also motivated by the thesis.

The thesis concludes with considerations for future work that have been provoked by this research.

Acknowledgement

I would like to thank Rikke Bjerg Jensen for her invaluable supervision and guidance throughout the development of this thesis. I would also like to thank all of the anonymous participants, without whom this research would not have been possible.

Publications

During the development of this thesis, a number of discrete papers based on the research were published. These are listed below.

- J. Da Silva. Producing 'good enough' automated transcripts securely: Extending Bokhove and Downey (2018) to address security concerns. *Methodological Innovations*, 14(1):2059799120987766, Jan. 2021.
- J. Da Silva and R. B. Jensen. 'Cyber security is a dark art': The CISO as soothsayer. *ACM Conference On Computer-Supported Cooperative Work And Social Computing (CSCW)*, Feb. 2022.
- J. Da Silva. Cyber security and the Leviathan. *Computers & Security*, 116:102674, May 2022.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

An effective cyber-security[1] function is of critical importance to commercial organisations, particularly due to the continuing and very public threat of data breaches and system compromises and the impacts they can have on stock market performance [269, 662].[2] As threats evolve in terms of sophistication from both external and internal sources, having an in-house capability that holds the responsibility for effective management of the organisation's cyber-security posture is a common means of risk mitigation. In order to lead such a capability, many organisations employ a Chief Information Security Officer (CISO). The focus of this thesis is, simply put, to understand the purpose of that role in commercial businesses.[3]

More specifically, the primary research objective was to understand the purpose of a CISO in a commercial organisation, as perceived by the leaders of that function and the leaders of the overall organisation, including how that may differ. This research objective is supported by the following four research questions:

- What factors influence a business's decision to employ a CISO?
- What are the possible roles that a CISO could perform within a business?
- What do senior stakeholders consider the purpose of a CISO within their business to be?

[1] Throughout, I refer to the field as cyber security, considering this to be more comprehensive than information security [759]. I am using security researchers Rossouw von Solms and Johan van Niekerk's definition of the term [759] and following computer scientist Robert Ramirez and political scientist Nazli Choucri in the avoidance of the single word cybersecurity [617, p. 2240].

[2] Although these impacts may be dependent on the type of breach [198].

[3] Throughout the thesis, I use 'business' and 'organisation' interchangeably for ease of reading. For the avoidance of doubt, all of the organisations referred to are commercial businesses. That is, they are profit-making entities rather than, for example, a co-operative which could be considered a non-commercial business.

- What do CISOs themselves consider their purpose within the business to be?

From an in-depth study of 18 UK-based but predominantly multinational businesses, and through the application of multiple theoretical lenses, I provide a number of novel perspectives on the role of the CISO that result in both a more nuanced understanding of the role and a greater appreciation of the experiences of those performing it. Throughout, I adopt a multi-disciplinary approach, as this reflects the inherent nature of cyber security [381, p. 107]. Cyber-security practice is increasingly recognised as more than a technological exercise and the application of sociological and political viewpoints to such practice, particularly in organisations, is becoming more and more common, e.g. [182, 716]. The thesis adopts an interpretive approach and is grounded in the socio-organisational paradigm. That is, it considers organisations as being dynamically constituted by social interactions rather than neutral environments that can be studied objectively. It supplements previous research on cyber-security practice within organisations, although perspectives from other disciplines are brought into conversation, with bi-directional benefits, throughout. Cyber security represents a source of uncertainty for businesses, and uncertainty is a consistent thread that runs through this thesis. Cyber-security uncertainty relates to, and is generated by, multiple human, sociological and political factors, and, therefore, warrants exploration beyond its surface representation.

CISOs perform an important, challenging, and yet poorly understood and ill-defined role [97, 421]. By focusing on perceived purpose, both from the perspective of CISOs and from the perspective of their most senior stakeholders, across a relatively large and varied sample, I gain a greater understanding of CISO practice that offers value to practitioners[4] and their employers – and to multi-disciplinary scholarship.

A brief note on writing style. Much of the thesis is written in the first person. I adopted this approach following my reading of philosopher Don Ihde [436, p. 3], which led me on to a pivotal work by philosophers of science Simon Schaffer and Steven Shapin [671], as well as supervisory feedback relating to the potentially 'alienating' effects of a third-person writing style. Shapin and Schaffer suggest that conventions such as this within 'traditional' scientific discourse are intended to "display . . . a certain sort of morality . . . [and] modesty" [671, p. 65] in an attempt to demonstrate objectivity, to describe "the matter of fact" [671, p. 66]. I consider that the use of such conventions would seem at odds with the social constructionist approach I have followed, as explained in Chapter 3. Furthermore, psychologists Virginia Braun

[4] As I explain in more detail in Chapter 3, I am a practicing CISO.

and Victoria Clarke[5] suggest that the use of the first person also "acknowledge[s] the creative and active role of the analyst" [164, p. 98n4] which is a key consideration in qualitative research, e.g. [254, p. 649].

1.1 Contributions

While many other works have explored, and problematised, cyber security in organisational contexts, including the role of the CISO,[6] my work provides a number of different perspectives. This is achieved through the use of multiple analytical lenses that provide deep understandings of empirical data, data which is broader and more extensive than many previous studies, e.g. [97, 623]. The primary contributions that this thesis makes are as follows:

1. A theoretical contribution through the application of sociological concepts of identity work, exploring the role that cyber security plays in identity, for both practitioners and their organisations. This includes the identification of a number of contradictions and conflicts.

2. A theoretical contribution through an examination of cyber security from the perspective of normative concepts of risk management and governance, including both sociological and political viewpoints.

3. A theoretical contribution through the application of a lens of political philosophy, contextualising cyber security in wider society, including the consideration of cyber security within business as a component of wider societal power structures.

4. A practical contribution through the enablement of greater reflexivity and reflection for practitioners and business leaders with regard to cyber security, as well as the identification of pathways for future research.

5. An empirical contribution through the engagement of a more extensive sample of CISO participants than many previous studies, as well as a sample of senior business stakeholders that provides a broader perspective.

6. A methodological contribution through being a practitioner-led study, unlike much previous research which has been performed by non-practising academics, e.g. [97, 687, 777]. Further, this thesis responds to calls for computer security research to be grounded in an interpretive socio-organisational paradigm [285]

[5] Referencing fellow psychologists Jeremy Foster and Ian Parker [335].

[6] As I discuss in more detail in Chapter 2.

> and for sociological perspectives to be applied to cyber security within organisations [272].

The sociological aspects of cyber security have been explored by many scholars e.g. [224, 278, 673, 716], with direct calls being made for sociologists to research cyber security within organisations [272]. The role of the CISO has also been explored e.g. [97, 490, 615], including the importance of the social aspects of this role [421]. However, no other work to date has applied the analytical lenses that I utilise in this thesis, nor studied as broad a range of empirical data. As a result, previously unexplored perspectives on the purpose of the CISO have been developed which deepens the understanding of this increasingly important role.

1.2 Structure of the thesis

The thesis is organised into seven main chapters. Following this introductory chapter, I begin in Chapter 2 with a discussion of key literature that has influenced the thesis, and which is returned to throughout. In Chapter 3, I explain the methodology followed, and this chapter also describes my own positionality as a researcher. I then present the findings from the research through three theory-based chapters. In each of these chapters, literature from Chapter 2, as well as additional literature where relevant, is brought into conversation with the data. Chapter 4 employs a lens of identity work and ontological security, and explores how cyber security is enmeshed with business identity, including moral aspects that feature in both business and CISO identity construction. These sociological lenses were chosen due to multiple aspects of identity that were apparent in the data and provide a theoretical basis with which to draw deeper meaning from the findings. Next, Chapter 5 explores the findings through a lens of risk management and governance, considering how normative concepts of risk and duty are reflected in organisational approaches to cyber security and identifying a number of paradoxes in relation to this. Again, these lenses were considered appropriate due to multiple references to these concepts in the data. Chapter 6 then builds on aspects of control identified in relation to risk management, utilising the work of political philosopher Thomas Hobbes to examine the role that cyber-security practices within businesses play in wider society, discerning benefits that accrue to states as well as to those businesses. Hobbes was chosen as a lens because of numerous references in the data to power and control which resonated with his work. In each of these findings chapters, I present opportunities for greater reflexivity on these topics for practitioners, businesses and academics. I conclude the thesis in Chapter 7, summarising my contributions and providing directions for future research. Appendices are provided that include methodological findings as well as supplementary information on data gathering and analytical method. Throughout, sections and subsections are numbered, with subsubsection headings appearing in bold type and paragraphs titled in italics.

Chapter 2

Literature review

This chapter provides a review of the literature that is relevant to the thesis. This literature is brought into conversation with the findings in later chapters.

2.1 Introduction

In this chapter, I present an overview of key literature underpinning this thesis. This literature is drawn from multiple disciplines, which reflects the different directions that the research led me in and, indeed, the inherently multi-disciplinary nature of cyber security itself [194, 387]. As a result, this chapter includes perspectives from across sociology, management studies, risk, and international relations (IR),[1] as well as from research in cyber-security practice, the most applicable 'home' literature for this study.

In subsequent chapters, the data from this study is interpreted through distinct analytical lenses. In order to present this analysis, it is necessary to lay a foundation of core concepts that are then brought into discussion in Chapters 4, 5 and 6. Specifically, Chapter 4 explores cyber security through a lens of ontological security and identity work, Chapter 5 develops the analysis further through themes of risk and uncertainty, and Chapter 6 applies a broader political and societal lens to cyber-security practice utilising the work of political scientist Thomas Hobbes. Therefore, in this literature review, I present an overarching discussion of prior research that provides context and background to these later theoretical discussions. The key thread that runs throughout the thesis is that of cyber-security practice and the context in which it operates, as a means of understanding the purpose of the CISO role, which is charged with overseeing that practice.

[1] The application of the breadth of disciplines covered in this thesis is itself an important contribution, as is the corresponding conversation between cyber security and those disciplines.

The literature is presented as a whole, for the purposes of readability. However, the relationship between the literature and the empirical data from this study is more organic than linear. The literature that supports the discussion in later chapters was identified inductively from the data itself throughout the analysis.[2] This resulted in the development of themes that indicated a number of theoretical directions, leading to deeper engagement with, and further exploration of, literature, which then provoked further analytical insights. For example, the data indicated that organisational identity was a concern related to cyber security, which resulted in a rigorous engagement with literature relation to identity. Therefore, although I set out the literature and conceptual grounding of the work here, before bringing it into conversation with the themes that were developed through the data analysis in later chapters, this grounding was developed in light of the thematic findings from the analysis and not *a priori*.

This chapter is structured as follows. In Section 2.2, I focus on the literature relating to cyber-security practice within organisations which provides a foundation for a deeper exploration of specific concepts in the following sections. This begins, in Section 2.3, with a broad discussion of concepts of security, including cyber security, as well as identity. As will be explained, cyber-security practices in businesses are directly relevant to the identities of those organisations, and hence, concepts of identity are pertinent. Next, as cyber security in organisations is typically framed from the perspective of risk, in Section 2.4 I explore concepts of risk and bring these into conversation with cyber security. Finally, I summarise the overall thread of this chapter in Section 2.5 and explain how this literature will be employed in subsequent chapters.

2.2 Cyber-security practice in organisations

I begin by discussing research that explores cyber-security practice in organisations. Many studies have had limited sample sizes e.g. [97, 652], suggesting a level of difficulty in studying cyber security in businesses, although some recent studies have succeeded in gathering larger samples e.g. [663]. Previous research has highlighted the importance of support from top management, e.g. [206, 776] but also a lack of alignment between cyber-security functions and the businesses they support, e.g. [65], including practitioners being distrusted by their business stakeholders [96]. A study performed by security researchers Debi Ashenden and Angela Sasse suggested that cyber-security functions are created by "senior managers" to fulfil "legal and regulatory requirements" [97, p. 403], although they do not define who these senior managers are. Cyber-security practitioners themselves have been studied by a number of researchers, e.g. [687, 777].

[2] The analysis process is discussed in more detail in Chapter 3.

This has included identifying disconnects with other employees, e.g. [400, 623], including in relation to how threats are perceived and how they should be dealt with [609]. Misunderstandings between cyber-security practitioners and their stakeholders may occur [777], including a lack of understanding as to what those practitioners actually do [795]. Others have studied the psychological characteristics of cyber-security professionals, including the need for various social capabilities [272]. A practitioner's role may be, at least in part, an interpretive one, as published global cyber-security standards are too generic and unreliable to be used in a prescriptive manner, and should be treated as guidelines [690].

A more limited research corpus exists on the study of CISOs and, to my knowledge, no research on this topic has been performed by a practising CISO. Previous studies have explored the effectiveness of CISO communication [97] and the role that CISOs play in responding to cyber-security incidents [464]. Others have noted a lack of clarity regarding the role of CISOs and what they are expected to do [421], with the CISO being subject to multiple "paradoxical tensions" [663, p. 2]. A number of studies highlight that CISOs appear to be somewhat disconnected from the rest of their organisations, being seen as blockers [97], governors [464, 623], translators [421], or even adversaries [96]. CISOs may be recruited in response to a cyber-security exposure [464], and thus occupy an identity that 'fixes' rather than 'prevents', yet may implement controls that are negatively perceived [623] or ignored [474], as discussed above. Ashenden and Sasse [97] adopted a psychological approach and identified some identity concerns among the CISO participants in their study on organisational culture. They identified CISOs as occupying multiple, possibly conflicting identities with regard to other employees, both an "authoritative role" and a "shar[ed] responsibility" role [97, p. 401]. They compare the difference in attitudes towards employees as that of towards either a "mature adult or irresponsible child" [97, p. 402], using similar language to that of psychotherapist Eric Berne [134].

A number of studies have investigated cyber-security behaviours within organisations, e.g. [121, 236], and the effectiveness of programmes aimed at improving such behaviours, e.g. [624], with some concluding that top-down, policy-based approaches to improving cyber-security behaviour, such as those called for by other researchers, e.g. [424], were ineffective [474] and others finding more effective results from game-based interventions [442]. Security researchers Andreas Poller et al. [607] highlight the centrality of both communication and management perspectives by calling for security initiatives implemented in organisations to be "reconciling people's ideas of security with the requirements of the organizational setting" [607, p. 2502].

Cyber security may be perceived as an individualistic practice and thus not 'cooperative' as noted by information systems researchers John Goodall et al. [367]. Their study showed that cyber security is inherently collaborative both within and across organisational settings – while also being grounded in a community of experts. Effective cyber security depends on multiple actors, not just those who are cyber-security practitioners [623]. Security researchers Laura Kocksch et al. [479] used the notion of care as an analytical lens to bring to light the often invisible aspects and practices that underpin IT security. Here, "caring for IT security" establishes "a moral stance that refrains from blaming insecurities upon single actors" [479, p. 17]. Other research has shown that cyber-security practice within organisations is a social activity, e.g. [777], both in terms of internal relationships and also external ones [727]. According to some, the effectiveness of a cyber-security programme can be improved by encouraging "prosocial" behaviour [733].

An acknowledgement that an effective cyber-security programme relies on social as well as technical aspects appears common across geographies, e.g. [652, 706]. Further commonality across geographies is seen with regard to the importance of user awareness, e.g. [201, 206], although this is not as straightforward, as I discuss shortly. National culture has been shown to have an effect on security control design, including the level of inclusivity of users in that process [639], supporting the conception of cyber security being, like other forms of security, culturally situated.[3] The importance of applying social, and philosophical perspectives to cyber-security practice in organisations was identified some time ago [285], a call subsequently repeated by many researchers, e.g. [227].

Much of the literature on cyber-security practice refers to the use of various 'controls' as a means of dealing with threat. I now explore the use of such controls in more detail.

2.2.1 Cyber-security controls

Controls are often discussed in relation to cyber security e.g. [453, 789], and the concept appears normative. International "best practice" [789, p. 2] control sets exist, such as those defined by the ISO27002 standard [44], the latter defining 'control' as a "measure that is modifying risk" [17, p. 3].[4] Multiple factors, including social factors, can inhibit the establishment of effective security controls in organisations [776]. Security improvements may be seen as of little value within organisations [607], with security itself being seen as "scary, confusing, and dull" [385, p. 411], or focused on attributing

[3] National culture may be oriented around characteristics that are stereotypically masculine or feminine [639]. I discuss masculinity in the context of cyber security in Section 2.3.3 as well as in Chapter 6.

[4] This can include "any process, policy, device, practice, or other actions which modify risk" [44, p. 3].

blame for failings [479]. Organisational culture has also been identified as a factor in the effectiveness of cyber-security practice within organisations, e.g. [319], particularly in relation to employee behaviour [262]. This includes the role of social norms [402], and values, e.g. [263], although, in a wide analysis of literature relating to information security culture [566], policy was the only common dimension identified. Van Niekerk and von Solms propose that knowledge of cyber security is a pre-requisite to achieving a cyber-security culture [754], and cyber-security education itself is a common theme from the literature to which I now turn.

Education

Sociologist Bill McSweeney highlights the importance of education as a response to risk [545, p. 92], and education is commonly articulated as a key control in the management of cyber-security risk, e.g. [622, 689], despite potentially being ineffective [403], although efficacy may depend on the type of educative approach followed [691]. Some of these approaches seemingly adopt what sociologist Ulrich Beck suggests is a common, but ineffective, philosophy, in that they seek to address a population that is "'poorly informed' ... [and] irrational ... [due to] inadequate information" [123, p. 12], and expect that, by providing additional information, those individuals will take fewer risks. For example, "lack of knowledge" of employees in relation to cyber security has been proposed as a critical risk [754, p. 477] to organisations. Such a dearth of understanding can lead to "undesirable behaviors" [583, p. 83], indeed, "misbehaviour[s]", that threaten organisational prosperity [261, p. 196]. Beck argues that this is an over-simplistic approach that ignores cultural aspects and indeed the inherent subjectivity of risk [123].[5]

There appears to be a normative conception of employees as being inherently risky [66, 602], although this concept has also been challenged e.g. [66, 657]. Cyber-security education needs to be frequent [624] and take into account cultural factors, not being "one-size-fits-all" [100, p. 231]. Such education is seen as important both for organisations and for broader society [622]. It may help to counteract risky behaviour attributable to both "organizational and individual inertia" [682, p. 109], and affect the willingness of users to accept controls [288], particularly as policies alone are ineffective without education [384]. Along with other factors, it may reduce the likelihood and impact of cyber attacks [180] but yet may be ineffective, "rational[ly]" ignored, and even detrimental [403, p. 133]. Improved awareness does not necessarily result in improved conduct [95] and education alone is not sufficient; organisations need a combination of "information security technologies, qualified information security personnel, and se-

[5] And may, in fact, result in 'non-knowing', as I will discuss in Chapter 5.

curity awareness of organizational users" [201, p. 397] in order to effectively manage security threats. Employee actions in relation to cyber security may be influenced by their personalities [679], and even their gender [90], suggesting that the effectiveness of educative approaches may be inherently limited, and even if employees are suitably 'educated' by the organisation, they may still intentionally disobey policies [244].

Discipline and punishment

Organisations do not just make their employees aware of cyber-security threats and the conduct expected of them; they also subject them to discipline in relation to cyber security. Organisations implement regulations and limitations on employees [153] by defining and enforcing policies. Such policies are seen by some as a "vital tool ... to ensure the secure use of information assets and data in an organizational context" [212, p. 448], and have been described by others as a core facet of the most common approach to managing cyber-security risk [663]. If compliance with policy is not forthcoming, then employees may be punished [402]. Equally, the 'correct' behaviours may be rewarded [153], although some have found that neither sanctions nor rewards significantly influence compliance [590]. Security researchers Lijiao Cheng et al. identify "the severity of sanctions" as having a significant effect on employee compliance, in contrast to the "certainty of sanctions" [212, pp. 454-5]. As they point out, other research has been non-conclusive on the effectiveness of sanctions, e.g. [462, 590, 652], and this may also be related to cultural factors [212]. Others have identified the relevance of organisation size and industry sector to the effectiveness of deterrent-based approaches [462] and it may be the case that "[p]erceived sanctions ... have a stronger influence than perceived benefits for more serious behaviors" [266, p. 654].

While deterrence may be ineffective, "moral commitment" [706, p. 300] may be a factor in employee compliance. Others have also made a connection between employee morality and cyber-security behaviours, e.g. [691], including highlighting the consequences of employee actions [792]. Those actions may be deliberate or unwitting, a distinction characterised by some as "deviant behavior" versus "misbehavior" [249, p. 91]. Similarly, information systems scholars Barlow et al. suggest a value-judgement to non-compliance with policy, referring to "violations" [111, p. 145] as well as "guilt or shame" [111, p. 146].[6]

The "social relationship between employees and their organization" may also influence employee behaviour [384, p. 61], as may their hierarchical position [266, 702]. Additionally, social and cultural norms are relevant, such as those described by Cheng

[6] These aspects of morality associated with cyber security are discussed further in Section 2.3.5, and in Chapter 4. Policies themselves are "expressions of values" [400, p. 373].

et al. who identify “the expectations of immediate supervisor, co-worker, organization and family” as factors in employee behaviour [212, p. 455]. The invocation of these in educative messages has been encouraged [792] and the greater import provided to security messages that originate from “mass media, friends, and co-workers” [609, p. 563] rather than from the organisation itself has also been acknowledged.

Technological controls

Cyber security is often considered to be a technological field and, therefore, technological controls are often articulated as a response to cyber-security risk, albeit not necessarily in isolation from non-technological controls [402, 569]. Examples of technological controls include those intended to stop users from doing something, e.g. [718, 741], or to identify them doing something, e.g. [267, 715]. These can result in staff experiencing security as being a technological barrier [795], as an imposition, which may affect their performance and motivation [215]. Other technological controls may be more focused on systems rather than people e.g. [342, 367], although aspects of these controls may be ineffective [453].

Alternative approaches to focusing cyber-security programmes on control have been suggested. For example, informatics scholar Karin Hedström proposes a “value-based” model that considers “information security as contextual and see[s] users as resources instead of problems” [400, p. 383]. In such a model, “non-compliance” of employees is considered deliberate and “rational” [400, p. 381] and, therefore, addressing such behaviour is not a matter of providing education to fill a ‘gap’ in knowledge. Employees may actively and deliberately resist controls [492], creating “workarounds” [475, p. 29] [623], particularly where security controls are considered as impacts to productivity [474]. Workarounds may also be developed in response to poorly designed systems, including those that don’t reflect the reality of employee working patterns and demands [625], but may also be due to “value conflicts” [480, p. 9]. Employees may be deliberately non-compliant if they feel antagonised by the organisation, considering resistance as “a way to seek retribution for some form of perceived injustice” [609, p. 563], including grievances that have nothing to do with cyber security. Security researchers Lizzie Coles-Kemp et al., when researching user experiences of state benefits systems, found that users considered circumventing (“twisting”) user controls as “an act of empowerment” [227, p. 154],[7] although it is important to acknowledge that this research was conducted in a community where attitudes and perceptions towards the system (and its creators) were seen to be negative and antagonistic, particularly regarding the perceived ‘fairness’ of the system. Security researchers Iacovos Kirlappos et al. suggest

[7] Similarly, disobedience of the law may also be empowering [224].

that primacy must be given to the design of security controls from a productivity and usability perspective, and that "trust" [474, p. 11] of employees is crucial in achieving effective cyber security. Trust has also been highlighted as "the start point for an individual's security ... [rather than] protection" [224, p. 47]. Despite these calls for trust-based and user-focused security, many commercial organisations still adopt a policing approach, despite this being ineffective in improving security [762], with "a set of persuasive approaches based on morals and ethics" [691, p. 39] being seen as more appropriate by some. Governance, discipline and control are features that manifest within organisations in other ways besides cyber security, as I describe in the following section.

2.2.2 Governance

The UK's Corporate Governance Code defines corporate governance as "[t]he system by which companies are directed and controlled", adding that "[b]oards of directors are responsible for the governance of their companies" [243, p. 1]. Economists Eugene Fama and Michael Jensen describe boards of directors as a crucial method of internal governance for listed companies [322], with management scholars Saeed Akbar et al. stating that "the board of directors is considered to be the main internal governance mechanism in modern corporations" [78, p. 108]. Management scholars Ingrid Bonn and Andrew Pettigrew describe how organisations face an "increasingly heterogenous and hostile environment" [149, p. 5], leading to more formalisation in organisational structure, which echoes fellow management scholar Henry Mintzberg [549]. Bonn and Pettigrew state that boards are "a mechanism ... for reducing environmental uncertainty" [149, p. 6] and also describe how directors play a role in "enhancing the corporate reputation, credibility and legitimacy of the organisation" [149, p. 5]. Similiarly, management researchers Pornsit Jiraporn et al. found that "firms with more effective governance exhibit a substantially lower degree of risk-taking", with their focus being on financial risk [446, p. 111]. Differing views on the role of the board exist, however, ranging from "monitor[ing] management, who otherwise may act in their personal best interest and not in the interests of the principal (e.g. shareholders)" to "foster[ing] legitimacy... [whereby governance] activities and structures are primarily ceremonial and serve as symbols of effective oversight" [120, p. 69], or where the board is "helper or partner, rather than monitor of management" [120, p. 70]. The board may even be intended "to promote shareholder value through their superior knowledge of the company" [120, p. 70]. However, there are possibilities for them to be "purely symbolic and consistently supportive of management, even when the members appear to be independent", with management "choos[ing] friends to serve as passive directors" [120, p. 70]. Therefore, despite the intentions of regulators [243], there is opportunity for organisations to act disingenuously, and governance appears to exist on a continuum from "weak" to "strong" [208, p. 358]. Management researchers Murali Chari et al. show that "strong governance motivates managers and aligns their interests with shareholders" [208, p. 370],[8] and effective corporate governance may result in improved stock market performance [216]. Economist John Roberts highlights the selfish aspects of human behaviour that may not lead people within organisations to act in a way that is desirable to the organisation, including determining "what risks to take" [636, p. 118]. He attributes this in part to the imbalance between how the benefits and costs of the activities performed are accrued to the organisation versus the individual themselves; in other words, the individual bears too much cost for too little benefit, such as working longer hours for no extra pay, or experiences more benefit than cost, such as taking short-cuts that limit the effort spent on a particular activity with no observable direct impact on them, the increased risks being accrued to the organisation.

Corporate governance needs change over an organisation's life cycle [149, 328]. Bonn and Pettigrew posit that the primary concern for a company in decline is dealing with "threat[s] to survival" with a need for them to "ensure effective control and monitoring mechanisms are in place" [149, p. 11], echoing viability concerns described above, whereas a "mature" company will engage in "regular dialogue with stakeholders ... [to signal] that the board is effective and vigilant" [149, p. 10]. They argue that boards in mature organisations are focused on the existence of "adequate controls" and legal compliance [149, pp. 10-11] and describe how, as the breadth of an organisation's stakeholders increases, organisations "exercise control-related activities", in part to "demonstrate organisational legitimacy" [149, p. 8]. I return to the topic of legitimacy in Section 2.3.4.

External governance

Within the UK, company directors have a duty under the Companies Act 2006 to "promote the success of the company" and "exercise reasonable care, skill and diligence" [4, §172, §174]. Additionally, they must be made aware of "principal risks and uncertainties facing the company" [4, §417]. The UK Corporate Governance Code [243, Provisions 24-25] defines a Principle stating that "the board should ... establish a framework of prudent and effective controls, which enable risk to be assessed and managed" and fur-

[8] And, according to the UK Corporate Governance Code, "[t]he shareholders' role in governance is to appoint the directors and the auditors and to satisfy themselves that an appropriate governance structure is in place" [243, p. 1].

ther requires the establishment of an Audit Committee whose responsibilities include "reviewing the company's ... internal control and risk management systems, unless expressly addressed by a separate board risk committee". As mentioned earlier, this code is not legislative, and while the UK Government has indicated that it does not intend to introduce specific legislation to enforce corporate governance principles, preferring to continue with voluntary, principles-based regulation [280], it did, however, legislate "to require all companies of a significant size to disclose their corporate governance arrangements in their Directors' Report and on their website, including whether they follow any formal code" [6, Part 8].

In some industries, external governance includes regulations that involve accountability of individual employees to the regulator, with criminal liability arising as a result of non-compliance. For example, UK Financial Services regulations[9] include a "Senior Managers Regime" [46] that involves individual accountability to the regulator, with criminal liability arising as a result of non-compliance. The Senior Managers Regime applies to individuals that perform a "controlled function", including "overseeing the firm's systems and controls" [40]. The regulations refer to a "[h]ead of key business area" as an applicable senior manager, with a "key business area" including "areas such as risk" [535]. Personnel fulfilling these roles require prior regulatory approval before appointment and are directly accountable to the regulator for any failure to fulfil their responsibilities, including the appropriate management of risk. Under the same regime, board members have similar accountability to the regulator [2].

While organisational scholars Paul du Gay and Signe Vikkelsø argue for the focus of organisational theory to be re-aligned to the internal aspects of organisation [301], in the context of cyber security the wider industry and societal context cannot be dismissed. For example, the UK Government's first National Cyber Security Strategy described a reliance on "initiatives ... [being delivered] with or through partnerships with industry" [411, p. 34] and, additionally, that there are a number of regulatory and legislative provisions that require "industry [to act] to protect itself from the threat" [411, p. 41]. The same document states that the Government "will not accept significant risk being posed to the public and the country as a whole as a result of businesses and organisations failing to take the steps needed to manage cyber threat" [411, p. 26]. This makes it clear that individual organisations are seen as occupying a role within the overall system of national cyber defence, something that was reiterated in the subsequent National Cyber Strategy [412]. Additionally, some UK industries[10] are subject to license conditions that obligate them to act in concert with other actors in that industry with

[9] Arising from such legislation as the Financial Services and Markets Act 2000 [13] and subsequent amendments.

[10] Such as energy [28, pp. 308-45].

regard to security.

Manifestations of governance

Although its origin is unclear [271], the 'three lines of defence' model is commonly encountered in risk management, e.g. [271, 511] and accounting disciplines, e.g. [114, 646]. This model states that the first line of defence is the consistent enactment of process by operational staff in accordance with defined policies and standards, the second line of defence is the definition and maintenance of those policies and standards by staff in governance roles and the third line is the verification of the effectiveness of the first two lines by a separate auditing function [516, 796]. Although this model appears to be in widespread use, its interpretation and implementation may vary [796]. This model has been applied to cyber security, e.g. [553, 651], with cyber-security functions being proposed by some as performing a second line of defence role [643]. Criminologists Les Johnston and Clifford Shearing describe "professionals/experts/specialists" as "agents ... of governance" [450, p. 24], further arguing that "the desire to promote local capacity and knowledge ... [is a] basis for effective governance" [450, p. 73]. On this basis, an organisation's cyber-security team can be considered as such agents of governance.[11]

Doctoral research performed by economics scholar Maria Zhivistkaya identified a disconnect in employees' conception of which of the three lines of defence they were performing, specifically that while those in the second and third lines of defence were consistent in their "self-identification", those in the first line were not [796, p. 163]. This may suggest either that communication is lacking or that those in the first line reject the responsibilities assigned to them. If those in the first line are not clear on the role that they play, they are likely to be ineffective in performing it. Zhivitskaya identifies potential weaknesses with the 'three lines of defence' model, including that it "diffuses responsibility" [796, p. 164]. Writing alongside economist Howard Davies, she poses further challenges to the model's effectiveness including its "potential ... to reduce accountability rather than enhance it" [271, p. 41].

Governance is strongly associated with discipline and control, in particular with boards of directors "monitoring and controlling top management" [149, p. 3]; indeed, this may be the primary task of the board [322]. Boards are considered to be a crucial method of internal governance for listed companies [322] and, as a form of governance, "constrain managers from pursuing risks that erode shareholder returns" [208]. I now discuss boards, and the role that they play in cyber-security governance.

[11] These points also relate to the grouping of specialist expertise within organisations and associated dissemination of knowledge, which will be discussed further in Section 2.3.

Board-level governance. Management researchers Andrew Pettigrew and Terry McNulty identified that non-executive directors (NEDs) regarded their most important responsibilities to be those related to control [600, p. 11]. Boards are "a mechanism ... for reducing environmental uncertainty" [149], with directors playing a role in "enhancing the corporate reputation, credibility and legitimacy of the organisation" [149, p. 5]. A reputational aspect to boards was also highlighted by management scholars Saeed Akbar et al. [78], who additionally identified that corporate boards that were more independent, i.e., were composed of a higher number of independent non-executive directors, took less corporate risk.[12]

Bonn and Pettigrew suggest that the relative importance of different roles performed by boards of directors changes over time and argue that as companies grow, monitoring and control becomes more important due to the risk of management taking action contrary to shareholder interests [149, p. 9].[13] A later cross-sectional study performed by management researchers Thomas O'Connor and Julie Byrne agreed that "the relevance of individual governance provisions" [582, p. 40] changes across life cycle stages. Therefore, if the CISO acts as one of these "governance provisions", its purpose may change over time.

Cultural aspects of governance. Economist Oliver Hart argues that "governance structures, incentives of managers, culture" are a more effective "starting point" for understanding the behaviour of an organisation than its "objective function" [390, p. 112], and organisational culture is often associated with governance, whereby a particular culture may either inhibit or support aspects of governance. An organisational culture where security is considered "a technology issue not a business one" [728] can contribute to security breaches, as UK telecommunications provider TalkTalk experienced in 2014 and 2015. Culture was explicitly referenced by this organisation's CEO as a factor in these breaches [242]. Subsequently, the organisation claimed to have developed a different culture whereby "security is discussed at every meeting ... is embedded in everything we do ... and has become part of the day to day discussion" [290].

The TalkTalk incident also provides an example about the importance of language and discourse in relation to culture [42]. Organisations may profess to have a strong culture in relation to a particular risk, and yet, such rhetoric does not prevent disasters

[12] What is not mentioned, however, is the potential link with career progression. Building on both management researcher Edward Bowman [159] and Chari et al. [208], it may be advantageous from a career perspective for a non-executive director to be associated with a firm that has not been impacted by (significant) materialised risk.

[13] They also identify that monitoring and control are of crucial importance to companies in decline, whose primary concern is dealing with "threat[s] to survival" [149, p. 11], something I return to in Section 2.4.

from occurring [87]. Despite safety being claimed as the "number one priority", a firm's ideology may in fact be economic efficiency and cost control [87, p. 62]. Culture is also associated with ethical behaviour, e.g. [327] a topic I turn to in more detail in Chapter 4.

Cyber-security governance

The need for cyber security to be governed appears normative, at least in the UK, with listed businesses being assessed on their "cyber governance health" [7].[14] The 2018 'FTSE350 Cyber Governance Health Check' published by the UK's Department for Digital, Culture, Media and Sport (DCMS) observed that "[companies whose boards had] a more comprehensive understanding of cyber threats and their potential impacts have more extensive cyber governance practices" [7].[15] Cyber security has been described by some as "today's most pressing corporate governance issue" [576, p. 425], particularly given the interest from markets and regulators. Some industry-specific regulators explicitly reference cyber security in their governance requirements, e.g. [12, Annex 11D] [1] as well as making implicit references in the context of risk management, e.g. [12, SYSC4.1.1].[16] Board members are expected by regulators to "ensur[e] the adequacy of a company's cybersecurity measures" [74]. Board members, although not the primary focus of this study, are an important group of participants within it and, therefore, it is important to understand the context of their role with regard to cyber security.

In some cases, regulators will subject the organisations they govern to "cyber stress testing" [58, p. 38]. Some regulation requires mandatory divulgence by companies in the event of a cyber-security breach [576] and, regardless of industry, broader, and increased, focus on cyber security from regulators is anticipated [576]. Cyber-security regulations can even impact on, or undermine, other areas of governance [547]. Self-regulation has been shown to be ineffective in other areas of risk, e.g. [675], with some observing similar outcomes in relation to cyber security, e.g. [752]. Beyond regulatory requirements, UK businesses are also subject to cyber-security assessments from government departments. These include the DCMS "health check" mentioned above which surveys board members, with the primary respondents for each company in the 2018 survey being the chair of the Audit Committee [14, p. 57]. Further, they are

[14] This, again, indexes moral associations, as to be healthy is to be 'good' [329].

[15] It also identified that "[w]here businesses have a Chief Information Security Officer (CISO) reporting directly to the board, they are more likely to rate the information they receive as comprehensive" [7].

[16] "A firm must have ... effective processes to identify, manage, monitor and report the risks it is or might be exposed to, and internal control mechanisms, including ... effective control and safeguard arrangements for information processing systems" [12, SYSC4.1.1].

also subject to cyber-security governance from their insurers, which may even be more effective than some forms of direct regulation [407].

Examples of cyber-security governance include the use of published standards, creation and enforcement of policies, establishment of organisational norms and the use of dedicated security teams [726]. International standards of 'best practice' in cyber security, such as ISO27001 [43], describe the components required for the effective management of cyber-security concerns within an organisation, and practice-based studies of cyber-security governance have focused on developing maturity measurement models against such standards, e.g. [525]. Cyber-security governance may become more overt or formalised following a data breach [489], which, as mentioned above, can include making the decision to hire a CISO [464]. Effective governance may depend on the existence of cyber-security expertise at board level [391]. The importance of cultural factors in security governance, including "human values" [470] and "civic virtue" [423] have also been highlighted, which implies that a 'one size fits all' approach to cyber-security governance, particularly in a multi-national organisation, may be ineffective.

While some assume that cyber security is the responsibility of an organisation's information technology (IT) department, e.g. [106], others argue that security should not be considered in this way, e.g. [760]. Although distinct from IT [225], cyber security is often associated with this domain, e.g. [276, 487], and, therefore, with IT governance. Computer scientists Peter Weill and Jeanne Ross define the latter as "*specifying the decision rights and accountability framework to encourage desirable behaviour in using IT*" [773, p. 2] (italics in original). Deciding not to implement IT governance may "no longer [be] a plausible option for any organization" [522, p. 78], and this is a topic to which I now turn.

IT Governance

Accountancy scholar Roger Debreceny states that "we know very little about what constitutes a successful path to ITG [IT Governance]" [276], while information systems scholars Johan Magnusson et al. state that "not governing IT is no longer a plausible option for any organization" [522]. Weill and Ross define IT governance as "*specifying the decision rights and accountability framework to encourage desirable behaviour in using IT*" (italics in original) [773, p. 2]. Extending Weill and Ross, Roberts discusses 'desirable behaviours' within an organisation as being "initiative" ("pursuit of individual goals") and "cooperation" ("promoting . . . common goals") but highlights the conflict that exists between them in a complex environment that involves the performance of multiple activities [636, pp. 106-7].

Information systems scholar Jannis Kallinikos [459] utilises a metaphor from philosopher Nelson Goodman [368] to describe information systems as akin to a musical score: he mentions “a set of instructions . . . [producing] outcomes” [459, p. 40]. What is not addressed, however, is that different, unintended, outcomes can be achieved with regard to information systems. These could result from software vulnerabilities, misconfiguration or user error. Building on the musical metaphor, notes could be played out of sequence or new notes introduced, with the result that the integrity of the piece is affected. Furthermore, this may not be noticeable to the listener, particularly if they are unfamiliar with the piece being performed and, in addition, an unauthorised party may be involved. While cases of guerrilla musicianship may be rare, they are certainly possible, whereas with regard to information systems, such situations are widespread [173, 239, 438]. Philosopher Aaron Smith, contrasting the positions held by fellow philosophers Bruno Latour and Don Ihde, highlights that culpability for undesirable events may lie as much with the designers of the technology that brings about such events as it does with those who use it [698, p. 190], which would extend to designers of software being culpable for breaches involving that software. From the perspective of cyber security, if there is a question of ‘culpability’ then this may suggest a need for policing, in order to identify transgressions, or assign blame.

2.2.3 Summarising cyber-security practice in organisations

The literature presented here shows that considerable attention is focused on implementing and operating controls on staff, including education, discipline and technological restrictions. Cyber security is one of a number of areas requiring governance by organisations, which itself is a normative concept across UK businesses, partly due to a mandate from government, via regulators. Governance manifests in a number of different ways, with oversight being a common theme. This supervisory aspect appears to be part of the role of a CISO but, importantly, the literature shows that the overall purpose of a CISO is unclear, with them inhabiting multiple and potentially conflicting roles within commercial businesses.

In order to understand more deeply the factors involved in this gap in knowledge, the remainder of this chapter explores more conceptual aspects of cyber-security practice that relate to the purpose of the CISO, beginning with concepts of security and identity.

2.3 Concepts of security and identity

In this section, I present core concepts of security and identity, which provide an important foundation to understanding how cyber-security practice manifests within commercial organisations. I begin by synthesising broader concepts of security from the literature, as 'security' must be understood as a precursor to understanding 'cyber security'. I then turn to concepts of identity, due to a number of overlaps between security and identity, not least in relation to the continued existence of self.

2.3.1 Security and cyber security

The compound nature of the term 'cyber security' results in meanings and metaphors relating to the modified word 'security' being appropriated by the composite phrase [162]. These "foundational metaphors" [162, p. 40] may be either distinct or implied, and may have both deliberate and unexpected consequences [162]. These associations have been constitutive for cyber security, and understanding these connections to broader concepts of security provides a crucial foundation for exploring how cyber security is practised.

Following critical security theorist Jef Huysmans, I approach 'security' as a "thick signifier" [430, p. 228], which brings into play societal interactions and political motivations. Descriptions and definitions of security as a concept are many and varied, with a number of scholars arguing its indefinability [151, 190] and others arguing against a "myth of ... intractability" [545, p. 83]. Huysmans highlights the importance of clarity, arguing that it is critical to establish, for the audience, exactly which topic is being discussed, particularly where that topic may be ambiguous [430]. Security itself is a "philosophically problematic" [282, p. 149] concept that "[f]rom its origins ... has had contested meanings, indeed, even contradictory ones" [282, p. 152]. While it is debatable whether security is an "essentially contested concept" [190, p. 7] [105],[17] it is "far from being a stable or universally homogenous concept" [179, p. 291] and is "insufficiently explicated" [105, p. 24] to the extent that some variations such as "national security", a topic to which I return further below, become "useless for everyone but the politicians" [105, p. 26].

McSweeney makes the point that the very concept of security, like other terms within IR, is "ideological[ly]" conflated [545, p. 84]. Critical theorist Mark Neocleous also highlights the ideological aspects of security and its intangible, even transcendental nature [568]. Another critical theorist, James Der Derian, makes a similar point, describing how security is perceived as "metaphysical" [282, p. 149] in nature, and further implying a deification of the concept. Der Derian questions "dogmatic" conceptions of security, arguing that this has resulted in unclear meanings, and "hubristic, even damnable overconfidence" [282, p. 152]. Discussing Hobbes [414], Der Derian challenges the assumption that security is an *a priori* requirement for existence [10,

[17] Although this belief persists, e.g. [248]. The term originates from social theorist Walter Bryce Gallie [350].

pp. 153-4]. However, for many in the IR field, security is about survival. Security theorist Barry Buzan describes this as "the bottom line" [190, p. 19], a position also held by Huysmans [430]. McSweeney disagrees [545, p. 92] with Buzan and fellow security theorist Ole Wæver that security is "the pursuit of freedom from threat" [190, p. 18] [764, p. 23]. Coles-Kemp et al. summarise McSweeney's view of security as "the freedom to live free from fear as well as protection from harms" [226, p. 3] [16, p. 3], echoing the thoughts of security theorist Paul Roe who considers security as the protection of "values" [641, p. 779], distinguishing between "freedom to" and "freedom from" [641, p. 793]. Others have differentiated various types of security, with "security as survival" being distinct from "security as being" [714, p. 526]. The former is a "traditional" notion [714, p. 527], with the latter being distinguished as ontological security, a concept from sociologist Anthony Giddens [359] that political scientist Jennifer Mitzen defines as "security of the self" [551, p. 341], and which is explored in more detail in Section 2.3.3.

Cyber security is one of "many different kinds of security, e.g. economic security, environmental security, military security, social security, physical security . . . " [105, p. 24]. Although these may, and possibly should, overlap, they are often "compartmentalis[ed]" such that "people working on 'social security' have absolutely no contact with people working on 'national security' " [568, p. 6].[18] However, cyber security does not exist in isolation. It is part of, and constitutive of, "other forms of security" [223, p. 3]. Coles-Kemp proposes the broader term "digital security" to encompass the combined social, political and technological issues associated with "everyday" security interactions [223, p. 3], including the psychological security of the individuals concerned [223, pp. 5-6]. However, this terminology, "focuse[d] on technologies that predominantly rely on access to the World Wide Web" [223, p. 3] does not necessarily provide enough breadth to encompass organisational forms of cyber security that include non-technological interactions with data, such as those that are paper-based, or, arguably, those that are designed to be self-contained networks that do not communicate externally, such as those used by industrial control systems, although the latter may not be as segregated as they once were [570]. Hence, I continue to utilise the term cyber security throughout this thesis, and, as explained in Chapter 1, this term is preferred over 'information security'.

As a term, cyber security suffers from multiple, and inconsistent, definitions [194] and is, "at best, poorly defined" [107, p. 587]. Typically, it is conceptualised as the protection of technological systems from forms of technological attack [194] but is in-

[18] Cyber security is, however, one area where there are regular interactions with national security, as I discuss further below.

creasingly recognised as a much broader sociotechnical concept [225, 246], that includes human, political and other social factors [223, 673]. Security researcher Tim Stevens describes it as "a means not only of protecting and defending society and its essential information infrastructures but also a way of prosecuting national and international policies through information-technological means" [716, p. 11], further defining it as "a sociotechnical 'assemblage'",[19] constituted by its various "actors and artefacts and their contingent and dynamic relations" [716, p. 32]. As well as being ill-defined, its definition can be fluid, and its practice performative, with such performances contributing to the ongoing negotiation of its meaning [673]. This fluidity and dynamism, this entanglement of multiple participants, underlines that cyber security[20] is, as IR scholar Lene Hansen and information scientist Helen Nissenbaum [387] highlight, socially constructed. The socially constructed nature of cyber security, and the influence this has on the methodology adopted in the present study, is described in more detail in Chapter 3.

Discourse about security

Security can be considered as "a discursive (intersubjective and performative) practice" [303, p. 106], as summarised by security researcher Myriam Dunn Cavelty, even as a "*speech act*" (italics in original) [763, p. 46]. Security depends upon discourse for its meaning [179], and indeed its power [282, p. 154]. How security is articulated, the language used and indeed the wider rhetoric surrounding it, construct its meaning for its audience [179, 282, 568],[21] possibly with very deliberate, manipulative intent [568, p. 172]. However, as Neocleous states, "talk about security is often unintelligible" [568, p. 2]. Similarly, Stevens points out an "inability to settle upon mutually comprehensible language" [716, p. 3] with regard to cyber security. This unintelligibility and intangibility perpetuates uncertainty, a topic I return to later in this chapter. The very ambiguity of security may indeed be beneficial, "an asset rather than a liability" [189, p. 111].

A 'linguistic turn' has been evident within security research for some time [432], as well as in organisational research, e.g. [85] and information systems research, e.g. [298], and it is crucial to consider the effects of language as constitutive of reality regarding security. Talk about security and security issues creates a reality for its audience that becomes broadened through association [432], expanding explicit references to threats and controls to create implicit relationships, creating a "network of suspicion" [432,

[19] Utilising a concept originating from philosophers Gilles Deleuze and Félix Guattari [279] and employed by many others, e.g. [497], although not necessarily in equivalent ways [559].

[20] Including cryptography [642].

[21] As well as an identity for its author, a topic discussed in Section 2.3.3 and in Chapter 4.

p. 377]. Huysmans refers to "little security nothings" that he considers to be more important than explicit speech in creating a securitized reality and which "challenge the boundary between security practice and daily life" [432, p. 377], thus making them more 'real' for the general population. Huysmans also describes how these practices result in an extension of securitization, including "meshing ... business with national security" [432, p. 377], a point to which I return in Section 2.3.2.

Dunn Cavelty refers to the creation, through discourse, of a "reservoir" [303, p. 107] of terms and concepts that are drawn on by those who talk about security. Specifically in relation to cyber security, she identifies how different actors contribute to this reservoir which is then tapped by others, particularly political actors, but also by media. She identifies how security practitioners contribute to sustaining the reservoir, and the implications of "discursive constructions ... both setting the linguistic rules of the game and ... being used instrumentally" [303, p. 118]. Such implications include logics of security influencing apparently unrelated issues [618] and, as organisational scholar Barbara Czarniawska points out, "other people or institutions concoct narratives for others... *this is what power is about*" [256, p. 5] (italics in original).

Metaphor. Many of the constructions referred to by Dunn Cavelty involve metaphor. Organisational scholar Ann Cunliffe describes how "[m]etaphorical and poetic ways of speaking can be very potent in connective and suasive ways" [253, p. 367], highlighting their importance in constructing concepts of security for an audience. Dunn Cavelty refers to metaphor regarding security as "powerful perception-shapers and anchoring devices" [303, p. 118]. That power can manifest in ultimately "unhelpful and dangerous" ways, including in relation to cyber security [171, pp. 83-4]. As security researchers David Betz and Tim Stevens point out, metaphors and analogies are "linguistic device[s] for transferring meaning from one subject to another" and those meanings bring with them other associations, with both intended and unintended consequences resulting [137, p. 148], something also highlighted by IR scholar Jordan Branch. Branch describes how such transference of meaning can be "politically consequential", affecting how resources are allocated and where accountabilities are seen to reside [162, p. 39], as well as arguing that tacit associations of meaning may prevent the consideration of alternative responses [162, p. 62].

One metaphor common in security practice is that of perimeters and fences, of protecting internal assets from external threats. This is observed in cyber security, e.g. [115, 501], as well as broader concepts of security. For example, Neocleous uses a similar, but distinct, metaphor of security being a "garden ... an ordered environment" with both "order and surveillance . . . cultivation and progress" [568, pp. 91-2].[22] In cyber security, such approaches are increasingly considered to be obsolescent, particularly due to deliberate deconstruction of boundaries by organisations [501]. A "barricaded castle" [115, p. 146], even one built on sophisticated and layered controls [440], is not just unfashionable but ineffective, even "hopeless" [501, p. 255].[23] This metaphor also reflects and maintains a particular (dated)[24] attitude to security [501] of self and other that may index other metanarratives [247, 447], a concept I now explain.

Master and metanarrative. Metanarrative is a concept developed by philosopher Jean-François Lyotard [517]. A metanarrative is a form of narrative that "seeks to suppress other narratives by imposing its logic on all of them" [517, p. 952]. As a result, it can have a constraining (and regulatory) effect,[25] inhibiting the consideration of other perspectives [517]. An associated concept is that of master narrative. This refers to established narratives that exist at a wider societal or "cultural" level [129, p. 43]. They may provide referenceable features including characters and specific language, cultural norms [472, p. 266] and also moral positions. Sociolinguist Scott Kiesling refers to "indexicality" [472, p. 265], where such references tap into a wider pool of cultural knowledge and can carry a rich meaning as a result. Specific words or phrases can be accompanied by a deep cultural significance and these associated meanings may be used wittingly or unwittingly, consciously or unconsciously, and provide opportunities for deliberate manipulation. For example, indexing a master narrative through a rhetorical device, for example that of tragedy, an individual, organisation or state can emplot themselves as a tragic or triumphant character [256, 693]. Czarniawska points out "the lack of structural differences between fictional and factual narratives [which] is suspected to account for most of their power" [256, p. 9] and others also point out the potential for fictive components in meta and master narratives, e.g. [366]. Political researcher Ariane Bogain refers to the use of "incantation technique[s]" [145, p. 488] in security discourse, particularly in their use to legitimate actions taken by invoking concepts, such as "laws and principles" [145, p. 488], that have not, in fact, been followed. This introduces an aspect of power in relation to discourse which I now briefly discuss, as this is particularly relevant to security discourse.

[22] Spatial metaphors are also common in traditional concepts of security, particularly in national security, and, indeed, their predominance in cyber security may originate from this source [162].

[23] Security researchers Christian Leuprecht et al. call for an alternative metaphor to be employed of "*computing in compromised environments*" [501, p. 255] (italics in original).

[24] "[M]edieval" [501, p. 251].

[25] Regulatory effects are discussed further in Section 4.2.4.

Discourse and power. Discourse relating to security often originates from those in positions of power, whether from local management in organisations, e.g. [618], or more broadly, such as from politicians, e.g. [179]. Those with power have "the ability to mobilize discursive resources in order to marshal discourses or counter-discourses, and the ability to get others to acknowledge or take seriously a position that is being proposed" [124, p. 69]. However, this power is not just reserved for managers and politicians. Those in specialist or 'expert' roles, particularly "security professionals" also have considerable power to define what is and what is not a security issue [431, p. 72].[26] Security discourse can also be resisted by those subject to that power. In a study performed by criminologist Prashan Ranasinghe, resistance was identified as an attempt to establish broader definitions of security, exploiting an existing discourse from management. However, management's definition ultimately prevailed [618].

The media also plays an important role in security discourse. Criminologists Adam Crawford and Steven Hutchinson describe[27] how people experience and form opinions on security in modern life (and by extension, modern business) as being affected by non-local factors, such as what they hear or read on the news [245, p. 1196].[28] One important source of power in the creation and use of narrative is emotion. As psychologist Nico Frijda points out,

> "[u]nder appropriate conditions, implausible stories are considered possible or likely if they foster hope or hate; dubious sources of information are believed. The hopes engendered by fear can have the slenderest of bases, without the slenderness being noticed by the subject. Apprehension may alert to possible dangers but it also tends to create belief for unbelievable stories" [341, p. 118].[29]

I now explore these emotional aspects in more detail.

Emotional aspects of security

Crawford and Hutchinson discuss the inherent emotion in security [245, p. 1196], particularly fear and anxiety. Citing political scientist Jon Elster [313], they describe how "fear, anger and anxiety" [245, p. 1196] "induce *urgency* as well as *impatience*" [313, p. 218] (emphasis in original), and indeed, elsewhere, Elster himself describes how "[for

[26] I discuss expert roles in more detail in Section 2.3.3 below.

[27] Alluding to Giddens' thoughts on the disembedding of social relations [358].

[28] Both the role of media and those in power in shaping of security discourse is discussed in more detail in Chapters 4 and 6.

[29] She adds that "[w]artime rumors offer striking examples. They concern successes of one's own side as well as evils perpetrated by the enemy" [341, p. 118].

some people] emotion might be so strong as to blot out cognitive analysis" [312, p. 14]. Further, biologist Ralph Adolphs points out that a biological response in humans is observed "not just by occurrent stimuli, but merely by thinking about such stimuli [as fear and anxiety]" [72, p. R88], adding that such thinking can distort perceptions. This is important as emotions relating to security issues may have a strong influence on decisions relating to those issues. Emotions also "provide the main support of social norms" [312, p. 98]. The latter "guide behaviour by the sanctions imposed on those who violate them" [312, p. 99], which highlights an aspect of punishment that I discuss further in Chapters 4, 5 and 6. As well as potentially inhibiting cognition, emotions may both "modify and distort" [312, p. 108] it, which affects behaviour. This includes "undermin[ing] rationality" [312, p. 156], affecting "probability and credibility estimates" [341, p. 118] and having a complex role in decision-making [312, p. 163]. Therefore, considering emotion and emotional responses is crucial in understanding security.[30]

Fear is fundamental to the perceived need for security, and, by extension, to the need for society [282, p. 158]. These fears may also have a historical dimension [190, p. 137]. The association between fear and security is both long established and an apparent necessity,[31] although Der Derian, summarising a perspective from philosopher Friedrich Nietzsche, suggests that achieving security "at the cost of ambiguity, uncertainty, paradox" is detrimental, as these are "all that makes a free life worthwhile" [282, p. 159].[32] Fear and anxiety can motivate actions relating to security, including the "purchase [of] security technologies ... even where this constitutes a 'grudge spending' " [245, p. 1197].[33]

Neocleous, referencing philosopher John Locke [508, p. 217], describes how "uneasiness" [568, p. 28] drives the need for security, as well as driving human actions. Cyber security can be "scary" [385], with threats often narrativised as fearful, e.g. [302], often with specific intent, such as to affect behaviour, e.g. [449]. Media coverage relating to cyber security often positions it in a similar manner, e.g. [451, 735], particularly in combination with crime, where "fear becomes normalized" [770, p. 862], but also as part of an "apocalyptic" [716, p. 121] war, e.g. [616], a point I return to in Section 2.3.2. In particular, cyber security can be subject to "[t]hreat inflation" [137, p. 148]. These emotional aspects, particularly in relation to fear, also introduce a moral aspect to cyber security which I now present.

[30] Emotions also play an important role in identity construction, as I will discuss further below.

[31] "Security is always threatened by danger" [304, p. 16].

[32] Although this opens up a further question regarding what a "free life" actually entails [620].

[33] This is an extension of a concept from criminologists Ian Loader et al. [507].

Moral associations of cyber security

Cyber security is often positioned as being imbued with morality, whether through threats from ‘bad guys’, e.g. [761], and established ‘enemies’, e.g. [238, 771], through an association with rights, responsibilities, and societal obligations, e.g. [422, 423], or through user behaviour being either ‘good’ or ‘bad’, e.g. [712], ‘right’ or ‘wrong’, e.g. [627]. Those who do the wrong thing are often subjected to “blaming and shaming” [479, p. 13]. Further moral associations arise from the alignment of cyber security with “the common value of freedom from harm” [573, p. 64], and with caring [479].

Sociologist Jean Baudrillard suggests that there is a moral conflict associated with technological progress [116, p. 173]. Cyber-security threats may reflect an element of “technological suicide” [116, p. 173], a consequential counterpoint to the prevalence of technology in everyday life, including business. They may even be an essential part of the picture, with society requiring a “Devil” [116, p. 173] with whom a pact has been made. Cyber security features aspects of moral ambiguity [222, 674], including whether cyber-security practices in businesses themselves introduce moral problems [532].[34] Perceptions of whether certain cyber-security behaviour qualifies as ‘moral’ may also be variable [352, 613], with a risk of “immoral socialization” [268, p. 248] needing to be considered. Moral consensus is equally elusive [344] and much debate persists in relation to whether morality is subjective or objective, e.g. [293, 797].[35] Personal morality can also affect the effectiveness of cyber-security controls on users [267].

Some discourses of risk may be dissociated from moralistic opinion, preferring non-emotional, practical explanations of hazard instead [344]. Risk-taking behaviour, however, has itself become associated with its own morality [344]. Cyber-security discourse, despite its potential for non-emotional risk-focused narratives, appears to be strongly influenced by moral positions, both explicit and implied. These often index other moral positions, such as references to cyber-security “hygiene”, e.g. [712, 757]. This is a moral judgement that, when taken to extremes, may even result in the categorisation of the non-hygienic as “pre-criminal” [329].

Building on these moral aspects, I now turn to a discussion of political aspects of cyber security.

2.3.2 Cyber security and politics

As summarised above, there is no single ‘security’; rather, security is contextual, culturally and politically [430], and is, therefore, also manipulable. Security issues can

[34] Beyond cyber security, the ethics of security more broadly is also debated – IR scholar Jonna Nyman [581] provides a useful summary.

[35] These aspects will be discussed further in Chapter 4.

be, and have been, used politically to exert controls, cement power [469] and conduct atrocities [234, 377]. Crawford and Hutchinson, referencing Buzan et al. [192] and IR scholar Matt McDonald [541], point out that "framing something as a 'security' issue allows things that might ordinarily be politically untenable to become not only thinkable but widely acceptable, including the introduction of extraordinary or exceptional new legislative powers or measures" [245, p. 1188]. As Huysmans describes, "[t]he key political quality of the speech act of security is a break in the normal political rules of the game" [432, p. 372]. Such an approach has been observed in organisations, as well as at a state level, with security issues used to limit workers' rights and regulate behaviour [567].

Further, as IR theorist Didier Bigo points out, while there are actors interested in security, there are also actors interested in insecurity [138, p. 314]. As noted by Neocleous, there is a wider security industry that "must . . . ensure that security is never really achieved" [568, p. 156]. He also states that "[t]here is no shortage of insecurities, but all of them can be dealt with . . . if the money is right [568, p. 156] and, as well as the commercial benefits alluded to, he describes how insecurity is relied on by the state to achieve its aims.

Security creates and maintains power for states, as well as for "security professionals and the political elite" [432, p. 378]. Huysmans' concept of "security act" allows for questioning of the actions and performances that contribute to this power [432, p. 378]. States are concerned by "changes that can destabilise [them]" [138, p. 304] and, similarly, Der Derian points out that current practices of international security are based on "normalization or extirpation of difference" [282, p. 151]. As Coles-Kemp calls for, it is important to "critically examine the power relations and political imperatives that give rise to . . . [security] concerns", and I return to this topic in greater detail in Chapter 6. These aspects of state power are further connected with the enmeshed nature of cyber security and national security, as I now explore.

Cyber security and national security

Cyber security in both academic and mass media communication abounds with military tropes, e.g. [147, 463, 504]. Narratives relating to cyber-warfare are common, providing a number of referenceable components which can be observed in popular discourse relating to cyber security, as well as themselves reusing components of a broader geopolitical narrative, such as 'arms race'. The term "cyber arms race" [504, p. 50] is established in IR scholarship [463, 692] and technology [721], as well as in business, e.g. [486, 616] and other non-academic circles, e.g. [632]. Such narrative extension goes beyond simple language re-use however; more conceptual elements such as the sense of there being a ‘good side’ versus a ‘bad side’, of there being ‘old enemies’ and of a threat to a way of life, are also prevalent.[36] Attributing a hacking incident to North Korean hackers, e.g. [238], indexes a wider narrative relating to the threat to the Western way of life from communism; communism or threats to way of life aren’t explicitly mentioned but are *indexed* by the reference to North Korea. Indexing may be more subtle than this and refer to more complex discourses, such as those of masculinity [472], and may be value-laden [472, p. 285]. There may also be “hidden transcripts” [668] at play that are supportive of hegemonies [375], a point I return to in Chapter 6.[37]

Cyber security has been used to “support claims to exceptionalism” [191, p. 268] through government legislation, e.g. [745], and state acts, e.g. [55], which may qualify it as a “macrosecuritisation” [191].[38] Security scholar Eneken Tikk-Ringas describes how “[n]ormative frameworks provide a grid for legitimating and illegitimating the exercise of state power” [736, p. 48] and those who define security threats, and the responses to them, occupy “a privileged position” [701, p. 498]. ‘National security’ has become a powerful “semantic guide” [282, p. 163]. Security narratives that relate to terrifying potential future events also contribute to national identities [130], and “the projection of sovereignty is demonstrated, at least in part, through state activities around cybersecurity” [224, p. 47].[39]

The UK government refers to cyber-security threats against “critical national infrastructure” [21, 411], underlying the seriousness of the perceived threat to society. They also highlight the role that businesses play in this, describing how “[t]he cyber security of certain UK organisations is of particular importance because a successful cyber attack on them would have the severest impact on the country’s national security” [411, p. 39]. Businesses are seen as a crucial component of the UK’s National Cyber Security Strategy [412] and, as described earlier, have their cyber-security “health” regularly surveyed [7]. Similarly, legal scholars Le Cheng et al. identify that “critical infrastructure is the key referent object in U.S. cybersecurity legislative discourse” [213, p. 297], which equally highlights “the critical role of private sectors” [213, p. 297]. Other scholars have highlighted the importance of corporations in achieving national security, e.g. [199], with some problematising this relationship, e.g. [307]. Cyber-security threat is positioned by governments as a form of permanent emergency, a concept I now discuss.

[36] Morality in cyber security will be discussed further in Section 2.3.1.

[37] And acknowledging that hegemony itself may be an “overly loaded term” [736, p. 47].

[38] Buzan and Wæver do not mention cyber security in their discussion of macrosecuritisations, however, other scholars have subsequently brought cyber security into critical security studies, e.g. [750, 482].

[39] Linkages between cyber security and state identity are discussed in more detail in Chapters 4 and 6.

Permanent emergency

The concept of permanent emergency has been established and discussed by a number of scholars within the domain of IR, e.g. [568]. This refers to the perpetuation of a state of threat, whereby a population's security, and often its way of life, are subject to, or positioned as being subject to, various forms of continuing menace. Such a state may reflect a 'requirement for insecurity' that has been a feature of international relations "for centuries" [545, p. 2]. The existence of such an emergency can support the disciplining and directing of citizens [179, 568] through extraordinary interim measures that are never revoked and thus become firmly established [568], both in wider society and in workplace environments [567], even undermining human rights [374]. The implementation of various restrictions on freedom in the name of 'security' [179, 568] is a concept which has many parallels with the 'state of nature' described by Hobbes [414, 546], and which has been highlighted as underpinning power structures by others, e.g. [337]. Permanent emergency can also be motivated by "attach[ment] to conflict . . . a harmful or self-defeating relationship can provide ontological security" [551, p. 342], even where seeking the latter results in a position of increased risk [551].

A permanent emergency offers benefits as a master narrative that can be invoked to support actions taken by businesses, and individuals within that business, whether to justify investment or to justify restrictive controls such as surveillance, as I discuss further in Chapter 6. The positioning of cyber security as warfare, which is a narrative repeated by both media and governments [716], establishes that concept in the minds of all parties to that war, whether attacker or attacked. Adversaries, or even just those who disagree, will respond to the narrative of cyber security-as-war and then treat it as such, focusing on attack and defence, rather than seeing it as anything else, for example, as a collective problem of identifying and addressing weaknesses that threaten all. This could lead to actions that have unintended consequences, such as state purchasing, and hoarding, of vulnerabilities, e.g. [756]. Cyber security-as-collective-problem could be considered a "flattened narrative" [323], with preference instead provided to the cyber security-as-war concept, which supports the maintenance of existing power structures. This can also be considered as indexing a metanarrative of existing or 'traditional' enemies [716], and the "superiority of . . . the West" [568, p. 172], as suggested by the references to (ex-)communist states[40] observed in media reports relating to cyber-security threats e.g. [148, 238, 597]. There is an almost paradoxical relevance of both (philosopher) Michel Foucault's and (military theorist) Carl von Clausewitz's perspectives on war, with cyber war being a "mere continuation of policy by other

[40] Who are also competitors of Western states.

means" [758, p. 12][41] and cyber politics being "the continuation of war by other means" [337, p. 15]. The implications of this on power structures, something that Foucault also describes [337], and the economic benefits associated [568], are discussed further in Chapter 6, which primarily employs the work of Thomas Hobbes as an analytical lens. As mentioned above, Hobbes' work is particularly relevant to the notion of permanent emergency and, hence, I provide a brief introduction to this below.

The relevance of Thomas Hobbes. Hobbes has been influential in the very definition of security [461, p. 69]. Other scholars have previously employed his work in exploring the links between cyber security and state security, e.g. [224, 460], including aspects of surveillance, e.g. [117, 227] and cyber warfare, e.g. [169]. Previous research has highlighted the importance of corporations in achieving national security, e.g. [199], with some problematising this relationship, e.g. [307]. The threat that cyber security may pose to national and international security has also been extensively explored by others, e.g. [771], including the societal risks posed, e.g. [692], the impacts that responses to this may have on freedoms, e.g. [573] and the threats to state power associated with cyber-security risk [199]. In a broader context, the application of social perspectives to risk is well established, e.g. [122] with the impact, and use of, fear within society, e.g. [123, 344, 358] and how this supports wider power structures, e.g. [568], being a common thread. Hobbes' work is discussed in more detail in Chapter 6.

Cyber security is a consumable commodity

Narrativising cyber security as a geopolitical issue, and as a necessary military capability [504] may help to transform it into a consumable commodity [116, p. 61]; this may have the associated impacts on growth, alongside perpetuation and re-constitution of power and privilege, that Baudrillard describes [116, pp. 59-61]. He notes that "military expenditures" are "more reliable, easier to monitor and more effective in achieving the survival and goals of the system [the "industrial or capitalist systems"]" [116, p. 59]. Others also note the "for-profit" aspects of security [274], and that "to sell security . . . [the security industry] must first help generate insecurities" [568, p. 154].[42] Society, and its associated hierarchies and inequalities, is maintained through consumption in Baudrillard's view. A threat to that society can therefore be utilised as a means to perpetuate it if dealing with that threat relies on consumption and, in which case, the continued existence of that threat would be beneficial for that society. He suggests a role for "violence" in society, that " 'pacified' daily life thrives on a daily diet of con-

[41] Although this conception may not be original to von Clausewitz [337, p. 48].

[42] I discuss consumption of cyber security further in Chapter 6.

sumed violence" [116, p. 160], speculating that this acts as a form of "inoculat[ion]" [116, p. 160] against "fragility" [116, p. 160], the latter contributing to a "fund of anxiety"[116, p. 162] that has parallels with the discursive "reservoir" referred to by Dunn Cavelty [303, p. 107].

Building on the aspects of fear and permanent emergency introduced above, I now turn to a discussion of how that fear impacts upon identity.

2.3.3 Ontological security and identity

In this section, I build on the concept of ontological security that was briefly introduced in Section 2.3.1 and discuss its relevance to concepts of identity, both organisational and individual. To recap, ontological security relates to the security of the self and is thus closely associated with concepts of identity. Both ontological security and broader concepts of identity offer a valuable perspective on understanding different aspects of cyber-security practice within businesses, as I will expand upon throughout this section.

Identity is considered important as not only does it influence how individuals and organisations are perceived by others, an identity may also have functional use in enabling "acting with foresight" [136, p. 58]. As management scholars Sierk Ybema et al. describe, "the notion of 'identity' may be regarded as a fundamental bridging concept between the individual and society ... it refracts what can be seen as a 'permanent dialectic' between the self and social structure" [793, p. 300]. Organisational identity, in particular, has been linked with purpose, e.g. [64, p. 1050] and "long-term survival" [175, p. 38]. Therefore, understanding its construction offers more than simply a perspective on interaction and presentation but also potentially an appreciation of how identity may influence action in multiple domains.

Ontological insecurity

A lack of ontological security, or "ontological *in*security" [219, p. 509] (emphasis added), can motivate individuals, or organisations, to respond by constructing their identity in a way that (re-)establishes that security of self. This process is known as identity work, a term which refers to the tactics used by individuals [705], or organisations [176], to construct and maintain an identity. This well-established concept was developed from a seminal study by sociologists David A. Snow and Leon Anderson [705] that drew significantly on earlier work by sociologist Erving Goffman, e.g. [365] and has been extended broadly, including to organisational research, e.g. [176, 203]. Organisational identity itself is an established concept, e.g. [84], although others have challenged this, e.g. [256].

Cunliffe suggests that individuals build a sense of ontological security through dialogic identity construction [253, p. 364]. This may be seen from the perspective both of an individual's sense of ontological security in their own sense of being within a group, such as an organisation, as well as their sense of being in wider society, particularly where that security, that sense of comfort even, in having a particular identity derives from that identity being both well-known and respected. If that identity is recognised as heroic or worthy, for example,[43] then the sense of ontological security obtained from that identity may be stronger than that of being associated with, by self or others, an identity that is trivial. Constructing an identity that is seen in a particular way could subsequently become self-sustaining, both from the perspective of the virtuous (or vicious) circle of the identity but also the 'self' of the individual, accruing to their sense of ontological security. While identity is continually being negotiated, as psychologist Michael Berzonsky describes, "to be adaptive and functional, individuals need to perceive a sense of identity or continuity across the separate temporal episodes of their lives" [136, p. 56].[44] Although self-identity may fluctuate, any changes may be constrained by a desire to maintain continuity, as this contributes to a sense of ontological security. However, this may be more difficult in conditions of uncertainty such as those in the "rapidly changing world" [136, p. 56] of modernity [358].

Ontological security can be theorised as existing at an organisational level whereby the organisation is motivated to ensure its own continued existence[45] and, therefore, identity work may be performed by organisations for this reason. Organisational scholars Brianna Caza et al. summarise a number of different motivations for identity work within organisations that all suggest, at least in part, a concern with ontological security [203]. Through organisational dialogue, such as that expressed in annual reports or other publicly-available company documentation, organisations may seek to build their identity and maintain ontological security in the same manner as individuals. An organisational drive to develop a sense of ontological security may also support the development of an individual's ontological security and vice versa.

Ontological insecurity resulting from cyber-security events. An inability to effectively respond to, and recover from, crises, including those relating to cyber security, can impact on reputation [87, 728], and, therefore, identity [64]. Impacts on reputation result in shame, which can have a considerable impact on identity [359], particularly as shame, as an "anxiety-state ... [is] public" [359, p. 65]. Giddens insists that "[s]hame should be understood in relation to the integrity of the self" [359, p. 65], underlining its im-

[43] Heroic identity constructions are discussed in more detail in Section 2.3.5.

[44] Here, Berzonsky is citing another psychologist, Erik Erikson [318].

[45] As will be discussed further in Section 2.4.2.

portance as a threat to ontological security. Public narratives relating to cyber-security breaches often contain an implication of ‘the abnormal’ through the use of terms such as “sophisticated” e.g. [47] or “sustained” [41]. Czarniawska describes how “[n]arrative thrives on the contrast between the ordinary, what is ‘normal’, usual, and expected, and the ‘abnormal’, unusual and unexpected” [256, p. 9]. Such abnormality implies an imbalance, and this “disequilibrium” [737, p. 111][46] provides a “minimal plot” [256, p. 19] that may be enough to change a narrative (‘there has been a cyber-security incident’) into a basic story (‘there has been a disruptive cyber-security incident; this is not normal. We are taking action’), which can further be embellished to make it more powerful (‘We have suffered a “sophisticated, malicious criminal attack” [47]. We are taking action’). The latter is, according to Czarniawska, “a pretty standard story” [256, p. 86]. This demonstrates the use of a “classical rhetorical trope” [256, p. 20] that indexes a master narrative. In this case, the organisation positions themselves as a tragic character [256, 693].

Building on this sense of ontological insecurity being a motivator for identity work, I now briefly discuss the concept of identity threat.

Identity threats

Identity threat as a concept has been explored by a number of scholars, e.g. [125, 310], and may be well established [177, p. 1318], but the term itself is contested [599, p. 641]. Organisational behaviourist Jennifer Petriglieri defines “individual-level identity threats as *experiences appraised as indicating potential harm to the value, meanings, or enactment of an identity*” [599, p. 644] (italics in original) and also highlights “identity threat’s unique feature of arising from present cues of future harm” [599, p. 644]. Identity threats are considered to motivate identity work [177, 434], in order to maintain the (present) identity and by extension, ontological security. Organisational behaviourist David Sims suggests that an ontological dimension is present in identity work, particularly with regard to how an individual’s identity is narrativised. He describes how “not being able to excite any interest with your story seems to question your very existence” [685, p. 100]. This can be viewed as particularly important using Sims’ model of an individual’s identity being distributed; if an identity depends upon being ‘present’ in other people’s minds, then there is a risk to that identity if those people stop thinking about it. Although Petriglieri’s definition refers specifically to threats at an “individual-level” [599, p. 644], the concept of identity threat has also been applied to collectives, e.g. [177, 310]. For organisational scholars Andrew Brown and Christine Coupland,

[46] As also cited by Czarniawska [256, p. 19].

> "identity threats are regarded as being construed through identity work: they are any discursively constituted thought or feeling that challenges one of an individual or group's preferred identity narratives" [177, p. 1318].

Different strategies may be adopted dependent on both level of engagement and also whether it is the individual- or group-level identity that is under threat [310]. Social psychologists Naomi Ellemers et al. suggest that "strength of commitment to the group" [310, p. 178] is a factor in an individual's response to identity threat, although it is not clear exactly how "strength of commitment to the group" [310, p. 178] can be measured.

Brown and Coupland identified that identity threats may be deliberately constructed by individuals themselves. The participants in their research[47] used these "as a resource to author narratives of their desired occupational and masculine identities" [177, p. 1316].[48] Not only were threats constructed, they were also "appropriated" [177, p. 1316], which they use "to refer to processes of self-meaning production" [177, p. 1321]. In their study, such threats and appropriations became "shared cultural resources" [177, p. 1322], established narratives within that collective. Therefore, identity threats may be advantageous to an individual or group, and this may lead to their deliberate construction. As Brown and Coupland summarise, "putative 'threats' may constitute a supply which professionals draw on to articulate preferred versions of their selves" [177, p. 1316]. Projecting an *undesirable* future state may itself be a form of identity work; rather than a "coping strategy" [75, p. 1002], it may present an opportunity to construct or reinforce an identity that resolves that undesirability. However, while uncertainty may motivate identity work, there may be a limit to its motivating ability [359]. I now discuss specific strategies of identity work.

2.3.4 Strategies of identity work

Cunliffe advances that "authorship of self is an embodied, contested dialogical practice" [253, p. 363] and is continuous; identity is not fixed but is continually constructed and negotiated. Multiple dimensions are at play in this construction. Management scholar Nic Beech describes "tensions of meaning" [124, p. 66] that contribute to the formation of an identity and how different positions within multiple continuums of tension can result in an individual's self-identity being distinct from the identity they are ascribed by others [124, p. 67]. He proposes that "the meaning of the identity construc-

[47] Male rugby players, who they argue are "an 'extreme' case of surveilled elite professional workers" [177, p. 1319].

[48] The masculine dimension is important to consider with regard to cyber security and I return to this further below, as well as in subsequent chapters.

tion is the sum of a set of 'meaning giving tensions' which are the spectra along which people can place themselves, and be placed by others" [124, p. 68], which highlights the dialogic nature of identity as well as the multiplicity of actors potentially involved in constructing identity. As well as other actors, Ybema et al. point out that other factors affect the formation of identities, including "emotions, moral judgments and approbations, and political or economic interests" [793, p. 307]. This is particularly relevant to consider with regard to cyber security, given the economic and political interests already mentioned above.

While some may consider identity work "as a single undifferentiated category of activity" [427, p. 1120], others discuss discrete identity work strategies, e.g. [75]. These involve the construction of identities through various means, which can include narrative [256], dialogue [253], and external displays [601, 638]. I briefly describe each of these in turn as they are relevant both to how identity is created in relation to cyber security and to how cyber security features in identity constructions.

Narratives in identity

Narratives are central to the creation of identity. Linguistics scholar Bethan Benwell and social psychologist Elizabeth Stokoe argue that "it is in narrative tellings that we construct identities: selves are made coherent and meaningful through the narrative or 'biographical' work that they do" [129, p. 42]. Giddens describes how "[a] person's identity is not to be found in behaviour, nor – important though this is – in the reactions of others, but in the capacity *to keep a particular narrative going*" [359, p. 54] (italics in original). Therefore, narratives must be sustained and continually expressed in order to maintain an identity. Narrative as identity work has been observed both at an individual and organisational level, e.g. [219, 629].

Czarniawska highlights the centrality and importance of narratives in organisational life in creating identity, as well as the power dimensions associated with these [256, p. 5]. She further distinguishes between narratives and stories; the former are "purely chronological accounts" whereas the latter are "emplotted" [256, p. 17]. Both forms may be used to conduct identity work. Storytelling, or "mythopoeisis" [145, p. 480], can be used by an organisation to "control the memory of its members" [294, p. 112] in order to maintain a desired identity. Stories are richer than narratives and may be richer in affect as a result; they "permit access to the emotional life of organizations" [256, p. 42]. Importantly, as philosopher Kwame Anthony Appiah points out, stories also shape values, both in their telling and their discussion [91, pp. 28-31]; he highlights that "[w]e appeal to values when we are trying to get things done *together*" [91, p. 28] (italics in original), suggesting that an emotional connection is important for collaboration as it enables alignment between narratives.

Educational scholar Bronwyn Davies and philosopher Rom Harré introduced the concept of "positioning"[49] with regard to establishing and maintaining identity [270]; they define this as "the discursive process whereby selves are located in conversations as observably and subjectively coherent participants in jointly produced story lines" [270, p. 48]. Importantly, they note that this process, whether performed by the self or by an other, may not be deliberate [270, p. 48]; in other words, identities may be unwittingly created or assigned through discursive positioning, and identities can be created for parties *in absentia* [256]. These identities may be desirable or undesirable, congruent or incongruent with a sense of self [124, p. 65]. Benwell and Stokoe point out that individuals may "resist, negotiate, modify or refuse positions" [129, p. 43]. In addition, narratives can be "challenge[d]" [129, p.152] as a form of identity work, including the challenging of master narratives. For example, opposing or contradicting an established master narrative may construct a non-conformist identity.

Dialogue

Beech highlights the importance of dialogue in identity construction, including external discourse [124, pp. 55-57]. Dialogue involves "different intralinguistic practices" [253, p. 368], including "metaphors, stories, social ghosts, and dialogical triggers" [253, p. 368]. 'Social ghosts' is a phrase introduced by social psychologist Mary Gergen [354], and extended by fellow psychologist Kenneth Gergen [353], to refer to "inner dialogues . . . [that relate to] relationships both real and imagined" [353, p. 71]. In other words, an individual's internal dialogue with others they may or may not have ever corresponded with contribute to their sense of identity; a perspective, real or imagined, from a family member, ex-colleague or celebrity [353] could be influential in establishing their sense of self [253]. Therefore, one person's discursive identity work may affect the identity of others as they adopt, and possibly adapt, what they have heard, read, seen or otherwise experienced. These ghosts may be articulated explicitly in discourse, as well as being internal resources, and could be either highly personal or shared, and may function metaphorically [253]. Dialogue in which one of these entities is mentioned results in an identity being formed, or maintained, both in the mind of the speaker and their audience.[50]

[49] Building on earlier work by critical theorist Paul Smith [703].

[50] Association with others, particularly with groups, is another form of identity work that I describe in more detail in Section 2.3.5.

Performativity. Discourse, whether spoken or written, may have various performative effects. These can be "perlocutionary" [101, p. 101], that is, they result in effects upon their audience, and those effects may be inadvertent [101]. However, such effects are dependent on various conditions, on "good circumstances, even luck" [188, p. 151]. Philosopher Judith Butler considers that while "illocutions [i.e., utterances that have an intention, possibly, but not exclusively, directive] produce realities, perlocutions depend upon them to be successful" [188, p. 151]. In other words, the external environment, including aspects of structure such as (perceived) authority and normative concepts, may be necessary for a perlocutionary effect to result. Performativity is important to consider with regard to identity work, including whether discourse relating to identity is stating a fact about that identity, i.e., is locutionary, is intending to result in its audience perceiving a certain identity, i.e., is illocutionary, or is the actual result, inadvertent or otherwise, in the audience perceiving, or assigning, an identity as a result of that discourse, i.e., is perlocutionary. Additionally, performativity in relation to identity, whether locutionary, illocutionary or perlocutionary, can be exclusionary [513].

Associations made with other parties, as well as the use of symbols, can similarly be viewed as performative [565]. References to others may be deliberately intended to have a perlocutionary effect on an audience. Bogain refers to the use of "incantation technique[s]" [145, p. 488] by President Hollande and how "the mere mention of ... [the judiciary's] name was sufficient to give his [extreme] measures legitimacy" [145, p. 489]. Incantation may be used in identity creation, even to the extent that a role title itself may serve an incantative function in defining both an individual's identity, and that of those with whom they interact [203]. Therefore, in the context of this thesis, the job title of CISO may be implicated in the broader identity construct of the person who is assigned that role.

External displays

Externally facing artefacts can be a form of identity work for individuals [638] and for organisations [468]. These may be totems, "representations of stories" [229, p. 20] that help maintain ontological security [601]. As well as physical totems, organisational actions may be viewed as totemic [229]. Individual roles within a business may also act as totems [554], in particular, "experts" [601, p. 26], and the existence of a role, and what it represents, rather than the person occupying that role, can be "the most important part" [601, p. 4].

An external display may be an attempt to demonstrate legitimacy, particularly for an organisation. Legitimation is an established concept within social science, and management sciences in particular, e.g. [294, 719]. Management scholar Mark Suchman defines legitimacy as

> "*a generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions*" [719, p. 574] (italics in original).

Bogain builds on Suchman's definition to describe legitimation as "discourses that explain and justify the appropriateness of a social phenomenon within a 'socially constructed system' " [145, p. 480]. Organisational scholar Mary Douglas refers to the need for organisations to "[found their] rightness in reason and in nature" [294, p. 45] and Brown describes how "legitimate status is a *sine qua non* for easy access to resources, unrestricted access to markets, and long-term survival" [175, p. 38] (italics in original), survival being a key organisational concern, as discussed earlier.

Communication scholars Theo Van Leeuwen and Ruth Wodak describe how "[s]trategies of perpetuation and justification attempt to maintain, support and reproduce identities" [753, p. 93]. Similarly, Ybema et al. describe how "to claim or enact an identity facilitates the creation of a self-referential truth which maintains an ongoing position of status, defends an interest, or makes oneself acceptable or respectable to others and to oneself" [793, p. 306]. On this basis, identity and legitimation are cyclically linked; identity can legitimate and legitimation is a tactic used to sustain an identity, something observed by others studying organisations, e.g. [219]. Bogain summarises a number of legitimation techniques identified by Van Leeuwen's research, including

> "appeal to history, teleology (divine purpose or final cause), belief systems, authority, rationalisation, moralisation, narrativisation (construction of a compelling plot), mythopoeisis (storytelling), blame allocation, exceptionality or effectiveness" [145, p. 480].

Similarly, Douglas describes the importance of "analogy ... metaphor ... resemblance" [294, pp. 45-53] in achieving legitimacy. As described already, these are all techniques employed in the construction of identity.

Identity through consumption. As introduced earlier, Baudrillard suggests that "violence" [116, p. 160] drives consumption by stimulating uncertainty. The resulting "fund of anxiety" [116, p. 162] both undermines ontological security and is also a factor in its relief, by "stimulating consumption" [116, p. 163]. That consumption can include either "consumable goods or distinctive cultural signs" [116, p. 163]. According to Baudrillard, the need to drive consumption (in a society that depends on it) "*fetishis[es]*" elements that can drive consumption; not just "objects ... [but also] ideas, leisure, knowledge, culture" [116, p. 62] (italics in original). Neocleous similarly discusses the "*security fetish*" [568, p. 153] (italics in original) associated with the "commodification of security", linking this further to "the ideology of security" [568, p. 153]. Baudrillard considers the use of these 'fetishistic' elements "as signs" used to signal an identity, including that of "status differentiation" [116, p. 63]. Borrowing a theological concept, he suggests that, in a consumption-driven society, status differentiation indicated by visible signs of consumption is motivated by a desire for "*salvation by works*" [116, p. 62] (italics in original). In other words, visibly signifying what an individual or an organisation has consumed constructs an identity that is somehow virtuous, something I return to in Section 2.3.5. This sense of identification through signs is also suggested by Baudrillard as having a socially hierarchical dimension; "needs and satisfactions trickle down" [116, p. 64]. If governments and the military are at the top of that hierarchy, then their signification of the importance of a cyber-security capability may 'trickle down' to businesses, and indeed, at least in the UK, this is demonstrated by government messaging about the role that businesses play in national cyber security [411, 412]. Different types of businesses may occupy different roles in that social hierarchy of needs. Those that form part of critical national infrastructure or are part of the financial system, for example, may feature more prominent signs of cyber-security capability than other businesses, whether directly through public statements in their annual reports or through indirect means such as advertising.

Assignment and association

Self-assignment of a role is a form of identity work often observed in organisations. Management scholars Robyn Thomas and Alison Linstead's study identified an example of this whereby one participant described themselves as "an expert" [730, p. 79] as a means of identity protection when another role assigned to them, that of manager, was under threat; using their participant's words, the expert identity functions as an "anchor" [730, p. 79]. Expert identity may also be constructed through membership of a professional association, such as those that exist for cyber security and IT, e.g. [18]. Of particular relevance here is the idea that defining oneself as an expert, whether explicitly or implicitly,[51] may be a mechanism of achieving ontological security of the self.

Identity can be considered as a "nexus of relationships" [694, p. 167], with associated entities being "not only influential but also constitutive" [694, p. 160]. Benwell and Stokoe describe how certain theories of identity are based upon "the self [being] de-

[51] And possibly through perlocutionary effects.

fined primarily by virtue of its membership of, or identification with a particular group or groups" [129, p. 24]. Goffman discusses the use of different expressions to refer to those in the "in-group" versus the "out-group" [363, p. 160] and how these can maintain that difference between those groups. One example of this in an organisational context is the use of the distinct term "the business" to differentiate a non-IT out-group, as identified by scholars who have researched technology functions [273, p. 14]. Group membership also functions as a form of what Goffman refers to as "information control" [363, p. 141]; the group determines what information is presented to others. This activity, and the information itself, helps to cement the identity of that group as a group and "maintain[s] ... stability" [363, p. 108]. Groups feature "standards of conduct and appearance" [363, p. 81] that are expected to be maintained, and these serve as markers of identity [363, p. 81]. As well as affiliation *with* a particular group, identity work can also involve affiliation *away from* a group. An identity as *not*-X may be a particularly useful construction where X is seen as undesirable [401].[52]

An organisation may construct its identity based on its relationships to other organisations, including those with organisations that are, or are seen as, competitors. References to unrelated businesses may also feature in identity construction. Such construction may take place through public statements from the organisation (such as annual reports or press releases) as well as through internal dialogue between individuals within the organisation. Sociologists Stewart Clegg et al. describe how "it is in reference to others that organizations define their own identity position vis-a-vis their own putatively unique characteristics and those characteristics that they have in common with other firms in their industry" [219, p. 498]. Ybema et al., referring to earlier work by management researchers Susan Ainsworth and Cynthia Hardy [76], describe how "linguistic binary oppositions are often utilized in identity construction to set up a hierarchy and position the other not merely as different, but also as less acceptable" [793, p. 307], something observed by others in relation to organisational identity work, e.g. [311]. Organisational theorists Joseph Porac et al. describe how organisational "comparisons are embedded in belief systems" [608, p. 203], arguing that "rivalry is socially constructed" [608, p. 204]. Clegg et al. refer to these 'belief systems' as "allow[ing] them [i.e., organisations] to define boundaries and maintain their identities" [219, p. 498]. In addition, this identity work also supports economic goals, "enabl[ing] the market to be both created and exploited" [219, p. 510]. Therefore, the "nexus of relationships" [694, p. 167] that a given business exists within appears crucial to not just its identity but also its continued existence, and, by extension, its sense of ontological security.

[52] Although, as I discuss shortly, in order to be *not*-X, X has to exist.

2.3.5 Constructing identity

As established above, through identity work identities can be constructed for the self, for others, or both. In this section, I discuss the literature relating to some specific identity constructions from both an individual and organisational perspective. These are relevant to this thesis as these constructions index, and are indexed by, multiple aspects of cyber-security practice as I explain below.

Heroic identity

Individuals may perform identity work that casts themselves in a heroic light through an "aspirational identity narrative" [734, p. 371], and such an identity can be closely connected with an individual's self-perception of their status [734, pp. 363-365]. The close associations of cyber security with warfare may encourage, or lead to, such an aspirational identity construct for cyber-security professionals, who then cast themselves in a heroic role. The construction of a heroic identity can include triumphing over enemies, although victory itself is not necessary as "the process of becoming is itself valued" [734, p. 371]. This concept has implicit moral dimensions, as well as masculine aspects, as I explore shortly. As described above, metaphors of conflict, such as 'adversaries', 'arms race', 'attack' and 'defend' are common within cyber-security discourse, whether academic or mass media, and cyber-security professionals use phrases such as 'red teaming' and 'blue teaming' to describe simulations of attack and defence, e.g. [550], terms which originate from military practice [25]. Such terminology is also highly masculine, and is common within both IT, e.g. [230], and business, e.g. [722], a point I return to shortly. This appropriation of language is a form of identity work [124, p. 55]. The borrowing of language from the fields of IR and warfare provides cyber security, as a domain, with an identity as a highly important, dangerous (and, therefore, fearful) concern. Its identity becomes one of existential threat and those who work in the domain are, as a result, assigned an associated identity as those who are subjected to, and/or dealing with, that threat. The repetition of these terms within the cyber-security industry and within businesses is part of a process whereby this identity is continually reinforced and reconstituted.

Masculinity. Heroism is a traditionally masculine concept and while being a cyber-security professional is arguably not as traditionally 'masculine' as being a rugby player or a paratrooper, occupations that have been studied from an identity perspective by other researchers e.g. [177, 734], it is a highly male-dominated industry [594].[53]

[53] It is also notable that IR has a strong propensity towards 'masculine' concepts of protectionism, antagonism and rivalry [545, p. 96], and gender bias is common in IR literature, as highlighted by a

Cyber-security professionals, who are predominantly male, may develop or maintain discourse that casts cyber-security as a military concern, encouraging narratives of defence against enemies, in order to construct this heroic identity and "secure their status" [177, p. 1328].[54] It may even be (psychologically) necessary for "male aspirants ... to tell a heroic coming-of-age tale that would make them men" [177, p. 1328].

Discourse that utilises tropes of enemy threat associated with cyber security may form "a system of constraints that simultaneously discipline and enable the discursive identity strategies available to members" [734, p. 372] which could additionally deter anyone, regardless of gender identity, for whom a military identity is not aspirational. Such discourse may, therefore, be implicated in both the overall skills gap in cyber security [195, 594] and the lack of female representation in the industry [594]. An individual's identity work may also affect the identity of others, as they adopt, or adapt, what they have heard or otherwise experienced [253, 353]. References to cyber criminals and nation-state attackers, for example, whether "real or imagined" [353, p. 71], may function as "social ghosts" [354] that result in the identities of organisational leaders being developed as both 'the attacked' but possibly also as 'commanders',[55] responsible for ensuring that appropriate defensive measures are taken.

Villains. Negative identities can be constructed for others through the use of "demonizing narratives" [686, p. 1626] that result in their "evilification" [145, p. 486]. Such narratives also enable related identities to be developed, including "the hero who defeats them, the victim who suffers under them, or the prophet who warns others about them" [686, p. 1626], or even the "missionary, saving the soul of the other by converting them from their wicked ways" [686, p. 1636]. Demons may be sought out in order to benefit from the "warm glow to be had in knowing that someone can be looked down on" [686, pp. 1637-1638] and a role that is positioned as a defender against those demons may offer "identity rewards" [174, p. 321]. A demon may be necessary for the identity of the defender [686], motivating continued discourse relating to the demon's existence. It may even stimulate their invention, particularly where there is a possibility of "running out of demons" [37]. Where an identity is dependent on being *not-X*, the eradication of X is, possibly despite discourse to the contrary, undesirable [401]. This

number of researchers [308, 386]. Such bias presents limitations that should be recognised; equally, however, they provide useful insights into the motivations behind key concepts in this field. These limitations and the insights that can be derived from them will be reflected on throughout this thesis.

[54] Brown and Coupland specifically question whether "the identity narrativizations of other elite professionals (e.g. surgeons, lawyers, management consultants), or indeed organizational workers generally, feature the construal of anxiety-provoking threats and appropriation strategies" [177, p. 1331].

[55] Another highly masculine identity.

includes both X and *not*-X imbuing the other party with moral characteristics that each perceives to strengthen their positions [401]. Indeed, the X versus *not*-X relationship, and associated discourse, may be the crucial factor in identity construction [793]. Demonization also facilitates decisions to use exceptional and possibly draconian means in order to deal with the threats that the demons pose [145, 655].

Heroic and villainous identities also connote an aspect of morality, which is something I now discuss in more detail.

Moral identities

Identity work can include the construction of identities that are deemed to be 'moral' [388]. The concept of moral identities, while debated [299], has been established, and endures, e.g. [630].[56] Those who are "known for exemplary moral commitments" are considered as "moral exemplars" [388, p. 497]. Such individuals "may be experts in morality as others are experts at chess or piano" [388, p. 498].

Philosopher Joseph Heath summarises a criminological perspective on morality, describing it as both situational and driven by the views of others [397]. Referring to philosopher Thomas Nagel [564], management scholars Marc Cohen and Dean Peterson suggest that determining a moral course of action is not a binary decision, that morality is a continuum [220] and that there may exist "moral blind alley[s]" [564, p. 143]. This, along with their description of business ethics as "involving competing ethical considerations" [220, p. 86],[57] suggests that determining a course of action that is, or that appears, moral requires a level of interpretation.

As established above, entities with whom an organisation or an individual has a relationship can affect identity by association. If those entities have a moral dimension, then these moral aspects can also be transferred. Examples of such morally-implicated entities include law enforcement, national intelligence services and governments, as well as regulators, trade organisations and charities. It is not uncommon for law enforcement and intelligence services to be referenced by organisations experiencing cyber-security incidents, e.g. [50], and their invocation may serve a purpose of assuring stakeholders that the organisation is 'doing the right thing', but also indexing a broader narrative that the organisation is 'a victim of crime', further implying morality through the good versus bad, right versus wrong, dimension. The victim of crime position may even be referenced explicitly, e.g. [32]. Cyber-security providers also make reference to morally implicated entities, such as a number of organisations founded by veterans of national

[56] Detailing the (primarily philosophical) debate is outside the scope of this thesis; psychologist Julia Driver provides a useful explanation and refutation of the arguments against the concept [299].

[57] Arguing against Heath's focus on an economic and market-driven basis, e.g. [398].

intelligence agencies, e.g. [59, 255].[58] Additionally, the repetition of terms such as 'arms race' and 'nation state hackers' within the cyber-security industry, e.g. [486] and within businesses, can be considered part of a process whereby this moral identity is continually reinforced and reconstituted. As noted earlier, the use of emotional and value-laden language can be highly effective in identity construction [253].

I now turn to how aspects of risk are indexed in identity construction.

Risk and identity

Sociologist Gabe Mythen discusses how "risk-taking behaviour" [563, pp. 145-6] supports identity in some social groups.[59] He refers to sociologists Deborah Lupton and John Tulloch who suggest that "voluntary risk taking is often pursued . . . [to achieve] self-actualisation and a sense of personal agency" [514].[60] Psychologist Hélène Joffe also refers to the "'not me' phenomenon" [447, p. 32], which is motivated by "maintaining a sense of control" [447, p. 32].

Organisational behaviourist Sally Maitlis et al. cite examples where "an event or issue . . . become[s] a powerful sensemaking trigger" that affects "the organization's identity and its future" [523, p. 225]. There are examples of organisations changing (or attempting to change) their identity as a result of negative cyber-security events. For example, in the wake of a significant data breach, Facebook attempted to assert its focus on privacy [787]. Other organisations such as Apple have attempted to capitalise on security issues affecting competitors by reaffirming their own identity as a privacy focused organisation [56], as a contrast to those competitors, a clear *not-X* behaviour, as described above. Cyber-security risk may constitute what Maitlis et al. refer to as "new, dis-crepant [*sic*] data" [523, p. 226] that threatens identity. As they describe it, such data will often be "normaliz[ed] . . . to fit [an] existing story and self-conception" [523, p. 226]. A *not-X* construct may be an attempt to create "a sense of immunity to the crisis" [447, p. 32], that crisis being the permanent emergency of cyber-security risk.

Joffe describes how risk is used to distinguish between groups, and how this reinforces group identity. This includes the use of scapegoating [447] from the perspective of restoring order to a community and reinforcing group identity [447]. Scapegoating can be seen as a tactic that an organisation (as a group) may employ in response to a cyber-security crisis in order to reinforce, or recover, its identity, e.g. [11]. However,

[58] This example also illustrates a subjective aspect to morality, as national intelligence services will not be universally considered as moral.

[59] Particularly among youth.

[60] Giddens makes a similar link [359]. Elsewhere, sociologist Ian Culpitt has criticised Beck for "ignor[ing]" [252, p. 99] this aspect of risk.

such scapegoating may not be in the traditional sense [295] where those scapegoated are not responsible for the crisis. Scapegoats, as described by Joffe, may indeed be responsible, whether inadvertently or otherwise [447]. Scapegoating, or the threat of it, can also be viewed as a means of controlling another's identity, creating a regulatory effect. This is a topic I now explore in more detail.

2.3.6 Regulative effects of identity

As well as identity being a means by which an individual attempts to control how others interact with them [363, p. 15], identities can similarly be utilised by those in powerful positions. Benwell and Stokoe refer to identity as a "necessary regulatory fiction" [129, p. 29], and it is debatable as to whom that 'necessity' pertains, whether to the individual, wider society, other actors such as hegemons, or a combination thereof. Referring to philosopher Antonio Gramsci [371], they include both "repressive institutions" and "culture industries" as centres of power [129, p. 31] and describe how "[i]dentity or identification thus becomes a colonising force, shaping and directing the individual" [129, p. 31]. Management scholars Mats Alvesson and Hugh Willmott discuss the use of identity regulation as a form of "organizational control" [86, p. 619] which Beech refers to as a "normative control" [124, p. 52]. Here, Beech builds on earlier work by organisational communication researcher Stanley Deetz [277], and suggests that it may be "less obtrusive and more effective" to manage "the 'insides' of people" [124, p. 52]. Similarly, Alvesson and Willmott, argue that

> "self-identity, as a repertoire of structured narrations, is sustained through identity work in which regulation is accomplished by selectively, but not necessarily reflectively, adopting practices and discourses that are more or less intentionally targeted at the 'insides' of employees, including managers" [86, p. 627].

Caza et al. summarise how "[o]rganizations create and perpetuate dominant narratives to influence how individuals define themselves, with hopes that such identities will constrain behaviors in organizationally beneficial ways" [203, p. 897]. Therefore, organisational identity work can regulate an employee's identity, constraining their own identity work by limiting the identities that are available to them, or by presenting, or assigning, specific identities. This regulation may be deliberate or unintentional.

Identity regulation can also occur as a result of societal or professional norms. This can include what roles are (normatively) considered to be 'acceptable' for different gender identities [294], as well as which professions, and by extension which philosophies, are given the most credence [294]. Beech describes how those with power have "the ability to mobilize discursive resources in order to marshal discourses or counter-discourses, and the ability to get others to acknowledge or take seriously a position that is being proposed" [124, p. 69]. As an example of this, governmental discourse[61] can be viewed as influential in the construction of cyber-security identities, both at organisational and at individual levels.

Michel Anteby, a scholar of organisational behaviour and sociology, identified a nuanced form of organisational control based on apparent freedoms rather than repression. In his study, "leniency" [89, p. 202] served to support the workers' "desired identities" [89, p. 215], which was ultimately to the benefit of the organisation.[62] He refers to this as "identity incentives control" [89, p. 215] which he defines "as the selective positive arousal of identity feelings that induce action or motivate effort" [89, p. 213]. He suggests that such controls may take a variety of forms, including accepting less desirable workloads if also given the opportunity to work on those that are desirable, which are supportive of that individual's identity needs [89]. In summary, Anteby believes that "the role of organizations in shaping members' identities cannot be assumed to be unilaterally detrimental or beneficial to members – control and desire coexist" [89, p. 215].

2.3.7 Summarising security and identity

The literature shows that cyber security must be understood in the context of broader concepts of security, which includes multiple political and societal considerations. Cyber-security practice within organisations does not exist in isolation from these factors, and, therefore, they are directly relevant to understanding the purpose of the CISO, whether they are implicitly or explicitly visible. Security and cyber security are both discursively constituted, with various features of discourse, such as metaphor and narrative, being significant to how they are experienced and perceived.

As security is, at least in part, associated with survival, concepts of identity are germane to a deeper understanding of security-related practices. Threats to identity, to the security of self, are motivators of identity work i.e. the actions taken by an individual or organisation to construct and maintain an identity. Identity work may be performed discursively, through impression management or through specific actions. Each of these tactics may index broader concepts and narratives, as with security. This includes aspects of morality, which is another area of commonality between talk

[61] Such as that produced by the UK government's National Cyber Security Centre, e.g. [502], as well as individual UK government departments, e.g. [19].

[62] Specifically, the organisation concerned was being lenient with regard to employees working on personal projects in work time, using company resources, which was, strictly speaking, against the organisation's rules.

about identity and talk about security where each employ concepts of virtue. The construction of one identity can have an effect on others, which includes constraining the identities that are available to those others as a result, or through normalising certain characteristics.

Although security and identity are closely related, the literature does not explore the links between cyber-security practice and identity, whether organisational or individual. In order to understand the purpose of the CISO it is important to understand the role that they may play in organisational identity, whether in response to threats to that identity, as a mechanism of achieving legitimacy, or otherwise. However, there is another important concept that is applicable to understanding the latter, which is that of risk and risk management. The analysis of the data identified multiple references to concepts of risk and, therefore, it is to this subject that I now turn.

2.4 Concepts of risk

In this final section of the chapter, I introduce core concepts of risk and how these relate to cyber-security practice. Risk, and risk management, is embedded within corporate business, which makes it particularly relevant to any study of commercial organisations. Further, as presented above, responses to risk are closely associated with identity, and risks can be deployed for political motives. Therefore, understanding core concepts of risk is an important precursor to understanding cyber-security practice, particularly as cyber security is considered to be a fearful category of risk by organisations and governments, as was established in Section 2.2.

2.4.1 Risk, uncertainty and ambiguity

I begin by briefly distinguishing between some key terms. Similar to how others have characterised security [618], risk is described by Mythen as having a "polysemic quality" [563, p. 15], and the multiplicity of meanings [168] of the term is apparent from much of the literature. Lupton and Tulloch point out the predominantly "negative" connotations of the term, proposing that "[t]he emphasis in contemporary Western societies on the avoidance of risk" results from a drive for self-control and "avoid[ance] . . . of fate" [514, p. 113], with Giddens also highlighting these negative associations [360]. However, Giddens does highlight the potential for risk to be viewed "in a positive light" as "[s]uccessful risk-takers, whether in exploration, in business or in mountaineering, are widely admired" [360, pp. 3-4].[63] Beck also describes how "[r]isks . . . are in part

[63] Although this may be very much related to the gender of the risk-taker [769], as I discuss further below.

positive, in part negative . . . consequences of human actions and interventions" [123, p. 73]. Criminologist Sandra Walklate, summarising prior work, states that "it is misleading to address the concept of risk as though it only refers to risk **avoidance**" [769, p. 39] (emphasis in original). Another criminologist, Pat O'Malley, describes how "risk is never technically neutral" and that it "may take a wide diversity of forms that reflect the purposes to which it is put and the assumptions on which it is based" [584, p. 453].

Psychologist Paul Slovic states that "human beings have invented the concept *risk* to help them understand and cope with the dangers and uncertainties of life" [695, p. 733] (italics in original) and 'uncertainty' has been theorised as an originating concept of risk [512, pp. 9-10].[64] Avoidance of uncertainty is a recurring theme within business and organisational literature, e.g. [393, 548, 549] and economics, e.g. [281], as well as within sociology, e.g. [123, 358], psychology, e.g. [168, 695] and philosophy, e.g. [508, p. 232]. These bodies of work suggest that uncertainty avoidance is a powerful motivator for human action, both individually and within groups, such as businesses, as I describe in more detail below. Distinctions in the literature are made between risk and ambiguity, with the differentiator being the level of knowledge held, risk requiring knowledge of the likelihood of the event occurring, whereas ambiguity relates to the unforeseeable aspect of the event.[65] Beck describes the concept of risk itself as "the response to uncertainty" [123, p. 5] and Mythen agrees with a distinction, but makes a clear connection between the two [563, p. 14]. Beck distinguishes between actual loss and the "anticipation" of loss, the latter being how he defines risk [123, pp. 9, 135]. Mythen describes how "understandings of risk differ over time and place" [563, p. 14], also alluding to cultural differences in interpretation of risk, which are themes consistent throughout the literature.

Beck introduces a concept of "manufactured uncertainties" [122, p. 50] to refer to risks that result from the actions and decisions of human beings and institutions, as opposed to risks that emerge from nature. Such risks are "socially rather than naturally produced" [563, p. 16] and have the "shared characteristics of . . . dread, scientific uncertainty, unfamiliarity, voluntariness and irreversibility" [563, p. 108], further "possess[ing] . . . temporal and spatial mobility" [563, p. 19]. Based on these characteristics, I propose that cyber-security risks can be considered as being "manufactured". Mythen theorises that "manufactured risks may be accepted as the quid pro quo for tangible benefits and social progress" [563, p. 145], a point similar to that made by Baudrillard who, as mentioned above, positions such an exchange as a Faustian pact [116, p. 173]. Extending this to cyber security, perhaps society must

[64] In relation to maritime discovery, although this is debated [26].

[65] This distinction is made across disciplines, e.g. [141, 196].

accept that cyber-security breaches will happen as the price for technological progress and convenience, which could manifest in a blasé attitude to cyber-security risk.

Uncertainty is a consistent thread that runs through themes of security and identity, as established earlier in this Chapter, with each of these topics being relevant to commercial businesses. Therefore, it is pertinent to now explore uncertainty in business in more detail.

Uncertainty in business

Uncertainty is distinct from risk, as most famously established by economist Frank Knight who distinguished between the two on the basis of the latter's measurability [478]. As management scholars Sharon Alvarez et al. summarise, "[u]ncertainty, for Knight, existed when decision makers knew neither the possible outcomes nor their probability of occurring when a decision was made" [82, p. 169]. However, it is important to recognise that "real-world phenomena are often mixed cases of risk and uncertainty or, more precisely, uncertainty exists along some sort of continuum" [633, p. 985], similar to how governance was described in Section 2.2.2.[66]

Different perspectives exist on exactly how much influence uncertainty has, and attitudes towards it are also culturally variable [393]. Organisational theorist Mary Jo Hatch describes modernist theories of uncertainty avoidance conflicting with postmodern thinking that sees uncertainty as something positive, something to be "sought out as invigorating" [393, p. 94]. Others have critiqued the abstraction of external factors that could be considered as uncertainty as providing an 'excuse' for organisations to exploit both natural and human resources [677]. Mintzberg points out that different researchers have categorised the same variables in different ways when referring to uncertainty and complexity and, in some cases, conflated the two [549, pp. 273-4]. He is clear to distinguish between stability and complexity as two distinct dimensions. The implication drawn from the literature is that uncertainty is a symptom; issues with stability of an environment may result in uncertainty, as would issues with complexity. Equally, other environmental issues, such as organisational politics, as well as external factors such as regulation, national and international politics, could generate uncertainty.

In their seminal work, organisational psychologists Daniel Katz and Robert Kahn describe how "[i]n most formal organizations there arise ... structures which are specifically concerned with sensing relevant changes in the outside world and translating the

[66] And, indeed, how morality was described in Section 2.3.5. A requirement for interpretation and indeed judgement with regard to these dimensions is implied as a result, a notion I develop further throughout this thesis.

meaning of those changes for the organization", referring to these functions as "adaptive" [466, p. 42]. Organisational scholars Raymond Miles and Charles Snow identify that environmental uncertainty affects the importance that organisations place on different internal departments, with "high environmental uncertainty ... [resulting in] greater emphasis on externally oriented functions" [548, p. 213]. This changes the power dynamic within the organisation such that those externally-focused teams "tend to wield more power" [548, p. 213]. Summarising an earlier work by other organisational scholars James March and Herbert Simon [529], they describe how "organizational structure and process evolve so as to prevent uncertainty from overwhelming ... [human beings'] limited capacities" and link this to an inherent human limitation in making "completely rational decisions" [548, p. 8]. Hatch highlights uncertainty as being something that resides in the "individuals ... [who] make organizational decisions" [393, p. 90] rather than in the organisation's environment.[67]

Others have also suggested the role that uncertainty plays in organisational design, e.g. [265, 393]. The creation of individual units has been described as a reaction to complexity and/or uncertainty [393, 548, 549], with multiple reasons suggested that include the establishment of "formal authority ... [and] hierarchy", "sharing of resources" and "mutual adjustment" [549, pp. 104-6], as well as formalisation of job responsibilities [549] and creation of boundaries [393]. Other reasons include consistency, particularly where the unit grouping is based around a specialism, and for ease of management [393]. One of the pioneers of organisational research, Joan Woodward, alluded to both internal political motives and external factors as driving forces behind the growth of "specialist departments" [790, p. 21]. A cyber-security department can be considered as one of these structures, with the recognition, translation and application of external factors being highlighted by other researchers as important factors in organisational cyber security, e.g. [425]. A cyber-security department is also a grouping of expertise and there are important aspects of identity associated with such organisational subunits [98], as presented in Section 2.3.4 and which I will discuss in more detail in Chapter 4. Friction can occur between departments, particularly "when interdependent subunits have inconsistent goals, have differing perceptions on how to reach a commonly held goal, or must share scarce resources" [742, p. 207], and relationships can become so "[d]ysfunctional" that one department may deliberately undermine another [273, p. 24]. The importance of "political strength" held by internal departments has been highlighted, and such strength "depends on ... [the department's] *power* over other areas" [742, p. 207] (italics in original). Understanding

[67] Mitzen argues that the management of uncertainty is fundamental to an individual's ability to "be themselves and to act", and that their level of comfort with the management of this uncertainty is "an internal, subjective property" [551, p. 346]. I return to this in more detail in Chapter 4.

organisational politics becomes more important “as the change rate of technical and economic environments increases” [742, p. 214], such as is the case in modern life [358] and modern business [301].

2.4.2 Risks to viability

Businesses are concerned with their own sustainability and the perpetuation of their existence [126, 172].[68] Classical organisational scholarship such as that produced by management researchers Stafford Beer [126] and Paul Lawrence and Jay Lorsch [499], among others, highlighted behaviours of organisations concerning their continued viability. Beer applied both systems theory and a biological view to enterprises, building on biologist Humberto Maturana [536], by proposing that they exist to perpetuate themselves, that they are “autopoietic” [126, p. 405], that an enterprise, as a viable system, is in “*the business of preserving its own organization*” [126, p. 405] (italics in original). Taking Beer’s application of autopoiesis to business, if the purpose of an organisation is to self-perpetuate, which can be positioned as ‘the continuance of being’, then it should be concerned with threats to survival. More recently, autopoiesis as applied to organisations has been extended [172, 755] but also criticised [301]. Whether organisations are definitively autopoietic, that is they only exist for their own self-perpetuation, or whether Beer’s Viable System Model holds,[69] viability can be reasonably argued as a concern of most, if not all, organisations, while acknowledging that different businesses function in different ways and for different reasons. Viability is defined variously as “feasibility ... ability to continue ... financially sustainable ... practicable, esp. economically or financially” [35] and, logically, the fulfilment of these can be considered desirable by all commercially-oriented businesses.[70] Organisations that have a UK stockmarket listing are required to comply with certain reporting standards [12, §Listing Rules] [243], including the need to make a statement of viability in their annual report.[71]

[68] These concerns could be argued as ontological, as introduced in Section 2.3.3.

[69] Which continues to be debated and tested from a variety of perspectives, e.g. [666, 729].

[70] Beer’s definition of a viable system includes a qualifier of “[the capability of] independent existence” [127, p. 7]. From a business perspective, it is arguable whether this is mandatory. Considering a loss-making business that requires regular injections of additional capital (as Amazon.com, Inc. was for many years [39]) as truly existing independently may be a stretch, and such a business may not be considered viable based on the definitions above. However, with hindsight, it is difficult to consider Amazon.com as a non-viable business given its subsequent performance, growth and dominance. Conversely, in isolation, any business that suffers increasing losses year-on-year could be argued as non-viable from an intuitive standpoint at least, supporting the use of ‘independent existence’ as a valid test of viability.

[71] This requirement was introduced in 2014. Note that the UK Corporate Governance Code is “applicable to all companies with a premium listing [on the London Stock Exchange], whether incorporated in the UK or elsewhere” [243, p. 3] and while not technically legislative in its own right, compliance

Organisations face a number of challenges to their viability, and concepts of survival continue to arise in management scholarship, e.g. [410]. Cyber security has been positioned as a survival-level concern for businesses [231, 369], with technological advancement, including the cyber-security implications associated with this, being similarly situated [428]. Technology itself has been argued as a necessity for a business's survival [754]. Conceiving of cyber security as something fearful, that is a threat to viability and continued existence, is an important foundational context with which to understand the actions taken by businesses to mitigate or resolve those threats. Cyber security is similarly positioned as a threat to the survival of states, e.g. [504], or, at least, to their dominance [637].

A short note on management theory. Management theory from the 1960s, 1970s and 1980s continues to be influential, e.g. [146] and while some modern scholars view it as outdated [614], perhaps increasingly so [410], others view it as of continuing relevance, and even unfairly maligned [301]. However, it is important to acknowledge that the dominant work in the discipline has been authored from a Western perspective, to the detriment of organisations in the Global South [108]. Additionally, it is predominantly based on "an economistic paradigm" that does not address more "humanistic" concerns [604, p. 40]. Accepting these temporal, cultural and paradigmatic limitations, perspectives from established management theory provide an important and useful lens with which to analyse modern businesses, particularly those that are Western-based, not least because they predominate in most MBA programmes [356], including those outside of the West [503].

2.4.3 Experiencing risk

In this section, I explore how risk is experienced, according to existing scholarship, and bring this into conversation with cyber security. This includes emotional factors as well as aspects of duty that are associated with risk perception. I also discuss differences in group perception of risk.

Information systems scholars Hyeun-Suk Rhee et al.[72] describe how "[p]erceptions, whether accurate and rational or not, are themselves important factors of managing the realities of risk" [628, p. 391]. Beck believes that "risk . . . [and] perceptions of risk" are equivalent [123, p. 151], a position also adopted elsewhere, e.g. [650]. Therefore, any objective reality to a cyber-security threat may be irrelevant to how it is experienced, and, by extension, how it is responded to. The *perception* that an existential cyber-

with it is a requirement of the Listing Rules defined by the Financial Conduct Authority [12, 23].

[72] Summarising prior work from psychologists Jonathan Baron et al. [113].

security threat exists may be all that is required to motivate a response to that threat by a business. Individuals (and, by extension, businesses, as these are run by individuals) respond to risks differently depending on their own internal "risk thermostat" [68, p. 15], but one component of that thermostat is "perceived danger" [68, p. 15].

Mythen argues that because "local experiences are cultivated and situated, we must be aware that the meaning of risk will always be fixed in the eye of the beholder" [563, p. 182]. An important aspect with regard to exactly what that 'eye' is 'beholding' is how risk is presented, or what Beck refers to as "staging" of risk. He defines this as a means to "[make the] future catastrophe become present – often with the goal of averting it by influencing present decisions" [123, p. 10]. Beck describes how "*the staged anticipation of disasters and catastrophes obliges us to take preventive action*" [123, p. 11] (italics in original). The temporal aspects of risk implied by Beck have been highlighted by others, including Giddens who states that "[t]he idea of risk is bound up with the aspiration to control and particularly with the idea of controlling the future" [360, p. 3]. Sociologist Iain Wilkinson agrees, describing "ignorance of the future" as being fundamental to the concept of risk [785, p. 2], while psychologist Lola Lopes states that "[u]ncertainty is embedded in time" [510, p. 289].[73] As risk is experienced as a disturbing future event, mechanisms to predict, control or limit the likelihood or impact of that event are sought, and yet those same mechanisms may be the only source of information regarding the event in question.

Governmental and (particularly) media discourse regarding cyber-security threats can also be viewed as risk staging. Beck discusses the role that mass media plays in risk staging, particularly with regard to its role in perpetuating messages relating to risk that support political motives [123, pp. 98-100]. Mythen criticises Beck's view of the media as ignoring important factors such as cultural aspects, and "undervalue[s] the active role of the audience in decoding media representations", concluding that Beck "fails to delve beneath the surface layer of representation" [563, pp. 92-3]. Summarising prior work from sociologist Alison Anderson [88], he points out that "the most likely beneficiaries [of media-reported risk information] will be those who already possess background knowledge of the subject in question" [563, p. 92] and suggests that "[r]esource-related factors such as educational access, scientific knowledge and technical familiarity influence the meanings made of risk information" [563, p. 92]. While technical familiarity with cyber security may be low among non-specialists, technical familiarity with the technology *at risk* of cyber-security threats may be higher, at least with regard to consumer-facing technology such as mobile computing devices. If true, this would suggest a possible distinction between knowledge about the object at risk

[73] This sense of 'controlling the future' is developed further in Chapter 4.

and the knowledge of the mechanisms of threat to that object. As well as staging the existence and business impacts of those risks, e.g. [45, 647, 720], media reports also position cyber security as fearful, e.g. [451, 709], inevitable, e.g. [49], and difficult to understand, e.g. [52].[74]

Emotional aspects of risk

Risk is experienced emotionally, and emotional factors in risk perception are well established, although may have historically been overlooked in favour of cognitive aspects [447, p. 12].[75] Slovic suggests a distinction between risk events that are "dreaded" versus those that are "not dreaded" and how that difference affects risk perception [695, p. 734]. Uncertainty has been identified as having a direct physiological effect [779], suggesting that emotional responses to uncertainty are rooted in biology and perhaps also that while concepts of risk may be socially constructed [563, p. 97], fear of uncertainty may not be. However, Adolphs describes how "[e]motion categories such as fear are … seen as highly constructed, rather than as biological primitives" [72, pp. R88-9]. Summarising psychological theories, he describes

> "[the human] experience of fear … [as] a highly cognitive synthesis … [which] incorporates … knowledge of the state of one's body and of one's actions, but also of the context-dependent situation, knowledge stored in memory, and much explicit information stored in language and acquired in a particular culture" [72].[76]

These latter points are relevant to the use of emotionally laden terms in relation to cyber security. Beck notes that "[f]ear determines the attitude towards life" [123, p. 8], aligning with much theory in IR, and the perceived need for security, as discussed above. While risk and fear are not equivalent, if fear is involved in responses to risk, then the complex and constructed nature of the human experience regarding fear is important to consider, particularly with regard to coping strategies. As discussed above, emotions, including those relating to fear, can inhibit cognition [312].

Maitlis et al. highlight the importance of emotion with regard to "sensemaking in organizations" [523, p. 222]. They summarise sensemaking itself as "the process

[74] As well as militaristic and moralistic, as discussed earlier.

[75] 'Cognitive' is used here, and elsewhere, to imply conscious reasoning. However, the two are not necessarily equivalent, with cognition also referring to the unconscious processing of emotion, and "thought, feeling, and action" may all be connected [774, p. 186]. How, and indeed if, these are connected is a debated point in the field of cognitive science, e.g. [332], an exploration of which is outside the scope of this thesis.

[76] Other scholars in the social sciences have also introduced biological perspectives on risk responses, e.g. [447, pp. 108-112].

through which individuals and groups attempt to explain novel, unexpected, or confusing events" [523, p. 222]. Separately, social psychologist Bernard Weiner describes how "emotions . . . provide the motor and direction for behavior" [774, p. 186].

Militaristic language[77] in particular may, explicitly or implicitly,[78] generate an emotional response, particularly fear or distress. Political scientists James Druckman and Rose McDermott found that "distress encourages a more cautious approach [to risk]" [300, p. 317], as well as, slightly counter-intuitively, that "[a]nger encourages greater risk-seeking" [300, p. 317]. Druckman and McDermott also found that "emotions influence both individuals' tendencies to take risks and the impact of risky choices (e.g. emotions amplify or depress a [risk] frame's impact)" [300, p. 297], highlighting the potential for manipulation.

Mythen, disagreeing with much of what he perceives as Beck's assumption that individuals within society are "reflexive and risk-observant", states that "[l]ay actors will tend to prioritise their cognitive engagements with risk as a way of fending off feelings of engulfment" [563, p. 111]. Within a business, employees may feel 'engulfed' by the cyber-security risks that they are exposed to, as has been identified by other researchers, e.g. [385]. Equally, employees may experience a similar feeling when confronted with their cyber-security responsibilities. Using Slovic's terms [695, p. 734], from a cyber-security perspective, the same risk may be viewed by an employee as "dreaded" in one context (for example, a ransomware infection affecting their home computer and personal files) and "not-dreaded" in another (a ransomware infection affecting their work computer and work files). Extending management scholar Yuval Rottenstreich and social psychologist Christopher Hsee, the former would be "affect-rich", easier to imagine and, therefore, easier to dread, as opposed to the latter, which would be "affect-poor" [644, p. 188] and "not-dreaded" [695, p. 734]. Affect, therefore, may weight employee decisions regarding risk, and is a topic I now explore in more detail.

Affect

The impact of affect on risk perception and associated decision making has been discussed by a number of scholars e.g. [331, 644, 696], including in relation to cyber-security risk. Sociologists Dilshani Sarathchandra et al. suggest that cyber-security events that impact upon businesses "are not as easily lent to heart-tugging narratives" as those that "feature innocent victims to whom most people can relate" [656, p. 72]. This implies that employees may not relate to business-impacting security events, even

[77] And other metaphors [155].

[78] E.g. 'cyber attack' versus 'red team'.

when such events impact their own employers' business, as such impacts may not be affective enough. Baron et al. suggest that "even though worry is an unpleasant emotion, it may be important in moving people to protect themselves against harm, both individually and collectively" [113, p. 426]. This may support the use of fear appeals in cyber-security practice, an approach which is common, although is of questionable efficacy [103, 449, 626]. However, as the same authors also describe, referring to an earlier single-author study by Baron

> "although worry may motivate protective action, it may also be somewhat autonomous from beliefs. People may worry too much about risks they know to be minor and too little about risks they know to be serious. This discrepancy may weaken the effectiveness of attempts to inform people about the relative probability of risks" [113, p. 426].

This study from Baron suggests that "both normative beliefs and anticipated emotions affect decisions" [112, p. 320]. This can be viewed in the light of Adolphs' description, highlighted in Section 2.3.1, of the contemplation of risk motivating a biological response that influences decision making. Where an "anticipated emotion" regarding cyber security is one that results in negative affect, rather than motivating a change in behaviour, it could lead to a disengagement from the subject. This can have broader impacts than just individual disengagement, as negative affect can have impacts on wider group decision making [315]. Equally, Sarathchandra et al. suggest that "misplaced fear leads to a number of problems, including misdirected resources, poor policy-making, and poor decision-making" [656, p. 72]. Therefore, the use of fear appeals in cyber-security messaging may result in unintended effects from a risk management perspective.[79]

I now turn to a different aspect of risk experience, which is that of duty and expectation.

Recreancy

Sociologist William Freudenberg applies the concept of recreancy[80] to risk perception. He argues against a sole focus on "individual [risk] perceivers" [340, p. 909] and encourages "broaden[ing] the focus further – asking not just about the individual perceivers, nor about the risks they perceive, but also about the larger institutional context within

[79] Not least that happy people may be more risk-averse [380].

[80] "Unfaithful to duty or a person" [24]. Freudenberg chooses this (relatively archaic) word "to provide an affectively neutral reference to behaviors of persons and/or of institutions that hold positions of trust, agency, responsibility, or fiduciary or other forms of broadly expected obligations to the collectivity, but that behave in a manner that fails to fulfill the obligations or merit the trust" [340, pp. 916-7].

which the risks are managed" [340, p. 910]. He questions whether individuals within an organisation are in fact aware of their duties with regard to risk, and highlights how "the complex possibilities of technology and the division of labor make it entirely possible for social activities to lead to disastrous outcomes even when no identifiable human villain can be found" [340, p. 917]. Such disastrous outcomes are certainly associated with cyber security, e.g. [520]. The perspective of duty with regard to cyber security is also one taken by industrial standards bodies, e.g. [297], through legislation, e.g. [13, 46],[81] and by regulators, e.g. [2].[82]

Beck's theses on the distribution of risk [122, 123] could also be viewed through the lens of recreancy: as risks are created and distributed, there may be an expectation of duty on the (possibly unwilling) recipients, of which they may not be aware. Within an organisation, similar dynamics may be at play. Risk resulting from a decision in one part of an organisation may have a 'knock-on' impact on another part, resulting in responsibilities which may be either implicit or explicit, and, if not fulfilled, expose the organisation to greater risk.

Linking to the three lines of defence concept discussed in Section 2.2, the findings from Zhivitskaya's research suggested a rejection by the first line of defence of the responsibilities assigned to them [796]. Such phenomena may be foundational in complacent behaviours and attitudes of employees with regard to risk, perceiving it as something that other teams are responsible for managing, and resulting in recreant behaviour. User complacency and apathy with regard to technology have been themes explored by a number of researchers, e.g. [710, 733], with some specifically identifying that employees believe someone else is responsible for cyber security [79, 455]. This sense of cyber security being "somebody else's problem" [67, p. 25][83] may be countered by clearer explanation of the three lines of defence model. Equally, however, it may be exacerbated by it, as those in the first line gain a false sense of security from the existence of two additional lines of defence. There is also an implicit sense of culpability associated with the model, in that it suggests that the first line may be ineffective in managing or containing risk and, therefore, additional oversight is required.

Duty also has moral implications. This includes "the moral duty to behave responsibly and not knowingly put other people at risk" [389, p. 1217]. Cyber-security professionals, such as CISOs, should, according to some, possess a sense of "civic duty" [272, p. 2], a concept that itself has moral associations, if not necessarily equivalence [422]. Recreancy is, as Freudenberg points out, particularly relevant to group perspectives, and I now turn to a discussion of group perception of risk.

[81] Which includes individual criminal liability.

[82] Which includes explicit board member accountability.

[83] Which may result in it being, and/or enable it to be, ignored [67, p. 26].

Group perception of risk

Perception of risk within groups has been indicated as differing from that of individuals. Mythen summarises prior work which suggested that "groups will tend to make riskier decisions than individuals . . . [with] the responsibility for risk . . . [being] shared by the collective and [therefore] the individual burden is lessened" [563, p. 101]. However, he criticises the lack of attention paid by empirical studies to "the role of collective networks and symbolic factors in the formulation of risk perceptions", with "[c]ognitively based studies" having excluded "social and political contexts" [563, p. 105], which are important to consider with regard to cyber security, as I discuss throughout this thesis. Douglas highlights the (implicit and explicit) boundaries to thought that exist within organisations and within society [294], which provide constraints on individual thought and influence group decisions. As Mythen states, "[p]eople do not share the same life experiences. Ergo, they cannot possibly share the same interpretations of risk" [563], and neither do they share the same risk thermostats [68, p. 23]. However, they may share cultural beliefs[84] that affect how they respond to risk [447]. Those beliefs could be societal, even arising from childhood [447], or from organisational indoctrination [585], and may differ by geography [319].[85] Organisational indoctrination in particular may give primacy to masculine behaviours [589]. Specifically with regard to cyber security, other researchers have identified that different zones of cultural belief can exist within an organisation [263].

This literature implies that a common understanding of cyber-security risk within a business may be unachievable. However, extending Douglas, a CISO may be able to define specific risk-related boundaries that influence both group and individual decisions, and, as identified by IT scholar Adéle Da Veiga and industrial psychologist Nico Martins, directly addressing different group beliefs relating to cyber security may be effective [263]. Extending Rottenstreich and Hsee's work on risk perception,[86] as introduced earlier, it is possible that cyber-security risk is not "imagery-rich" [644, p. 186] enough in regard to its impact on the entire organisation. Although cyber-security incidents may be seen as being potentially catastrophic, visualising what that catastrophe looks like may be more difficult than, for example, imagining other catastrophes such as natural disasters. Even when cyber-security incidents cause the failure of an organisation, that failure may be difficult to visualise, particularly if it takes place over a long period of time e.g. [57] and takes place mostly on paper, e.g. [612]. Although resultant job losses, e.g. [524], may be easier to visualise, they may still not be as im-

[84] And morals.

[85] Cultural beliefs may also shape individuals' emotional responses to risks [112].

[86] Which itself built on prior work [314].

mediately relatable to a cyber attack as, for example, a fire would be to the risk of smoking in an office. These difficulties in visualisation may influence how employees perceive the probability of a risk occurring. Further, it could be the case that perception of a cyber-security impact is easier from an individual perspective than it is from a group perspective, which then leads to an imbalance in probability assessment.

A different perspective on risk experiences within groups is provided by business historian Hartmut Berghoff's study on corruption. He summarises Douglas's observation that "rational self-interest is not sufficient to bind institutions together and that the act of taking risks on behalf of the collective up to the point of self-sacrifice plays a key role" [133, p. 428] [294], suggesting an aspect of social pressure within a group to take on risk, which may be either implicit or explicit, as well as an aspect of identity, such as 'we're all in this together'. From a cyber-security perspective, this could manifest through behaviours whereby employees encourage each other to circumvent controls or ignore policies in order to 'get the job done', which, in cases such as the one investigated by Berghoff, could lead to significant negative impacts on the organisation. Such behaviours have been identified by other researchers, e.g. [81]. However, such circumvention does not necessarily result in negative or undesirable outcomes, e.g. [481], may not entirely undermine security goals, e.g. [476], and may offer valuable empowerment for individuals [227].

Industrial engineer Zuzhen Ji et al. extend the psychological concept of the 'Dark Triad' to risky behaviour within organisations [445]. The "selfish" [445, p. 10] personality dimensions defined by this concept are well established within psychology [346, 593] and Ji et al. propose a role for these in worker judgements on risk, extending this into a concept of "perverse agency" [445, p. 1], whereby individuals willingly expose themselves to increased risk.[87] They suggest that this can be motivated, at least in part, by "over-alignment" [445, p. 18] with organisational goals, particularly where remuneration is involved. This can be exacerbated or encouraged by cultural factors within an organisation, making risky behaviour, and resultant harms, more prevalent.[88] While their study (on health and safety risk) is not specific to cyber security, it is analogous in many regards. Where organisational goals are insufficiently focused on aspects of cyber-security risk, or organisational rewards are driven by factors that benefit from cyber-security concerns being disregarded, particularly if cyber security is seen as a blocker, then perverse agency may be exhibited. However, crucially, this agency may be on behalf of the organisation rather than (or as well as) the individual. The organisation is then behaving in a manner that exposes itself to greater risk. Therefore, it

[87] Which also aligns with geographer John Adams' work [68].

[88] These are also associated with aspects of cognitive bias, a topic briefly discussed in Chapter 4.

is important that organisations are at least conscious of the risk of perverse agency, in that actions they take, and the cultures they maintain, may voluntarily introduce cyber-security risk.

In this section, I have described how risk is experienced emotionally, which builds on the fearful aspects of cyber security that were presented in Section 2.3.1. These emotional aspects influence decisions regarding risk. I have also introduced the concept of recreancy, which enables obligatory aspects of risk to be considered and builds on the moral associations of cyber security discussed in Section 2.3.5. Finally, I discussed factors associated with group perception of risk and how this is distinct from individual perception. I now explore how risk is responded to.

2.4.4 Responding to risk

A number of mechanisms by which individuals make decisions regarding risk have been identified, e.g. [131, 163, 208], although these are often contradicted by actual behaviour [163]. Some research on risk suggests that the outcome of a risk occurring is a more important decision factor than that of probability [163, 696], although Slovic et al.'s research [697] identified probabilities as being more important than outcomes. However, in their research, the minimum outcomes presented were zero, i.e., no loss. Maitlis et al., citing prior studies, describe how risk perception differs depending on the type of event, stating that "individuals generally pay more attention to negative than positive events" [523, p. 226]. This may support the positioning of cyber security as 'bad news', and the use of fear appeals, as briefly introduced earlier. Social psychologists Gordon Moskowitz and Peizhong Li suggest there is a difference in cognitive processing of goals that require "nothing happening" [558, p. 115], as in the case of avoiding a cyber-security breach, with "proactive strategies [to prevent risks occurring] . . . [being] difficult for people to contemplate" [558, p. 115]. This suggests that, although CISOs may succeed in increasing employee attention on cyber security through fear appeals, their efforts to change behaviour, such that cyber-security incidents do not occur, may be futile.

Similarly, business psychologist Eduard Brandstätter et al. describe "maximum gain" and "minimum gain" [163, p. 411] as different focus areas for individual risk decisions. From a cyber-security perspective, "maximum gain" could be posited as 'nothing happens', i.e., there is no business impact from a cyber-security incident. Therefore, a cyber-security 'gamble' is primarily about loss avoidance rather than potential gain. Losses may have a greater psychological impact than equivalent gains [744] and if the management of cyber-security risk is solely focused on loss avoidance, this may strengthen the emotional perception of that risk, leading to more attention being paid. These psychological impacts may, however, also lead to a disconnection from those risks.

Disconnection and othering

Culpitt suggests that individuals disconnect from concerns regarding global, existential threats due to their scale and their lack of realistic control over a response to them; rather, they focus attention solely on those threats that are personal to them [252, p. 137]. Within a business, threats affecting the organisation may be so large that individuals within that business disconnect from them, and direct their attention only towards risks that they feel they can control. Cyber-security risks specifically may not be "cognitively graspable" [563, p. 109] enough to allow employees to direct energies toward them. Mythen extends Culpitt to "argue that, for the majority, the immediacy of risks within the everyday lifeworld will take cognitive precedence over potentially catastrophic but distant risks" [563, p. 109]. If cyber-security risks are considered to be "distant" to the extent that they are not given enough attention, then the employment of a CISO may be a necessity to ensure that there is appropriate focus provided to them.

Joffe describes how responses to risk[89] are used to reinforce identities of groups, which results in 'othering', that is, distinguishing between groups as a result of how risks may affect each [447, pp. 9-10]. She highlights how this has been historically used for scapegoating, and Mythen summarises Joffe by describing how "the not me – other" approach is a handy way of absolving personal culpability and despatching blame towards targeted groups" [563, p. 101]. Joffe describes how "the ongoing debasement of 'others' in Western societies . . . becomes magnified at times of crisis" [447, p. 27], but equally describes how non-Western societies also utilise the 'othering' concept in a similar way to assign "blame" [447, p. 29]. However, she points out the dominant strength of the Western perspective, particularly regarding the media and scientific establishment [447]. The use of risk to assign blame is a common practice, particularly "[s]ince control and choice are perceived to be at the heart of Western societies" [447, p. 67], and "[t]he next step is punishment" [447, p. 67].

Neocleous also explores the use of othering in constructing both identity and a sense of fear [568]. Mythen refers to the role that "governmental discourses" play in othering, including "reproducing negative stereotypes . . . [and] apportionment of blame, masking the multicausal reproduction of risk" [563, p. 172]. As discussed above, media and governmental discourse regarding cyber security often performs this 'othering' and "apportionment of blame", particularly with regard to non-Western actors.

[89] According to "social representations theory" [447, p. 10].

Measurement of risk

A number of scholars have identified inherent positivist and rationalist bias in risk assessment processes, particularly where quantification is attempted. Slovic describes risk assessment as "subjective and assumption-laden" [695, p. 733], psychologists Amos Tversky and Daniel Kahneman refer to "[t]he subjective assessment of probability" [743, p. 1124] and Joffe highlights the omission of emotional factors in risk assessments [447, p. 61]. Beck describes how mathematical models simply present a "façade of controllability" and, consequently, "underestimate *unforeseen* and *improbable*, but not therefore *impossible*, occurrences" (italics in original) [123, p. 130]. Walklate argues that attempting to "control" risk through "reason rather than emotion . . . through the increasingly technical management of risk" is a result of a "masculine world-view" [769, p. 38], which is interesting to consider in conjunction with the masculine aspects of cyber security which were discussed in Section 2.3.3.

Rhee et al. describe cyber-security risk as "highly subjective and difficult to quantify" [628, p. 383]. However, objective attempts to measure cyber-security risk are common e.g. [426] which omit aspects of emotion and, therefore, may not be providing an accurate reflection of risk [447]. Rottenstreich and Hsee's study identified that different affective outcomes impacted upon subjects' assessment of risk, with "more sensitiv[ity] to departures from impossibility and certainty and less sensitiv[ity] to intermediate probability variations for affect-rich than for affect-poor prizes" [644, p. 188], again highlighting the importance of emotion in risk assessment. O'Malley[90] describes how

> "a certain kind of expertise produces, manipulates and governs through statistics . . . exemplifying the positivist and alienating model of security, where experts define the problem in such ways that only their expertise can resolve the issue" [584].

Viewing risk from the perspective of what Mythen describes as the "natural objectivist model", where risk is "an objective and calculable entity" which "does not entertain either the social production, or the cultural cognition of risk" [563, p. 97], results in primacy being given to attempts to measure and objectively assess risk over cultural and social aspects.

Beck argues that, in order to properly assess risk, "[all] scenarios must be taken into consideration; to knowledge drawn from experience and science we must add imagination, suspicion, fiction and fear" [123, p. 53]. He quotes philosopher François

[90] Building on previous work from fellow criminologists Willem de Lint and Sirpa Virta [274].

Ewald[91] who asserts the need to "imagine the worst possible, the consequence that an infinitely deceptive, malicious demon could have slipped into an apparently innocent enterprise" [321, p. 286]. Business leaders may not want to consider all possible worst-case scenarios, and, particularly with cyber security, may experience "cyber fatigue" [260, p. 14].

An assessment of risk tends to be a precursor to the implementation of controls, a topic I now discuss.

The use of controls

Giddens, discussing risk, defines security as "a situation in which a specific set of dangers is counteracted or minimised" [358, p. 36]. Mechanisms to achieve this are referred to as controls, language that is common in cyber security, e.g. [73, 182], as discussed in Section 2.2.1.

In a discussion regarding security controls, IR theorist Ken Booth implies a need to balance protection and convenience [151, p. 320]. A similar need for balance is also commonly expressed in discussions regarding cyber security, e.g. [408, 591]. Lawyer, computer scientist and philosopher Mireille Hildebrandt argues that compensation in some form should be provided when security controls impinge on other freedoms, distinguishing between a concept of "trade-off" versus that of "balance" [408, p. 377]. Neocleous cautions against the "notion of balance" in relation to security, in particular warning against treating "liberty and security . . . [as] antonyms" and that this "myth" provides a foundation for the acceptance of authoritarian security measures [568, pp. 12-13], with citizens trading off their freedoms for perceived security.[92] Andrew Parker, Director General of the UK's domestic intelligence service MI5, stated in 2016 that "he thought the government had reached the right balance between privacy and security" [518]. Such rhetoric exemplifies what Neocleous is cautioning against, implying as it does that it may not be possible to have both privacy and security.[93]

Utilising the same core metaphor of balance, Giddens places "trust and acceptable risk" [358, p. 36] at opposite ends of the security fulcrum. Discussing Hobbes [414], to whom I return in Chapter 6, Coles-Kemp et al. discuss the need for the security relationship between the citizen and the state to be "re-negotiated" in the light of "digitally mediated interaction" [224, pp. 44-5], particularly as citizens and states ("or large organisations" [224, p. 45]) may disagree on what exactly needs to be protected, but also, and crucially, that "citizens may value particular types of behaviour

[91] Himself extending Descartes [283].

[92] Which I discuss in more detail in Chapter 6.

[93] However, neither concept is binary.

or interaction which may be hindered or even prevented by security measures, and which may therefore prompt the use of workarounds which undermine those measures" [224, p. 45]. Their argument is that, based on a Hobbesian notion of sovereignty, security controls will only be effective if citizens perceive those controls as being in their interest and that they feel consulted on them, otherwise the state may need to "rule by force, treating its own citizens as the enemy" [224, p. 45]. Both workarounds and engagement of those being secured are concepts alluded to by Crawford and Hutchinson who suggest that prior work has

> "give[n] prominence to actors with formal powers to 'securitize' at the expense of other actors who are too often conceived as passive recipients or bystanders to such moves. As a result, less attention has been accorded to the ways in which lay sensibilities and informal processes might influence, propel or work against such tendencies" [245, p. 1188].

This again raises the importance of trust, in order to ensure not just that controls are accepted, but that they are not actively worked against. Crawford and Hutchinson suggest that controls are experienced differently by different groups, including emotionally [245, p. 1192], describing both "unintended" [245, p. 1189] and "longer term consequences" [245, p. 1193] of controls. According to Beck, sociologist Max Weber's position is that "the logic of control triumphs in the modern response to risk" [123, p. 16], and Weber is particularly relevant given the influence his work has had on modern business, as is clear from the management literature e.g. [301, 549].

2.4.5 Summarising concepts of risk

What the literature tells us is that businesses are concerned with risks to their ongoing viability. This includes cyber-security risks, which, due to their fearful aspects as explored in Section 2.3, have an emotional impact. This affects how they are perceived and responded to. Risk, or at least the response to risk, has a moral tenor that may influence how it is responded to. This suggests a further indexable component of morality beyond that directly associated with cyber security that may be available to a CISO. The literature also shows that groups perceive risks differently than individuals, and, therefore, responses to cyber-security risks in businesses may be impacted by these factors, which includes making riskier decisions. Further, it shows that risk is associated with identity, including group identity, which provides further support for the use of an identity lens in any analysis of cyber-security practice, as I explore in Chapter 4. Finally, the literature suggests that there are normative aspects to risk response, including measurement and the use of controls. This is supported by the prevalence of cyber-security controls, as discussed in Section 2.2. However, it also suggests that the use of controls has political implications, or at least political utility, and, therefore, as with cyber security more broadly, it is appropriate to apply a political lens to any analysis of risk response.

What the literature does not make clear is how these aspects of risk management relate to cyber-security practice or the role of the CISO. For example, how do the aspects of obligation and recreancy relate to how businesses respond to cyber-security risk? What influence does the existential nature of cyber-security risk have on the way in which both organisations and CISOs approach their response to it? I will explore these aspects in detail in Chapter 5 where the literature will be brought into conversation with the findings from this study.

2.5 Summary

In this chapter, I have discussed key literature that is relevant to this study. First, in Section 2.2, I explored cyber-security practice within organisations, which established both that the role of the CISO is unclear and that cyber-security practice is characterised by the implementation and operation of various controls, operating as a form of governance. In Section 2.3 I then broadened the discussion to consider concepts of security and identity. This included the characterisation of cyber-security threats as existential to an organisation's identity, as well as a discussion of concepts of identity work, which can be performed in response to such ontological threats. Finally, in Section 2.4, I explored concepts of risk, which was discussed in connection with cyber security. This extended the aspects of identity threat relating to cyber security in a discussion relating to risks to organisational viability as well as introducing the concept of recreancy. I also discussed how organisations respond to risk, which, figuratively, closes the loop with Section 2.2 in relation to the use of controls.

The literature makes it clear that the context that the CISO operates within, both within an organisation and within broader society, is one in which cyber security is considered to be a risk. This risk is characterised as an emergency, and may be experienced existentially by businesses, threatening their continued viability and, as a result, their ontological security. Organisations respond to this risk through various means, including the use of controls and the application of governance mechanisms, which help the organisation to construct, and maintain, its identity. What the literature does not tell us is exactly what the purpose, intentional or otherwise, of a CISO is. Is it a mechanism of governance, a figurehead, an enforcer of controls, a manager of risk, or something else? What the literature does tell us is that the purpose of the CISO, and the expectations on them, is unclear, and that they may, in fact, occupy a multiplicity of roles, some of which may be conflicting.

Reflecting on the wide range of literature explored in this chapter, there are common threads throughout this literature, including uncertainty, emotion, morality and politics, which can be applied to cyber-security practice. More broadly, considerable insights could be derived from bringing a wider range of concepts into discussion with cyber-security practice. This includes considering the broader societal context that the CISO operates within, as well as the role that they, and cyber-security risk management in general, may play in organisational identity. Such conceptual lenses have not previously been applied to any studies of cyber-security practice within organisations and allow a deeper understanding of the role of the CISO than an analysis that solely focuses on cyber-security literature. This includes exploring how the ontological nature of cyber-security threat may affect organisational responses to it. Further, by introducing lenses of identity, it becomes possible to understand the identity of the CISO themselves and how their experiences within an organisation may be affected by the organisation's own identity work. Aspects of morality are also potentially insightful, particularly as they relate to organisational and CISO identity, but also in relation to the perceived obligatory aspects of risk management. These moral associations are also factors in the wider societal context in which the CISO operates, and again this is an under-explored dimension of cyber-security practice. This context, affecting as it does both organisational and individual experience, appears fundamental to an understanding of the role of the CISO and, therefore, its scrutiny can enable a richer insight than has previously been achieved.

In Chapters 4, 5 and 6, I bring this breadth of literature, and the multiplicity of disciplines that it represents, into conversation with the findings from this study in order to interpret and derive meaning from that data. In the next chapter, I describe the methodology adopted in establishing these findings.

Chapter 3

Methodology

This chapter describes the approach and methods followed in producing this research. Throughout the chapter, reference will be provided back to the preceding chapters to connect theory and method where relevant.

3.1 Introduction

In this chapter, I describe the approach followed in gathering, analysing and interpreting the data that underpins this thesis. Before I address these aspects, however, I begin by providing important context in the form of the epistemological basis for the research, as well as my own positionality. Data was gathered through interviews with CISOs and board-level executives across 18 commercial businesses, as well as analysis of each business's annual report.

As mentioned in Chapter 1, the overarching research objective underpinning this thesis is to understand the purpose of a CISO in a commercial organisation, as perceived by the leaders of that function and the leaders of the overall organisation, including how that may differ. This gave rise to the following research questions:

- What factors influence a business's decision to employ a CISO?
- What are the possible roles that a CISO could perform within a business?
- What do senior stakeholders consider the purpose of a CISO within their organisation to be?
- What do CISOs themselves consider their purpose within the organisation to be?

These are wide-ranging questions, and they formed the basis for both my literature review and the gathering and analysis of data. Throughout, they have guided my decisions, being employed as a touchstone, particularly during the interpretation and construction of Chapters 4, 5 and 6. I return to these questions in Chapter 7 in order to articulate how they have been addressed, and what further questions have manifested. I now turn to the epistemological aspects of this research.

3.2 Epistemology

This section follows management researchers Jacqueline Fendt and Wladimir Sachs' recommendation that "the researcher should explain early and clearly from which philosophical stance he or she is working and disclose in some detail what prior experience and knowledge he or she brings to the study" [326, p. 450]. My research has been approached from a social constructionist position, which is reflected in the methods that I describe below. Social constructionism is a philosophical position that does not consider there to be an objective reality that can be neutrally studied. Rather, that reality is constructed socially by those who experience it [132]. In particular, this position was adopted due to the core intention of this research being to understand how organisations, through the people within them, interpret and make sense of the purpose of a CISO; their interpretation and meaning-making will be a construction, rather than having an objective reality. Further, as an 'insider' within the cyber-security industry (and also within business), any attempt at an objective study would have been fundamentally flawed.

In determining this epistemological position, other philosophies were considered, in particular critical realism. Similar to social constructionism, critical realism considers the importance of social "conditioning" [781, p. 12] on how humans experience reality. Crucially, however, it considers that reality to be objective, to exist independently of that conditioning, whereas social constructionism does not consider there to be an objective, independent reality. Critical realism initially resonated with me, possibly due to my background in the natural sciences; however, upon more detailed reading, I concluded that it was not appropriate. I explain my reasoning for this rejection further below. The journey I took to arrive at this position was valuable and, as sociologist Clive Seale argues, "philosophical debates" can provide "sensitizing context" [669, p. 12] for the researcher, as well as improving overall research quality [669, p. 8]. He further adds that "social researchers should engage in philosophical and methodological reflection as an integral part of their practice" [669, p. 17]. Management scholars Christopher McLachlan and Reece Garcia found such reflection to be valuable in their doctoral studies [542, p. 208] and their experience was particularly helpful to me in assessing the practical applicability of critical realism to social research. The 'middle ground' that critical realism appeared to offer between extreme positivist and anti-positivist philosophies attracted me as a means of reconciling my limited reflections on ontology, my background, and my experience in social organisations. Others suggest benefits to the “novice researcher” [539, p. 163] of considering a “causal framework” [539, p. 161] such as critical realism and information systems researchers Markos Zachariadis et al. particularly argue for its applicability to “the study of IS [Information Systems]” [794, p. 856]. McLachlan and Garcia, however, warn of the “seductive” [542, p. 197] nature of critical realism, especially for naïve researchers.

Sociologists Martyn Hammersley and Paul Atkinson, referencing Foucault, describe the political dimensions of social research that undermine the applicability of realist concepts, including power and surveillance aspects [383, p. 14]. Such weaknesses could be particularly problematic if these concepts were applied to this thesis, given that aspects of power and surveillance have been identified as important constructs relating to cyber security, as discussed in the preceding chapter. A further reason why critical realism does not appear to be an appropriate epistemology is articulated by information systems scholar Heinz Klein, who believes that it does not reflect philosopher Ludwig Wittgenstein’s “linguistic turn” [477, p. 133] or the concept of a double hermeneutic [477, p. 135]. This was seen as particularly problematic with regard to the topic of security, where “socially created meanings” [477, p. 133] are considered key, as briefly discussed in Chapter 2. Klein also describes “[critical realism’s] ambivalence with regard to social norms and values” [477, p. 135], which again, would be problematic due to cyber security’s reflection of both normative and value-based judgements. A further reason why critical realism was not adopted is its confused position on method [333, 542, 700].

Social constructionism, however, was seen as particularly relevant due to its resonance with themes relating to cyber security that were identified from the literature such as “identities . . . power . . . rhetoric . . . [and] everyday activities” [676, p. i]. Psychologists John Shotter and Kenneth Gergen suggest that a “common thread underlying [social constructionism] is a concern with the processes by which human abilities, experiences, commonsense and scientific knowledge are both produced in, and reproduce, human communities” [676, p. i]. Cyber security as a domain is inherently social; it relies on, and affects, such “human communities”. Businesses, as organisations, are equally social [376, p. 13], as are the technologies that they rely on [257, p. 774] [435, p. 20]. Therefore, an exploration of cyber security within business cannot ignore the social dimensions, and in particular, how those dimensions affect the meanings attributed by individuals within the participating communities. As well as being social, cyber security is interpretive: there is no one objective method of ‘doing’ cyber security. I argue that the core concept explored by this research, namely purpose within cyber security, is interpretive – there is no objective, or consistent, understanding of this purpose across the industry and its stakeholders.[1] Rather, that understanding is jointly, and continually, constructed. Additionally, social constructionism has particular relevance to multi-disciplinary work [610] and, as detailed in Chapter 2, cyber security is inherently multi-disciplinary [381, 654]. The decision to approach this research from a social constructionist position has influenced the methods chosen, which are described further below. Most significantly, an interpretive approach has been adopted, which resulted in the use of semi-structured interviews, an application of inductive data coding practices and the use of thematic analysis. As other qualitative researchers have articulated, methods are not necessarily formulaic [699, p. 213] and an inductive approach allows for exploration and experimentation with different means of gathering and analysing data.

Having described how I arrived at this epistemological position, I now turn to my own positionality.

3.3 Positionality

At the time of performing this research, I was, and still am, a full-time practitioner in the cyber-security industry, employed as a CISO at a commercial organisation. I have business and information technology experience spanning over twenty years across a variety of industries, including some that have formed part of this research. This is important with respect to the present research from a number of perspectives. This experience is likely to introduce an aspect of bias, particularly with regard to my own opinions on the research questions and this section reflects upon these.

As a practicing CISO, I am researching a field that is highly familiar to me, and I can be considered an 'insider' within that field. Constructionist and interpretivist approaches contrast with "the positivist research paradigm that assumes the researcher is always on the outside looking in" [561, p. 293]. I considered that being an 'insider' in the cyber-security industry, as well as, more broadly, in the domain of those who work in UK-based commercial businesses, would be beneficial in both gathering and analysing data. However, I am also an 'insider' from the perspective of demographic and socioeconomic groups and the membership of these groups will have affected many aspects of this research. Psychotherapy scholar Charlotte Burck describes how "[t]he ways in which the researcher is positioned as similar and different to the research par-

[1] Which is similar to the field of legal and regulatory compliance, a closely linked and overlapping domain with cyber security [213], where interpretation is considered key [143, 144, 183].

ticipants, in relation to culture, class, 'race', ethnicity, gender, age, sexual orientation and ability ... need to be taken into account" [181, p. 242]. I discuss these aspects further in section 3.4.2 below.

My prior experience may have resulted in assumptions based on the responses of the participants, as well as interpretations being made that a non-practitioner would not necessarily make. Conversely, there may have been advantages to my interpretations being based on prior experience. My background makes it likely that I have identified with the interviewees, as described by Hammersley and Atkinson [383, p. 112], which I attempted to address in part through the use of an inductive approach to gathering data, rather than to potentially introduce bias through structured questioning. However, as sociologists James Holstein and Jaber Gubrium point out, a constructionist approach to interviewing challenges the concept of bias itself, as the subject is not a "vessel [of knowledge] waiting to be tapped" [419, pp. 17-18].

My prior experience may also have resulted in assumptions being made by participants themselves [606, p. 77], who may have assumed a level of knowledge or understanding on my behalf, resulting in omissions or limitations of their answers. However, this prior experience also provides a level of credibility which is likely to have been beneficial for the interviews, particularly as an interview with an informed interviewer may have been more appealing than one with someone with whom 'the basics' would need to be 'spelled out'.[2] This credibility may also have supported the generation and maintenance of rapport with the participants, particularly those who were cyber-security practitioners. A shared professional knowledge base and other common factors may have resulted in interviewer and interviewee considering the other as 'equals'. Conversely, an 'equal' level relationship was unlikely to have been established at the board member level, however, my 'insider' status may have helped position the interviews in a way that minimised any imbalance [631, p. 74].

Knowledge as a practitioner may aid the application of a critical analytical view [700, p. 15]. My experience could have resulted in a 'stronger' interpretation of the data [477], and, at least, is likely to have minimised the need to 'learn a new language' in order to understand participants' responses [178, p. 494]. This may have helped build rapport and meant that I required less "preparation" [316, pp. 62-63], putting me at an advantage compared to researchers who may not have this prior experience.

Sociologist Karen Locke explains that there have been different historical perspectives on the value, or otherwise, of "allow[ing] for ... prior theory, nontechnical literature, and personal as well as professional experience to help researchers gain insight into the data" [509, p. 242]. Du Gay and Vikkelsø point out that 'classical' organisa-

[2] Indeed, this was explicitly indicated by one participant.

tional texts were predominantly written by practitioners and they view contemporary literature as lacking, due to scholars having focused too heavily on the theoretical and conceptual aspects [301, p. 30]. Their argument is against an external point of view that examines the "conditions of existence" that affect the organisation [301, pp. 66-67] and supports a view that being a practitioner in the field under study may provide benefit. Management scholar Kevin Corley presents a culinary analogy based on a discussion with another management scholar, Davide Ravasi, to suggest that "your personal experiences [cooking stews and sauces] is [*sic*] usually more important than the recipe" [240, p. 603]. Reflecting on this throughout the research, I consider that my experience and knowledge has been both beneficial and crucial to its effectiveness and quality.

3.4 Methods

This research is interpretive in nature, which, as has been established within cyber-security scholarship, e.g. [182], is an effective means of studying cyber-security practice. As other qualitative researchers have articulated, methods are not necessarily formulaic [699, p. 213] and my approach has been primarily an inductive one, allowing exploration and experimentation with both gathering and analysis of data. Semi-structured interviews and publicly available company documentation were used as data sources which were coded and analysed, initially inductively, then subsequently through multiple deductive phases of analysis. Interview participants were CISOs and executive-level senior leaders from a range of UK-based businesses. These are treated as individual cases and the inclusion of senior leaders was intended to provide an additional perspective beyond that of solely security professionals. Interviews were conducted face-to-face in the majority of cases, however, a number of later interviews were performed remotely in response to the Covid-19 pandemic. Each organisation's annual report was also coded and analysed, providing a further top-down perspective.

I performed an initial pilot study in order to assess the effectiveness of my intended approach, as recommended by sociologist Joseph Hermanowicz [405, p. 494], which I now describe.

3.4.1 Pilot study

The pilot study involved semi-structured interviews with three CISOs, each employed at a different non-UK listed organisation. The rationale for this was that I already had contacts at a number of these organisations that had indicated their interest in supporting this study but would not meet an initial UK-listing criteria I had established, which I explain in section 3.4.2 below. Rather than omitting them altogether, their inclusion in a pilot study was seen as benefiting the overall research process.

I conducted the interviews based on an initial interview guide that I developed based on themes identified during my literature review, using my research questions to inform and validate the content. The pilot was particularly helpful in validating and adjusting this guide, which comprised prompts to help me explore specific themes.[3] It was notable that many of the prompts I anticipated using were not necessary due to the way the conversations naturally progressed, which helped in making the interview itself less 'artificial'. The results of the pilot were then coded and analysed. Analysis of the pilot data was not as detailed as the main study, as the purpose was primarily to assess the effectiveness of the interview approach; however, this analysis activity was particularly useful in providing me with an introduction to the process of coding and analysing qualitative data. The pilot also provided valuable practice with using the technology that I employed to support the interviews, particularly the encrypted recording devices that I had purchased. It became apparent that these devices were themselves conversation starters, particularly due to their encrypted nature, a phenomenon experienced by other researchers [405, 798].

Of considerable benefit was acquainting myself with transcription. I had no prior exposure to this and performing the transcriptions manually helped me to understand not just how much effort was involved in producing the transcript but also how rich the conversations were. The hard work of manual transcription was something that was helpful to be aware of in advance of subsequent interviews[4] and these initial experiences also inspired me down the path of developing a secure semi-automated transcription method [258].

A further benefit of the pilot was useful experience with regard to capturing fieldnotes.[5] These included aspects such as body language, room layouts and physical security arrangements, e.g. access control provisions at the sites where I interviewed the participants, as well as my own reflections both before and after the interviews. Getting into the habit of noting these down and reflecting on them was very helpful, particularly as my professional experience as someone who regularly visits other companies' offices may have normalised me to office security procedures, or at least may have led me to internalise any feelings of 'otherness'. All of this experience informed

[3] The final interview guides are presented in Appendix C.

[4] I did go into the second and third pilot interviews feeling a slight sense of trepidation about the amount of work that was awaiting me afterwards, which was recorded in my fieldnotes, but this was a minor concern.

[5] Although not technically performing 'fieldwork' in terms of immersion within a field, I have referred to my notes and reflections in relation to the interviewing process figuratively as 'fieldnotes' and these formed part of the data corpus for analysis.

my method for the subsequent phases of data gathering.

3.4.2 Data collection

Following the pilot study, the main research interviews took place in two phases between October 2019 and July 2020. In total, 21 interviews were conducted, representing 18 different companies. Of the 21 interviews, 15 were with CISOs and the remaining six were with senior organisational leaders, as shown in Table 3.1.[6] The industries represented are summarised in Table 3.2. During the same time period, each company's most recent annual report was downloaded from their public website.

Table 3.1: Participants & interviews

Participants		**Interview**		
ID	*Duration*	*Medium*	*Timing*	*Phase*
CISO1	00:48:29	F2F	Oct19	Phase 1
CISO2	00:49:28	F2F	Oct19	Phase 1
CISO3	00:47:33	F2F	Dec19	Phase 1
CISO4	00:44:41	F2F	Dec19	Phase 1
CISO5	00:43:44	F2F	Dec19	Phase 1
CISO6	00:41:38	F2F	Jan20	Phase 1
CISO7	00:45:19	F2F	Jan20	Phase 1
CISO8	00:49:41	F2F	Mar20	Phase 2
CISO9	00:51:30	F2F	Mar20	Phase 2
CISO10	00:38:43	Remote	Apr20	Phase 2
CISO11	00:55:45	Remote	May20	Phase 2
CISO12	00:40:56	Remote	May20	Phase 2
CISO13	00:40:07	Remote	Jun20	Phase 2
CISO14	00:46:07	Remote	Jul20	Phase 2
CISO15	00:50:02	Remote	Jul20	Phase 2
CEO1	00:24:59	F2F	Dec19	Phase 1
CEO2	00:42:45	F2F	Jan20	Phase 1
CFO1	00:45:41	F2F	Jan20	Phase 1
CFO2	00:40:52	Remote	Apr20	Phase 2
CIO1	00:47:28	Remote	Jul20	Phase 2
NED1	00:27:52	F2F	Dec19	Phase 1

21 semi-structured interviews were conducted with CISOs (15) and non-CISOs (six) between October 2019 and July 2020.

Participants

The research participants for this study were CISOs and executives and non-executives from a variety of UK-based, but predominantly multinational, commercial entities. Participants were selected primarily on the basis of availability of access through pro-

[6] As discussed in section 3.6, organisations were randomly assigned a pseudonym based on capital cities, but for ease of reading in this thesis, these have been substituted by the participant's abbreviated job role and an incremental number, i.e., CISO1, CISO2, CEO1.

Table 3.2: Industry sectors represented in this study

ICB Super-sector	*Number of organisations*
Banks	1
Food, Beverage and Tobacco	1
Industrial Goods and Services	6
Personal Care, Drug and Grocery Stores	2
Real Estate	1
Technology	1
Telecommunications	2
Travel and Leisure	1
Utilities	3
Total	**18**

Coverage of industries represented in this research based on classifications taken from [48].

fessional networks, as described in more detail below. However, one criterion applied was that research was limited to those working for organisations that were quoted on a major stock market, which was intended to provide a level of consistency across organisations on the basis of being subject to common corporate governance requirements. Initially, I limited this to organisations that were listed on a UK public stock exchange. This was relaxed in the second phase due to an opportunity arising regarding access to a non-UK listed organisation, however the vast majority[7] of organisations surveyed were UK-listed.[8] I provide the rationale for this criterion below.

Senior organisational leaders were chosen as participants in order to provide multiple perspectives on cyber-security practice and achieve a degree of triangulation. I considered it important to gain different viewpoints so as not to limit the scope of my analysis. Although the original intention was to gain both CISO and senior leader perspectives from each organisation, due to the difficulty in gaining access, this was not possible, as I explain further below. However, as each participant is treated as an individual case, and the focus of this research is not on the organisations themselves, this is not considered to be a limitation.

Distinguishing between "informants" and "respondents", sociologist Jennifer Platt describes how the former "is seen as providing objective information to be taken more or less at face value, and is a distinct person with something unique to contribute, not just a randomly-sampled and replaceable member of the crowd" [606, p. 85], whereas "[t]he respondent's task is to provide raw data to be interpreted by someone else, and he is an anonymous member of a large group" [606, p. 85]. Using these definitions, the subjects of my research are treated as "informants", although they are referred to as

[7] Over 90%.

[8] Notably, one of the UK-based organisations had recently been taken private and, at the time of interview, had been delisted for a short period of time (less than six months). There had been no change to the organisation's corporate governance in this time.

'participants' as this term suggests a more inclusive, and "active role" [555, p. 404], which is more accurate for this research. From an epistemological perspective, not only are the interviews jointly constructed, but also, as highlighted by political scientist Lee Ann Fujii [343], I have been studied by the participants as much as the other way around. This was seen as a particularly noteworthy perspective given my professional role as I could conceivably have been seen by the participants as a potential future colleague, subordinate or collaborator – or even as a competitor for a future position.

Rationale for selection of organisations. Within the UK, company directors have a duty under the Companies Act 2006 to "promote the success of the company" [4, §172] and "exercise reasonable care, skill and diligence" [4, §174]. As mentioned in Chapter 2, the Act places other obligations on company directors in relation to risk management and corporate governance. From a cyber-security perspective, prior research has shown that boards are specifically being consulted, briefed on and engaged in the management of cyber-security risk, e.g. [778].[9]

From the perspective of my research, the corporate governance requirements of UK-listed companies were deemed to provide a consistent basis of risk awareness, albeit not necessarily one of cyber-risk awareness. To expand this research to privately held organisations, or those not subject to similar governance requirements, was considered to have introduced further variables and complexity, unnecessarily complicating the analysis, and, therefore, these organisations were not in scope. As mentioned above, due to an opportunity presenting itself to interview a participant from an organisation that was not listed on the UK stock market, I relaxed my UK-only criterion; however, this was done on the basis that the organisation in question was listed on a major European stock market that had similar corporate governance requirements [580, pp. 23, 25]. Only one such opportunity arose and, therefore, the majority of organisations studied met my initial criterion.

Recruitment of participants

Prior experience provided me with "opportunistic" [669, p. 116] access to research subjects through my professional network, and other researchers have studied particular organisations due to the level of access that they knew they had or could arrange, e.g. [305]. As a practicing CISO, I already had a wide network of contacts across multiple industries who were considered to be suitable participants. The professional

[9] Further, audit researchers Md. Shariful Islam et al. refer to some organisations, predominantly in the financial sector, operating a dedicated "cyber-risk committee" [439, p. 383] which is implied to be at board level, although this is not clarified.

cyber-security community in the UK is a relatively open and collaborative one, with regular contact between CISOs occurring, across industries, at both professional and social events. This provides both a means to establish and maintain access, and to build rapport with intended interviewees, who are often supportive of experience-sharing.[10] Czarniawska identifies that "practitioners, especially those in elevated positions, are often quite lonely in their thoughts... [meaning that a] research interview... opens a possibility for an unusual but symmetrical exchange" [256, p. 48]. I considered this to be both relevant and backed up by my own experiences, but expected it to perhaps be less applicable to board members than to CISOs. However, positive feedback on the interview experience was provided by both groups of interviewees.

Participants were engaged through a variety of means. Those who I had a pre-existing professional relationship with, or were at least known to me through professional circles, were contacted directly via email, with a series of exchanges to introduce the research and gauge their amenability to being involved. A small number of participants were recruited through face-to-face interaction at industry events where I was able to explain the research in more detail in an attempt to influence their agreement. A similarly small number of participants were also recruited through mutual acquaintances who provided email introductions between myself and the participant. Finally, other participants, where there was no prior relationship, were recruited through direct contact on LinkedIn. This latter method was the least successful but did result in a number of interviews. Although I achieved what I consider to be a reasonably positive response rate, there were a number of potential participants who ultimately did not contribute to this research. In a high number of cases, despite several promising initial responses and dialogue, no interviews were forthcoming. Accepting that I am not the first researcher to have such experiences, e.g. [235, 316], I nonetheless was expecting to encounter less rejection from CISOs (my in-group) than I did, particularly where they had already responded to my initial contact.[11] In comparison with executives and non-executives, where I had made contact with these participants there was no subsequent ignoring of follow-ups, although admittedly there were far fewer of them and none of them were approached 'cold', i.e., I either had an existing connection with them or had been introduced by someone they trusted.

This use of my personal network meant that the eventual sample was effectively a "snowball sample" [383, p. 135] with a number of contacts being able to introduce

[10] For example, one participant in this research stated "I'm a massive advocate of helping others, you know and so I appreciate you reaching out and asking [for an interview] ... I think [this research is] only a positive thing and I think it gives back to the broader cyber community".

[11] Although this was never explicit rejection; in all cases, the potential participant simply stopped responding.

me to additional research participants. This occurred both through those who were directly involved in the research and were able to introduce me to others who might be willing to participate, as well as through those who were not involved in the research in any way, e.g. acquaintances at other companies who did not work in cyber security or at a board level but were willing to introduce me to relevant contacts that they had. I was deliberately "target[ing] those people who have the knowledge desired and who may be willing to divulge it" [383, p. 137], thus also making this a "criterion" [557, p. 10] sample. It could be argued that through my desire to restrict my targets to those that represented only listed businesses (for the reasons outlined above) this was, to some extent, also a "purposive" [557, p. 10] sample.

There is little opportunity to gain access to board members outside of a professional environment and access to these participants was approached through CISOs who were participating in the research, and who should already have a relationship with their own board members, as well as through the board members with whom I already had a relationship. These relationships are likely to have played a significant role in securing access. As others have noted, e.g. [316, p. 61], senior leaders are unlikely to engage with academic research philanthropically and there is an aspect of their participation which may have been related to 'doing me a favour' because of previous positive interactions, or because it may have put them in a good light with their peers. Only one of these participants ended up being a 'cold' engagement, i.e., where I had no prior contact and this participant was recruited through an introduction from that organisation's CISO. Despite requests being made to all CISO participants, and an indication of support being provided in many cases, only one was able to effect such an introduction. I did not find this surprising, as, due to the seniority of these individuals and associated demands on their time, the CISO participants may have either struggled to obtain agreement from them, or may have subsequently decided that securing their agreement was too difficult to attempt. Similar requests were made to the non-CISO participants for an introduction to the CISO at their organisation and two such introductions materialised as a result.

Negotiating access. I consider that my professional role has eased access. My role, and my employer, provided a 'badge of credibility' and also helped rapport. This was certainly the case with the other CISOs but I felt this was also the case with non-CISOs. If I were 'just' a researcher, as well as access having been harder to obtain, the power dynamic would have been different. With the CISO participants I was certainly an 'equal' and with non-CISOs, I occupied a role that they understood, at least superficially, and, therefore, it was easy for them to categorise me and to know how to engage with me. This 'occupational categorisation' may also have inhibited other prejudgements [558].

My role also provides a potential *quid pro quo* in that the participants may have seen me as someone who could provide useful information to them as well. This was certainly the case with a number of participants, both with CISOs and non-CISOs, where I have been asked to provide opinions and discuss matters relating to security. This may not have impacted upon the data collection, particularly as it occurred post-interview, however, it is important to note that the access I had to such experiences and information would have been implicit to the participants and may have affected their decisions to participate in the first place. Such exchanges are not unusual in qualitative research [71, pp. 175-176].

Hammersley and Atkinson highlight the importance of considering temporal aspects when interviewing those in organisations [383, p. 225]. Awareness of business cycles in particular was important as it may have limited or impeded access. For example, the likelihood of securing time with a board member would be lower if an interview was sought in close proximity to fiscal year end or to the release of an annual report. Understanding some of these constraints in advance was not possible; only publicly available information, as described in each organisation's annual report, was available to be considered. Based on this, I did not seek interviews with executives or non-executives close to their company's fiscal close periods.

Participant sample

Exact sample size was initially approached on a basis of data saturation, although the original intention was for a breadth of study in order to encompass different industry sectors. At the point of commencing my studies, I had intended to cover somewhere between 20 and 40 companies during the course of my research; these were arbitrary figures. At that stage I had not reviewed any academic literature and I subsequently realised that it was unwise for me to attempt to define my sample size upfront [140, 683], or to consider that a larger sample was preferable to a smaller one [142]. However, the literature highlighted continuing debate. Management scholars Kathleen Eisenhardt and Melissa Graebner argue that "[m]ultiple cases ... enable broader exploration of research questions and theoretical elaboration" [309, p. 27] and health researcher Janice Morse suggests that "over 20 interviews" equates to "a reasonably large sample" [556, p. 588]. However, sociologists Mira Crouch and Heather McKenzie suggest that "a small number of respondents ... is the way in which analytic, inductive, exploratory studies are best done" [251, p. 496], arguing for small samples[12] to be used in qualita-

[12] "[L]ess than 20, say" [251, p. 483].

tive research, an approach followed by some other cyber-security researchers, e.g. [97]. Others have experienced data saturation within as few as twelve interviews [378], but, as discussed below, data saturation itself is a problematic concept.

The interviews were phased, with an initial, arbitrary, target of five to ten interviews per phase. My first phase comprised a total of 11 participants, representing 10 different companies. This latter number, and the arbitrary target mentioned above, suggest that I was initially guilty of what social researcher Mark Mason identified, in that many PhD studies feature an arbitrary determination of sample size based on "multiples of ten" [534, p. 1] rather than through data saturation. Fortunately, I recognised this at the start of my second phase of interviewing and attempted to correct this approach. The second phase did comprise ten participants, representing eight companies, although 12 interviews were originally scheduled (two participants withdrew).

Data saturation. A number of participant discussions resulted in 'snowballing'. One potential limitation of the snowballing approach is that it "can lead to an unrepresentative account" [669, p. 116], although a concern with 'representation' can be argued as a positivist position. I was not initially familiar with the concept of data saturation and its perceived importance in qualitative research [557, p. 11]. Data saturation, as distinct from theoretical saturation [660, p. 1895], is considered to be reached when no new data emerge [347]. When considering whether data saturation was reached, it was important to consider how my individual interpretation of the data may differ from that of participants [347, pp. 1410-1411]. This difference will have affected how I determined data saturation and, therefore, I was conscious of approaching this judgement on the basis of what the participants were saying rather than what I was interpreting them to have said. I decided to approach saturation as an ultimately incomplete "cumulative judgement" [660, p. 1901] rather than a specifically identifiable juncture. As I began to notice repetition of comments from participants, in particular where their responses were echoing those from previous interviews, I considered that saturation may be approaching.

However, data saturation is a problematic concept. It has "a number of practical weaknesses" [586, p. 194], has been argued as a "legacy of quantitative science" [586, p. 195] and can even introduce "ethical issue[s]" [339, p. 1230]. Ultimately I made a decision to stop gathering data on "[t]he adequacy of the sample ... [not] solely on the basis of the number of participants but the appropriateness of the data" [586, p. 195]. I regularly revisited and revalidated this decision during the analysis phase, to continually confirm my judgement that the sample size was adequate.

Another consideration was the availability of participants and exhaustion of my contacts, although this is not equivalent with saturation [347]. When I felt that no new data was emerging, I decided that it was counter-productive to seek new participants via unsolicited contact. This could have impacted not just any future engagement of mine with those individuals if they had a negative view of 'cold-calling' but may also have been detrimental to other researchers studying these groups. There were also more limitations identifying willing participants who were in executive or non-executive roles. The difficulty of securing interviews with such participants may have influenced my decision-making regarding data gathering for this latter group in particular and I may have, consciously or unconsciously, made a judgement of saturation having been reached based on this. I was also conscious that I would have an opportunity to seek further participants at a later stage of the research if, after beginning the analysis, there were indications of data not being saturated. Therefore, I considered the judgement that I made to begin analysis after 21 cases to be relatively low risk to the overall quality of the study, and in line with other qualitative research [373].

Limitations of participant sample

There is a lack of diversity, from a number of perspectives, in both of the participant groups interviewed. This presents a limitation to the research that, while reflecting broader situations in both cyber security and business, possibly reinforces it as a result of restricting the voices that are represented. I describe these, and further limitations, in the following section. A range of demographic information was requested from participants through the use of an optional, and anonymous, demographic information sheet[13] provided to participants either at the point of interview or, in the case of the interviews performed remotely, beforehand. This requested information relating to gender, ethnicity, age and socioeconomic background. Out of the total 21 participants, 16 provided this information. Completion of demographic forms was noticeably harder to achieve in the remote interviewing mode. When interviewing in person, there were no situations in which this information was not provided, whereas for the remote interviews, and despite agreement to provide this information, only three (of eight) participants returned a completed form, even after a follow-up request.[14] The provision of this data was, of course, entirely optional, however, it is interesting that non-completion only occurred in the remote interviewing situations.

[13] See Appendix E.

[14] Only a single follow-up request was made in each instance so as not to impact rapport or undermine the optional nature of this information.

Gender. There was a lack of gender diversity in my sample, and this was more pronounced in the CISO participant group. This reflects the broader lack of representation of women in the cyber-security industry [594, 621]. While boards of directors are similarly over-represented by men [161, 433, 458, 533], I had not experienced particular difficulties identifying female participants for this group, albeit this is a smaller sample, which is still male-dominated, and most participants in this group were already known to me. As discussed briefly in Chapter 2,[15] security is a male-dominated discipline which perpetuates gendered language and concepts [769, p. 38] and both CISO roles and senior management roles may be inherently gendered [92, p. 85].

I did deliberately seek out female CISO participants at an early stage, given my knowledge of the under-representation mentioned above, and wanted to address what I saw as a potentially problematic dominance of male voices, but was equally conscious of avoiding tokenism. While I did attempt to use my professional network, unsuccessfully, identifying female participants was primarily attempted through unsolicited contact via LinkedIn. This was not successful either however; unsolicited contacts with male CISOs via this method did result in some success, but no unsolicited contacts with female CISOs resulted in an interview taking place, despite some initial positive responses.[16] One female CISO did agree to be interviewed but had to subsequently withdraw their participation due to work demands. Figure 3.1 summarises the distribution of self-defined gender identities provided by those who provided demographic information.[17]

[15] And explored in more detail in Chapters 4 and 6.

[16] I did consider, possibly paternalistically, and heteronormatively, that female CISOs may be more wary of unsolicited social media contacts than male CISOs. However, this may be a completely inaccurate interpretation and there could, of course, be many other factors involved.

[17] I recognise that some of the diagrams in this thesis may be difficult to read, particularly in printed format. All diagrams have been included as high-resolution images that allow zooming in when accessing this document digitally.

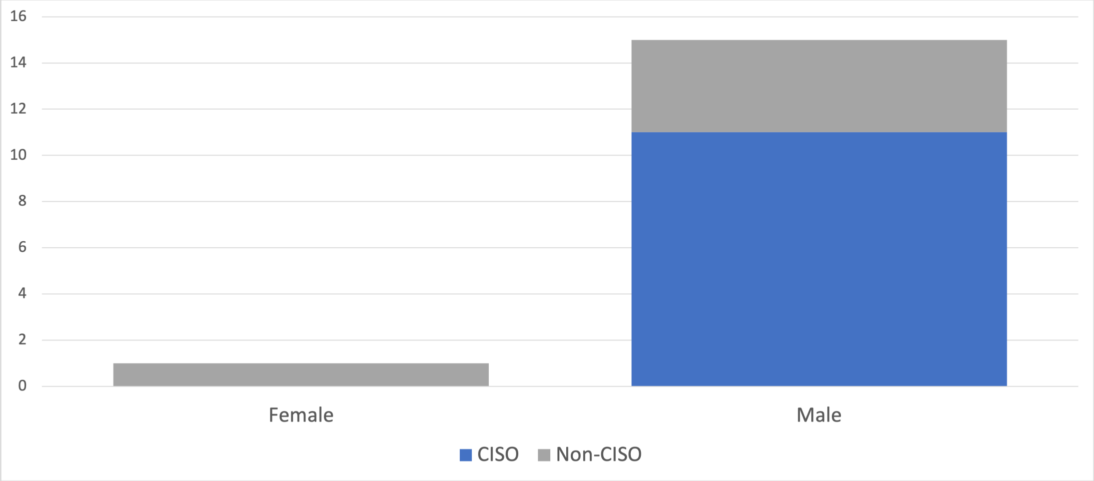


Figure 3.1: Distribution of self-described gender identities of research participants who provided demographic information (n=16)

This figure shows that the vast majority of my research participants identified as male, as do I. Therefore, there is a risk that this research is biased towards, and may reinforce, gender-based norms, and language [284, 545], that privilege males. Sociologist Margaret Archer's reference to how "[talk between] 'similars and familiars' . . . reinforce[s] normative conventionalism" [92, p. 33] seems particularly relevant to this point.

Sociologists Joseph Conti and Moira O'Neil argue for the "adopt[ion] . . . [of] feminist approaches to studying elites" [235, p. 64], including, specifically, "researcher accountability to knowledge claims and critical examination of the micropolitics of research" [235, p. 66]. Responding to this call, the analysis phases of this research have reflected upon potential bias and gender norms, whether explicitly identified or latent. Migration scholar Anna Boucher refers to prior research that indicates gender alongside other factors affecting "interview power relationships" including "class, educational status, race, ethnicity, disability and cultural context" [154, p. 99]. Boucher also highlights[18] a gender-based trust factor which can weight reticence relating to information disclosure by males in favour of female researchers, as female interviewers have a "heightened trustworthiness" [154, p. 100]. As I am male, there may have been a detrimental gender bias when interviewing other males, although there was no obvious indication of this and it may be difficult to identify.[19]

[18] Referencing political scientists Gabriele Abels and Maria Behrens [62].

[19] It is also possible that an interview between two males results in neither of them properly listening to what is said [284, p. 98].

Ethnicity. There was limited ethnic diversity in the participant groups, which again reflects a wider issue with both boards and the cyber-security industry [161, 680]. I was conscious that it was more difficult to identify different ethnic group membership from unsolicited contact, as such group membership may be less superficially obvious than gender identity, acknowledging that the latter may also not be obvious, and equally acknowledging that my perspective on this is as a cisgender male. As with gender identity, this was an open question requiring self-definition, rather than a series of choices for participants to choose from. I felt this was more empowering for the participants, rather than forcing them into a pre-defined category that they may not be comfortable aligning with.[20] I did receive a number of comments about the self-defined aspect of this[21] with a number of participants being uncertain about how to define their ethnic origin in the absence of a clear category.

One limitation of using self-described categories is that a presentation of the results may undermine anonymity of the participants. For example, if there is only one member of a community that identifies as a particular ethnicity, then the presence of that ethnicity in my results may disclose their participation, particularly when combined with other data such as industry sector. Because of this, I do not present the details of the ethnicity data gathered. The vast majority of, but not all, participants self-identified as 'white' in one form or another, although these were not exclusively Western definitions of 'white'. My own ethnic origin is very mixed[22] which may, or may not, have influenced my interaction with participants.[23] However, the mixed nature of my background may not mark me out as 'other' enough to have affected our interactions.

Age. Age demographics were requested from participants which used pre-defined age ranges rather than requesting exact ages, as the latter was not deemed necessary for this research. The age profile of the participants that completed the optional demographic survey is shown in Figure 3.2.

[20] This reflects a personal view that the use of pre-defined categories both enforces existing societal norms around ethnicity definitions and gives primacy to the convenience of completion for dominant groups. Self-definition of such categories has been recommended by others, e.g. [29, 99] although these approaches have also been criticised, e.g. [538]. As applying a demographic lens is not a core objective of this research, I have not explored this debate further.

[21] With only one similar comment about the self-defined aspect of gender, which occurred during the pilot phase.

[22] Representing both the Global North and Global South.

[23] At least one explicit comment was made about this by a participant.

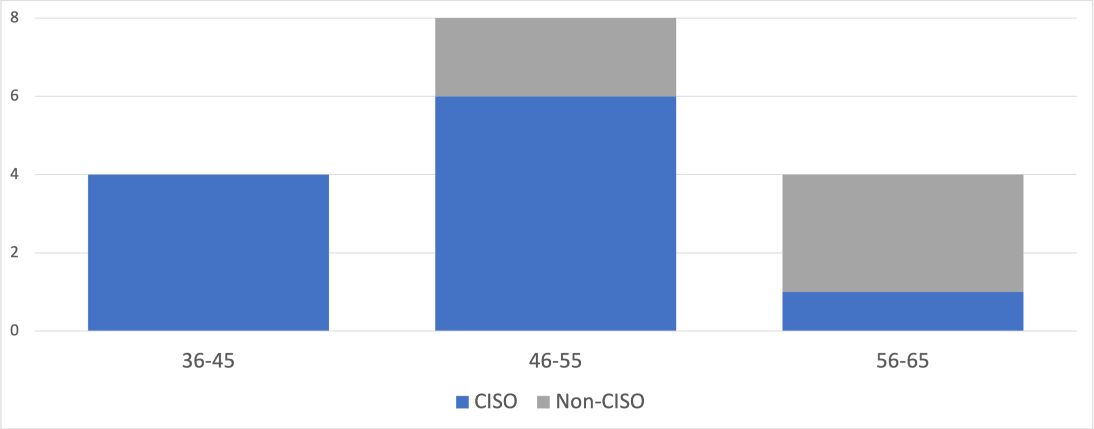


Figure 3.2: Age profiles of research participants who provided demographic information (n_{all}=16, n_{CISO}=11, $n_{\text{non-CISO}}$=5)

This figure shows a clear difference in age profiles between the CISO and non-CISO participants. At the point of performing the research, I was in an age bracket closer to that of the CISO participants than those at a board level. This may have eased rapport with the former and, potentially, have affected power dynamics with the latter.

Socioeconomic group. Level of education, based on pre-defined categories, was the final question on the optional demographic survey sheet. The distribution of responses is shown in Figure 3.3. Prior research has shown that socioeconomic background affects behaviour [527] and Archer suggests that "subjects' social backgrounds" [92, p. 16] are a determinant in the type of reflexivity they display. Although socioeconomic origin has been related to early career progress [780] and career choice [80], it is not necessarily the case that those occupying either CISO or board-level positions have originated from a particular socioeconomic group, although those from higher socioeconomic groups may be more inclined to seek out "positions of influence" [661, p. 120] due to their background. Level of education has also been associated with digital security skill development [291]. This may indicate a link between socioeconomic status and career choices in cyber security, if level of education is used as the determining factor in socioeconomic categorisation, as per [291], a method described as "prevalent" [292, p. 81].

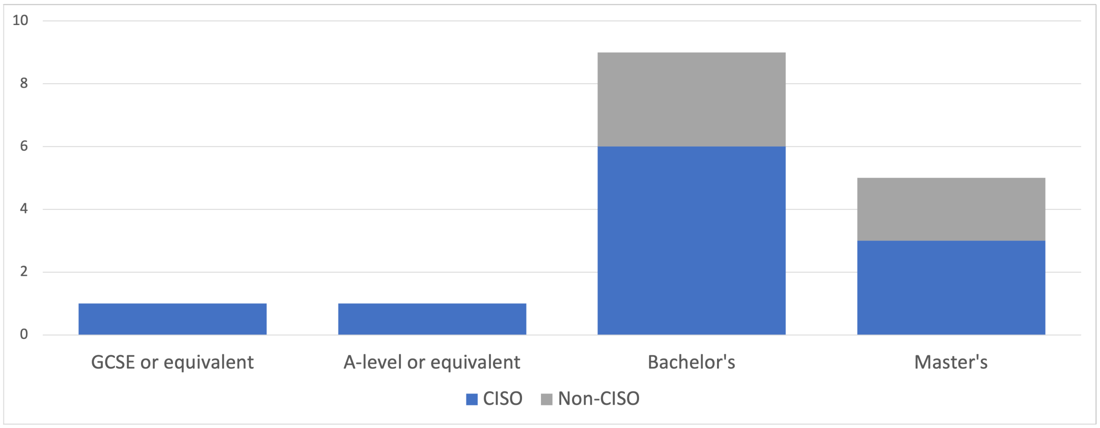


Figure 3.3: Highest level of education of research participants who provided demographic information (n=16)

This figure shows that the majority of participants in this research would be considered to occupy a high socioeconomic status, based on level of education as a proxy.

The participants fall into two broad categories, those that are executive or non-executive leaders of an organisation (n-1 in terms of organisational level, where n is the CEO or Chairperson) and those that are leaders of an organisational function (n-2 or n-3). Despite this difference in relative seniority, all participants can be considered to be 'elites'. Previous research has considered "functional experts" [154, p. 100] and "professionals as a whole" [316, p. 59] as elites, and taking a crude measure of salary,[24] CISOs in the UK typically fall into the top 2% of earners, whereas executive and non-executive leaders fall into the top 0.5-0.1% [452]. These distinct groups clearly have similarities, but there are also differences between them and I consider the CISO group to be 'sub-elite' on this basis. Of course, as a CISO myself, I fall into this group and, therefore, it may serve my ego[25] to make this judgement.

"Similars and familiars". As already quoted above, Archer describes how "the practice of communicative reflexivity, exercised through 'thought and talk' with interlocuters who are also 'similars and familiars', strongly tends to reinforce normative conventionalism . . . [and] privileges . . . certainty over uncertainty" [92, p. 33]. I am a "similar and familiar" in relation to the CISO participants, which suggests a potential limitation of the study, and, as discussed further below, there may also be a political dimension. Another consideration is that highlighted by leadership scholars Scott

[24] Excluding other measures of wealth.

[25] And/or conscience.

Snook and Rakesh Khurana; invoking Foucault, they describe how “the classification of knowledge ... limit[s] our thinking” [704, p. 58], as well as underpinning “professional identity” [704, p. 58]. As someone who works in the same discipline and performs the same role as the CISO participants,[26] it is likely that the joint construction of knowledge that we achieved in the interviews was constrained by our shared knowledge base. This limitation may also have existed, albeit to a lesser extent, with the other participants, where the common knowledge base was that of corporate business in the UK.

My own membership of certain demographic groups will have affected my research, both in terms of gathering and analysing data. However, my role as a CISO may also have inhibited any prejudgements from participants [558] on the basis of these group memberships. While there were limited explicit instances of any effects, I have reflected on this as much as possible and bring these reflections into conversation in later chapters. My professional career has involved extensive interactions with senior business leaders at a variety of organisations and, therefore, my engagement with elites and sub-elites is likely to differ to that of researchers without this background. As a result, I may have had more confidence in dealing with the research participants, which, as others have noted, e.g. [316, p. 61], is important when interacting with elites. However, as those participants represented companies that I had little experience with, this confidence may not have been as strong as when dealing with elites at my own employer, although conversely, elites from other organisations will have had no obvious stake in my career, which could have led to greater confidence as a result. I also occupy a role as a member of an elite socioeconomic group, and as a member of the cyber-security industry. This may support what Archer describes as “the maintenance of ‘contextual continuity’ ” [92, p. 18]. From this perspective, I myself, whether consciously or not, may have been performing a political act in reinforcing or otherwise encouraging particular perspectives that privilege elites, including myself, and the associated power dynamics. I reflected upon these considerations during the analysis and discuss a number of these aspects further in Chapter 6.

3.4.3 Interview approach

Semi-structured interviews are an established qualitative research method within the domains of business, e.g. [537, 598], cyber security, e.g. [97, 687, 751], and IT governance, e.g. [441, 611], with both elite, e.g. [775] and practitioner, e.g. [97, 777] participants. Such interviews are “methods for learning with an open mind” [306, p. 1162].

For the face to face interviews, participants were interviewed at their own office

[26] And is likely to have similar, if not identical, professional qualifications.

locations. Hammersley and Atkinson discuss the importance of location with regard to interviewing research participants [383, p. 149] and suggest that "interviewing them on their own territory, and allowing them to organize the context the way they wish, is the best strategy" [383, p. 150], particularly with regard to the interviewee's comfort, both physical and psychological. This approach has been followed by other cyber-security researchers, e.g. [97], and helps address, to some extent, the "artificiality" [383, p. 140] of interviews. Additionally, such an approach can be more convenient for participants with regard to securing a suitably quiet location to conduct an interview which will explore confidential topics. One particular limitation that was anticipated, particularly when interviewing CISOs, was that I considered it less likely that they would have a dedicated private office than board members, due to relative seniority, and, therefore, would have less control over the physical arrangement of the interview setting, e.g. arrangement of furniture. Although the interview was still 'on their turf', i.e., in a closed room in one of their office locations, it may not have put them entirely at ease in the same way that a dedicated personal office may do [363, p. 127]. It was certainly the case that none of the CISOs interviewed had their own dedicated office, however only two of the non-CISO participants benefited from such an arrangement, with the others being interviewed in undedicated meeting rooms.

I captured handwritten details of the physical security arrangements at the office locations where I interviewed participants. These ranged from the simple signing of a visitors' book through to 'airport-style' security, i.e., X-ray scanning of bags and the use of metal detectors before being provided access to the building. In some instances, the participant's own work areas were highly secure, some that were open only to the security team and included multiple identity verification steps and very thick steel doors, whereas in others the work area was an open plan office where the participant mixed with other, non-security, personnel. Aspects of this physical security, whether signing a book, X-ray scanning or working behind a steel door can be considered security theatre [664, 665]. In some cases, but not all, I was required to wear highly visible badges and/or lanyards that clearly marked me out to others in the office as a visitor, and an outsider.

One disadvantage of interviewing in the participant's 'space' was that it enabled or encouraged a power dynamic that put me in an unequal position. This may have encouraged behaviours, conscious or unconscious, in participants that affected their responses, e.g. what Goffman refers to as "information control" [363, p. 141], or may have limited the effectiveness of the interview process as a collaborative one [419, p. 18]. However, the role that I played as interviewer may have put me in a *more* powerful position than the participant [419, p. 41], although conversely my research could not complete without their participation and, therefore, it could be argued that the interviewee held the balance of power. It is conceivable that these different power dynamics cancelled each other out, and indeed such dynamics can be fluid throughout an interview [316, p. 60]. However, if there were an uneven weighting, arguably it was likely to be weighted in my favour and, outside of the interview, I clearly held the more powerful position in terms of the interpretation of the discussion [543, pp. 161-162].

I commenced each interview by using a standardised introduction, but this was not read "verbatim" [405, p. 495] in order to avoid the interview feeling too formal and potentially impacting upon rapport. I did, however, always clarify the anonymous nature of the interview and how interview data would be protected, which I describe in section 3.6. The introduction may also have supported sociologist Susan Ostrander's suggestions regarding taking control of the interview process [588, pp. 19-21]. I opened with a fairly straightforward question [316, p. 64], paraphrased from Hermanowicz [406, p. 645], namely 'could you describe your role for me please?', in order to enable both myself and the participant to relax into the interview, as well as providing a limited indication to me as to how responsive they were likely to be. I now describe further aspects of interview rapport.

Rapport and impression management

Hammersley and Atkinson, following Goffman [363, 364] describe how attention should be paid to "impression management", including dress [383, pp. 83-87]. My professional experience had identified benefits to rapport building through matching of dress and, therefore, I originally planned to ask CISOs on first contact what the dress code was at their organisation with the intention of adopting suitable dress to reflect this. When I began the actual data collection, however, the most convenient interviewing times for both participants and myself was during the working day and, as a result, I was interviewing participants on a day when I had either already been at, or was on my way back to, my own workplace. Therefore, there was little need (or opportunity) to change my dress and so I wore what I would usually wear, namely a suit but no tie. This was fortunate in that, unlike some other researchers, I had no need to have "upgraded my wardrobe" [235, p. 73] prior to commencing my interviews.

It may be beneficial to researchers to adopt a more deferential manner when interviewing elites, however, as someone who deals with elites in their own organisation on a regular basis, this is not something that I adopted, or felt was necessary, tending to approach such conversations on an equal footing, even though there is admittedly still a "power asymmetry" [316, p. 59]. Further, as a practicing CISO at a senior level in their own organisation, I am myself a member of an elite, or at least a sub-elite.

Management scholar Laura Empson describes situations in which elite research participants have expressed displeasure at “overly deferential” [316, p. 64] behaviour. Ostrander encourages researchers to assert their control over the situation when interviewing elites, which she found beneficial with regard to the overall quality of the interview [588, pp. 19-21] and, encouraging the use of feminist perspectives, Conti and O’Neil advise against “assuming a hierarchy of power of up or down” [235, p. 79] as this over-simplifies “the complex and multi-layered operations of power” [235, p. 80]. These aspects were reflected upon throughout the interviewing process and these reflections were captured in my fieldnotes. I did not identify any obvious conflict with regard to expected deference, although there were some clear displays of dominant body language from some participants, and, overall, I did not identify that any adjustments to my approach were required. It is also important to reflect again on the fact that I identify as male, and that most of my interviews involved participants who also identified this way; this will have had an influence on my own impression management, that of the participants, and my subsequent interpretation of these aspects. A detailed discussion on impression management and associated gender effects is considered to be outside the scope of this thesis, however, I feel that it is important to mention this potential bias.

Sociologist Michael Gilding describes how he “routinely prepared for interviews [with elites] by reading previous interviews in the print media” [361, p. 765]. I followed this approach for my interviews, using both online sources and print media, as I expected such pre-work to perhaps provide useful intelligence with which to build rapport or ‘break the ice’ at the start of interviews. Gilding “sometimes recognized well-practised narratives from . . . background research during interviews” [361, p. 765] and identified that it may be “difficult to draw respondents away from [these] narratives” [361, p. 767]. I considered that this could have undermined attempts to uncover insights from participants if they were practiced at repeating a particular viewpoint or story, however, I hoped that being able to identify such narratives would prompt me to probe further on these topics, supporting this type of interview preparation. I did not identify any such narratives during my interviews, possibly because my questioning was on topics that were unrelated to previous (public) interviews, which is perhaps indicative of the lack of detailed public discussion of cyber-security related themes in the media, or, more positively, that participants were being thoughtful about what we were discussing. However, I did detect what I considered to be other “well-practised narratives” [361, p. 765] from these participants in relation to questions relating to their roles and their business in general, which was not surprising as it is likely that they are often asked similar questions on a regular basis and have a ‘stock’ answer ready. Although narratives from public interviews were not identified, the interview pre-work was beneficial in identifying information that I could use to build rapport.[27]

3.4.4 Data capture and transcription

Interviews were recorded. Recognising that there are arguments against recording of interviews, e.g. [392, pp. 436-437], I considered the benefits to outweigh the disadvantages, particularly as I expected that recording would allow me to concentrate on being fully involved in the conversation rather than potentially being distracted by making notes.

Recordings were made using standalone digital recording devices,[28] one primary and another for redundancy purposes. A level check on each device was performed prior to commencing each interview. I recognised that audio recordings do not achieve total 'accuracy' as they do not capture important aspects of the interview such as body language, spatial information, including aspects of the physical interview location that provide context [419, p. 78], and affective states of the participants. These were, however, captured in a handwritten journal immediately following each interview, although affective state information was limited to what I could surmise from the other participant, as well as reflections on my own state.

Interviews were transcribed in verbatim "orthographic" [164, p. 88] form. Annotations were used to capture significant "conversational features" [284, p. 108] other than words, including gestures, which were considered as part of the analysis. Regardless of technique, transcripts are, by nature, "incomplete" [725, p. 33] [491, p. 71] and imperfect [284, p. 108], and, therefore, were not expected to objectively represent the interview scenario; they are "not just talk written down" [372, p. 172]. It is also recognised that transcription is a "theory laden" [491, p. 64] process which is "both interpretive and constructive" [491, p. 72]. This was reflected upon throughout analysis. Transcription occurred as soon as possible following each interview. I had intended to complete these within a day of the interview at most, but this was not achieved as my professional commitments meant that this was rarely possible. In most cases, I completed the transcription within three days of the interview. The longest time period between interview and completed transcription was 14 days[29] and the shortest was

[27] For example, in an interview with one non-CISO with whom I had had no previous interaction, mentioning a recent business transformation initiative that I had read about in the financial press enabled me to both build rapport and also to contextualise a question about changes to the organisation's cyber-security approach.

[28] Acknowledging that the use of recording devices is itself not without controversy, e.g. [578]. However, such debates are considered to be outside the scope of this thesis.

[29] This delay was due to a holiday.

zero days, i.e., transcription was completed on the same day as the interview. Table 3.3 below details the time elapsed between interview and transcription.

Table 3.3: Time elapsed between interview and transcription

Stage	*Participant*	*Time elapsed*
Pilot	Tórshavn CISO	2-3 days*
Pilot	Bogotá CISO	1 day
Pilot	Damascus CISO	1-4 days*
Phase 1	CISO1	0-1 days*
Phase 1	CISO2	1-2 days*
Phase 1	CISO3	4 days†
Phase 1	CISO4	3 days
Phase 1	CISO5	4 days
Phase 1	CEO1	14 days‡
Phase 1	NED1	13 days‡
Phase 1	CEO2	2 days
Phase 1	CISO6	2 days
Phase 1	CISO7	1-4 days*
Phase 1	CFO1	2 days
Phase 2	CISO8	0 days
Phase 2	CISO9	2 days
Phase 2	CISO10	0 days
Phase 2	CFO2	0-1 days*
Phase 2	CISO11	0-1 days*
Phase 2	CISO12	0-1 days*
Phase 2	CISO13	1 day
Phase 2	CIO1	0-1 days*
Phase 2	CISO14	1 day
Phase 2	CISO15	2 days

*Transcription completed over multiple days.

†Semi-automated transcription method commenced from this point forwards.

‡Both delays were due to the same holiday.

Interviews are shown in ascending date order. Note that pilot interviewees are referred to by an initial capital city-based pseudonymn, as explained in Section 3.6.

This table shows that, in the majority of cases, transcriptions were completed within three days of the interview. The majority of transcriptions were produced in a semi-automated manner, following [258]. I did not send any completed transcriptions to interviewees. Czarniawska cautions against this, highlighting that textual representations are distinct (and "distanciat[ed]" [256, p. 70]) from speech – they are "different forms of discourse" [256, p. 70] and, as a result, are treated differently. In addition to interviews, data was also collected through analysis of company annual reports. I had originally intended to supplement this analysis of public documentation with analysis of internal company documentation, particularly security policy documents. These documents were sought from CISO participants as part of the interviews, however, I did not manage to collect any examples despite initial agreements from participants to provide these. It is conceivable that the initial agreement to supply documentation was reconsidered on reflection, or that the effort required to 'sanitise' such documents was too great, or at least not enough of a high priority. Annual reports were, however, obtained for all cases. These data sources enabled triangulation of data, as well as offering additional insights for analysis. While the analysis of internal policy documents may have further enriched the analysis, I do not consider this to be greatly detrimental to the research, particularly as the primary analytic lenses deployed are not reliant on this additional data source. A research diary was maintained throughout the production of this thesis as well as a separate fieldnotes journal.[30]

The qualitative data underpinning this research is stored in Royal Holloway's Figshare research repository.[31] Given the sensitive nature of the data, and to avoid the risk of identification of either individuals or organisations, as I discuss further in section 3.6, access is restricted. However, in order to create public visibility of the research, a description of what is included in each dataset has been provided on Figshare.

Remote interviewing

The Covid-19 outbreak had an impact on my second phase of data collection. In mid-March 2020, a number of interviews were postponed due to participants working from home, either by choice or because their employers had enforced such a policy. At this early stage of the pandemic, one of my phase two participants offered to take part in what was intended to be an in-person interview by phone, however, I declined this offer, requesting a reschedule instead. I had conducted one of my pilot interviews through audio only and found it less effective than face-to-face interviews; not only was it more difficult to maintain rapport, it also appeared to lead to less reflexive answers. Other researchers have identified bias against the conducting of qualitative research by telephone [579] and while acknowledging that some have found this to be an effective method, e.g. [296, 324], there are others who may see it as second-rate [275, 405, 448]. The participant for the next scheduled phase two interview offered to host a videoconference instead of rearranging and, although I would have preferred a face-to-face meeting, I decided to take them up on their offer and explore the feasibility of conducting the interview in this manner.

[30] It is notable that the level of detail in these fieldnotes increased between the two phases of interviewing, with the fieldnotes for the second phase being richer in detail and more extensive, from one or two pages of handwritten A5 in the first phase to 3 or 4 pages in the second. As well as increasing in experience between phases, I was also increasing in reflexivity and capturing more of my emotional reactions as well as reflections on the participant's experience, which were considered to be "of analytic significance" [383, p. 192].

[31] Interview transcripts can be found at https://royalholloway.figshare.com/articles/dataset/Interview_transcripts_-_anonymised_-_Da_Silva_doctoral_research/19722109 and the annual reports at https://royalholloway.figshare.com/articles/dataset/Annual_reports_-_Da_Silva_doctoral_research/19738333.

As the Covid-19 situation developed, it became apparent that conducting future interviews via videoconference was going to become a necessity rather than an exception. Supervisory advice also pointed me down this route and therefore the bulk of my phase two interviews were conducted remotely, save for the two face-to-face interviews I had conducted in early March 2020, before widespread social distancing measures were implemented. I was also conscious that during this time, participants were likely to be busier than usual, and, therefore, may have had less time to support, or less interest in, my research than at other times. In particular, those in CISO roles were likely to be involved in crisis management activities[32] and such activities were cited by two participants as reasons why they needed to rearrange interviews. As well as being senior members of an organisation, CISOs are typically involved in business continuity activities due to the increased demands on technology required for remote working and the risks associated with both this and the nature of the crisis itself.[33] Although, time permitting, there could be a higher chance of securing an agreement to a video call than there was of arranging an in-person interview pre-crisis, I was also aware that potential participants may still be 'coming to terms' with the changed, and highly uncertain, situation and, therefore, may be less open to responding to the request. I was particularly conscious of the level of uncertainty and associated dread that participants may be experiencing, and how this may have impacted upon them psychologically [123, 447, 695], especially as we were still at an early stage of the crisis, and that it may have made sense to wait before contacting prospective interviewees [184].

In one instance, a video call was not possible for technical reasons and, therefore, this interview was conducted by audio-only over a mobile phone. One slight technical limitation of this was that the audio quality was reduced when compared to a computer-based solution. I was recording the audio using the devices described above and, comparing the recording of a audio emitted by a mobile phone's loudspeaker versus that from the computer's loudspeaker,[34] the former was noticeably less clear, with a narrower frequency range and greater sibilance. However, it was still distinct enough and usable. It was also fortunate that, for this call, there was a strong mobile network connection.

I was conscious of a potential limitation of remote interviewing in that there was a possibility for this mode to encourage me, whether consciously or not, to treat the interview more like an extraction of data. Sociologists David Johnson et al., in their

[32] As indeed I was.

[33] For example, targeted phishing campaigns specifically exploiting the Covid-19 situation [735].

[34] I maintained this method despite the technical possibility of recording the computer audio directly, as the resultant file would not be encrypted, which would not maintain my approach to securing interview data as described in Section 3.6.

analysis of a number of interviews conducted using differing modes, suggest this is more likely when interviews are conducted remotely [448]. In order to counteract this, I was mindful of making the interview as conversational as possible. This was something I had done in the face-to-face interviews already but I made more of a conscious effort to do this for the remote ones. This included ensuring I was providing clear facial cues to the participant where possible (a benefit of using video over solely audio) and ensuring I was not distracted during the interview.[35]

My fieldnotes for all the remote interviews comment on the difference in rapport versus a face-to-face mode. This could, of course, reflect an unconscious prejudice against this method, based on the normative primacy that face-to-face interviewing receives [579]. As accountancy scholars Muhammad Farooq and Charl de Villiers [324] point out, one omission from telephone interviewing in comparison to face-to-face interviewing is the visual context of the place in which the participant works. While videoconferencing obviously provides some visual information, this was, in my experience and admittedly very specific to this situation, not of their regular workplace. In addition, conducting the interviews by videoconference meant that I was not exposed to the wider experiential context of the overall workplace, including such factors as the security (and security theatre [664, 665]) of the site and my experiences of being an 'outsider' within their work environment. While this was not crucial for this research, it was something that I was noting as part of the interviews I had conducted to date and this additional data was providing an aspect of triangulation. Although being in what are often anonymous and nondescript meeting rooms provides limited environmental information [324], there can be rich contextual information arising from the experience of arriving and being present in another environment. Such experiences were clearly missed when conducting interviews remotely.

Given that both participants and myself were in our own homes for the remote interviews, it is possible that we were more at ease than we would have been if in our office environments [324]. Indeed, the flexibility offered by remote interviewing may provide participants with a greater overall ability to manage the interview setting [420, p. 116], which could result in positive affect. Qualitative researcher Amanda Holt highlights a potential benefit of remote interviews being less intrusive [420, p. 115], although this research was specific to disadvantaged communities, which is not how the elite or sub-elite participants in this study would be categorised. However, it is possible that some participants were emotionally more comfortable with this method for similar reasons.

[35] E.g. by ensuring I was in a room with a closed door and lowering the blind of the window that was in front of my desk.

Reflections on performance and performativity

I was 'performing' in the interviews and will have wanted to present myself in a particular way, notably as 'a researcher'. Interviews are an artificial situation in which I was playing a part, a part that I was unfamiliar with. As a result of its novelty, I was unsure what the 'right way' was to do it[36] and I wanted to make sure that I did it well, or at least well enough to be able to complete my study. This may further indicate that I have approached the interviews as a way of extracting data rather than as an "intersubjective" [254, p. 653] co-construction [185]. Through interviewing, I was playing a part that was different to my everyday activity and acting in a different way, occupying a different identity [185]. In addition, I was also directing the interaction, directing the performance in a way [648], for both myself and the other participants.

The participants were also performing, and some were more adept at this than others. Executives in particular, and especially CEOs, are highly likely to have been media trained [392, p. 433] and, therefore, be practiced in providing concise answers that give away no more information than necessary[37] and stick to 'facts' rather than reflections [717, pp. 73-74]. Media training is likely to result in executives being more careful in what they say and potentially in being less open, particularly if their media training has encouraged them to say what they want to say rather than clearly answering questions [717, p. 79].

From the perspective of performativity rather than performance, the statements made by participants helped to construct their identities, as did the statements I made as interviewer [102, 187]. During the interviews, the statements that we each made as part of the conversation served to co-construct our respective identities. By asking questions, I was constructing my identity as a researcher, a role that I am less experienced in occupying than that of 'CISO' or 'employee'. Communications scholar François Cooren uses a metaphor of ventriloquism to explore the use of speech as a way of representing something else, whether "principles, values, beliefs, ideas, ideologies, interests, organizations, etc." [237, p. 5]. In this way, the speech acts of the participants, including myself, both represented and helped to constitute our values and our identities, but also the identities of the organisations we represented. Through my own speech acts it could be argued that I was representing two organisations, i.e., the University in my role as a researcher, and my employer. Even though I was not there on behalf of my employer, I carried that identity as well, and, as reflected upon

[36] This sense of there being a 'right way' may be as a result of positivist conditioning arising from my background, even though I know there is no objective 'right way' – although I do feel there is probably a 'wrong way'.

[37] Which can be crucial with respect to cyber security [30].

above, this may have facilitated both access and rapport. Furthermore, I may have been representing a less formal organisation, namely the profession of cyber security, as established by industry certifications, e.g. [18, 8]. This professional nature establishes the 'expert' nature of the identity, and, as Cooren notes, the speech acts of an expert are "expressing . . . his/her expertise . . . [and] aspects of realities that he/she is supposed to represent" [237, p. 13]. These speech acts also set boundaries in terms of "rules, norms" [237, p. 5] and represent "ideologies" [237, p. 11], as I explore further in the following chapters. Speech acts of elites, and sub-elites, reinforce and constitute the power of the ruling classes; other voices "*speak through us*" [237, p. 12] (italics in original). These 'other voices' will have been present both in my speech as the interviewer and that of the interviewees. These reflections led me to consider the use of performative or constitutive aspects of speech as an analytical lens, and indeed the use of 'performativity' itself as a code.

3.5 Analysis

In this section, I describe the approach I took to analyse the various data sources. The analysis stages involved an ongoing process of "constant comparison" [561, p. 293], a concept borrowed from grounded theory, whereby "emerging data, extant data, and extant literature" [561, p. 294], as well as my own professional knowledge and self-reflection, were iterated and synthesised. I approached the analysis in a non-formulaic manner, combining multiple techniques in a 'cookbook' manner, as recommended by qualitative researcher Johnny Saldaña [653], and many others, e.g. [211, 362], although I acknowledge that different opinions exist regarding the mixing of techniques, e.g. [193].

In Chapters 4, 5 and 6, the data is interpreted through different analytical lenses. Methodologically, an 'analytic lens' can be understood as the application of a concept, or group of concepts, to data in order to derive meaning and to delve beneath a surface-level understanding. It allows a framing of data, through which the data can be seen in a particular way, enabling a "richer interpretation" [749, p. 9]. Such an approach has been utilised by others e.g. [500, 749], including those who have employed thematic analysis e.g. [749], a method I also follow, as described below.[38]

The use of these lenses, which are drawn from multiple disciplines, was entirely influenced by, and grounded in, the data. Throughout the process of inductive analysis, coding, and subsequent thematic analysis, as described below, themes were identified that led me to perform 'spikes'[39] of further literature-based research. This additional

[38] This includes the specific use of identity as a lens [500] as adopted in Chapter 4. Note that this reference was not discovered until after identity had been chosen as a lens.

[39] A term borrowed from the field of agile software development that refers to an unplanned, short-

research was then added to the literature that had already been studied in order to develop the perspectives that were eventually chosen as the most useful, and interesting, lenses through which to interpret the data. Therefore, the multi-disciplinary approach that has been followed in this thesis was not determined *a priori*, and it would be incorrect to claim that specific multi-disciplinary methods were adopted.[40] Rather, the multiplicity of disciplines that have been applied emerged from the analysis process, grounded in the data. Thematic analysis was the primary method adopted and, as Braun and Clarke describe, it is "theoretically flexible" and although it may not have the "kudos" of "supposedly more sophisticated" methods, that may themselves give rise to "methodolatry", it can still be rigorously applied and generate valuable insights [164, p. 97]. The latter may be "unanticipated" [164, p. 97], a particular benefit of thematic analysis which seems appropriate to this thesis.

3.5.1 Analysis of interview data

Transcripts were coded using NVivo 12 [22].[41] Coding was performed inductively, however, two specific codes were used that I identified from my literature review. These were "DQ ... [for] *demonstrative quote* ... [and] NQ ... [for] *narrative quote*" [484, p. 354] (italics in original), as used by qualitative researcher Glen Kreiner. Following Kreiner's approach, these were "double coded along with the code(s) [they] exemplif[y]" [484, p. 354]. Documentation, including notes from field journaling, were also coded using the same approach and analysed in comparison with interview data. The coding scheme is detailed in Appendix F along with "illustrative examples" [669, p. 155], as encouraged by Seale. Consideration was given to the use of gerunds in coding, following sociologist Kathy Charmaz [209, p. 245], as well as aspects of "[a]voiding accounts" as discussed by Czarniawska [256, pp. 54-55]. It was also recognised that the effectiveness of coding could be partially limited due to there being only a single researcher involved in this procedure, which may introduce consistency errors [669, p. 156], but is unavoidable in a PhD thesis.

Following two cycles of inductive coding of the transcripts, I applied a deductive approach in order to categorise and rationalise the codes. As with all forms of analysis, whether qualitative or quantitative, prior knowledge influences the process. Therefore, although no attempt was deliberately made to find indications of certain concepts in the data, it is important to acknowledge that my existing knowledge may have affected the coding.

term and highly-concentrated burst of activity focused on a particular topic e.g. [417, 528].

[40] Indeed, this work may not be considered multi-disciplinary in the sense of integrating perspectives from both social and natural science, as is the case with much multi-disciplinary research e.g. [738, 784].

[41] The NVivo project was password protected using a strong password.

A mixture of coding types were used. I began coding after reviewing a number of texts, e.g. [63, 484], but predominantly following Braun and Clarke [164, 165, 166]. During my analysis of the pilot phase data, I experienced problems with my first attempts at coding and analysis. A conversation with my supervisor pointed me towards a more comprehensive text on coding from Saldaña [653]. This was very useful, not just in helping me to distinguish between codes, categories and themes but also to help me reflect on my coding approach and provide useful preparation for analysis. After reading Saldaña, it was apparent that my analysis of the pilot data had used simple descriptive codes which didn't tell me much about the data, a trap that Saldaña describes [653, pp. 76-77]. The experience of coding and analysing the pilot data taught me a great deal about this process and in particular exposed me to in-vivo, process, versus, and dramaturgical coding, which were all used extensively in my analysis of the full data corpus. Analytic memos were produced, following both Saldaña and others, e.g. [210, 484] which were based on the coded data, fieldnotes and research diary. These memos were also subsequently coded using the same method.

Saldaña's prompts regarding analytic memos [653, pp. 46-53] were particularly useful and resulted in what I think have been interesting insights that may not have arisen otherwise. These memos aided reflexivity [181, p. 245] and ensured ideas were not lost [178, p. 83], as well as providing an opportunity for me to reflect upon the influence that I may have had on the data, as encouraged by Hammersley and Atkinson [383, p. 223]. Negative instances were also actively sought, as encouraged by a number of researchers as a quality improvement measure, e.g. [669, pp. 40, 75] [119, p. 513]. Alvesson's metaphorical framework [83] was a particular influence on my analysis, which I used primarily as a resource to test my critical thinking.

Following coding, I thematically analysed the data following the guidance provided by Braun and Clarke [164, 165, 166]. My approach made extensive use of diagramming[42] to explore relationships between codes and categories, combining several methods from Saldaña [653] including category relationship and operational model diagrams. I also produced code charts, as described by Saldaña [653, pp. 229-230]. These diagrams and charts were used to develop and explore themes based on the data, following Braun and Clarke [164, 165, 166]. As they note, themes are not discovered, they are "actively crafted by the researcher" [165, p. 740]. It is also important to note that thematic analysis is both inductive and deductive [167], and that themes are patterns, rather than groupings of categories, which may overlap [164, 167].

The thematic analysis was performed on the core data corpus of interview data as well as associated fieldnotes and research diary entries. This was supported throughout

[42] See Appendix B for examples.

by both analysis of existing analytic memos and generation of new memos. This was particularly important due to thematic analysis requiring "active, creative and reflexive researcher engagement" [165, p. 741], and analytic memoing was key in achieving, and capturing, this. Figure 3.4 diagrammatically summarises the output of this thematic analysis.

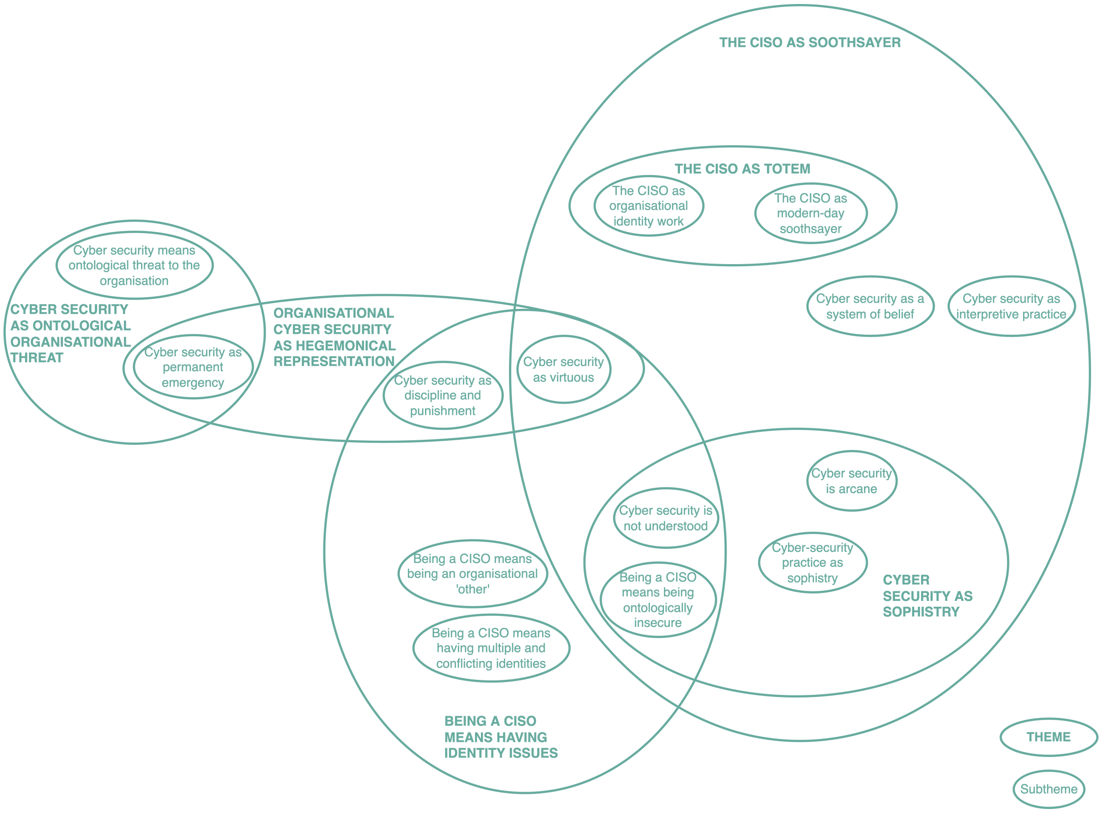

THE CISO AS SOOTHSAYER
THE CISO AS TOTEM
The CISO as organisational identity work
The CISO as modern-day soothsayer
Cyber security means ontological threat to the organisation
CYBER SECURITY AS ONTOLOGICAL ORGANISATIONAL THREAT
Cyber security as permanent emergency
ORGANISATIONAL CYBER SECURITY AS HEGEMONICAL REPRESENTATION
Cyber security as discipline and punishment
Cyber security as virtuous
Cyber security as a system of belief
Cyber security as interpretive practice
Cyber security is arcane
Cyber security is not understood
Cyber-security practice as sophistry
Being a CISO means being ontologically insecure
CYBER SECURITY AS SOPHISTRY
Being a CISO means being an organisational 'other'
Being a CISO means having multiple and conflicting identities
BEING A CISO MEANS HAVING IDENTITY ISSUES
THEME
Subtheme

Figure 3.4: High-level diagrammatic summary of interview data thematic analysis

This figure provides a high-level summary of the thematic analysis performed on the interview data.

3.5.2 Analysis of annual report data

A similar method, i.e., coding, was used to analyse annual reports. However, as this was performed subsequent to the interview coding cycles, coding became more deductive, as codes and concepts determined from the inductive coding of the interview transcripts were, consciously and unconsciously, reused. Two cycles of coding were completed and, as with the interview data, analytic memos were produced throughout and these were also subsequently coded.

Again, a thematic analysis was performed, following the same approach as for the interview data, and including associated research diary entries. Existing analytic memos were included in this process and new memos were generated. Figure 3.5 summarises the output of this activity. I had become more familiar with the process of coding and the use of NVivo and, although the annual report documents were much larger than the transcripts, and took longer to code as a result, the content was less rich. From coding the interview data, I had become more experienced at focusing on concepts rather than descriptions, and at challenging myself to look beyond the words on the page.[43] However, this was more difficult with these documents, which, as with most annual reports, were predominantly descriptive in nature. Certain concepts were applied that related to, or matched, concepts used in analysis of the interview data.[44] Analysis of the annual reports was also influenced by the various literature 'spikes' that I conducted during the analysis of the interview data. These involved delving into literature that I had not previously identified, prompted by themes and concepts relating to the data. As a result, this additional knowledge will have affected my analytical decisions, possibly with increased influence due to the relative proximity of this reading. At this stage, I had also become more experienced[45] with "craft[ing]", rather than "discover[ing]" themes [165, p. 740].

[43] I also considered the imagery included in the annual reports, although this was not a focus of the thesis.

[44] Such as identity, although it did feel coincidental that identity themes stood out, and, at the same time, unsurprising given the public nature and intended audience of company annual reports.

[45] And indeed, comfortable.

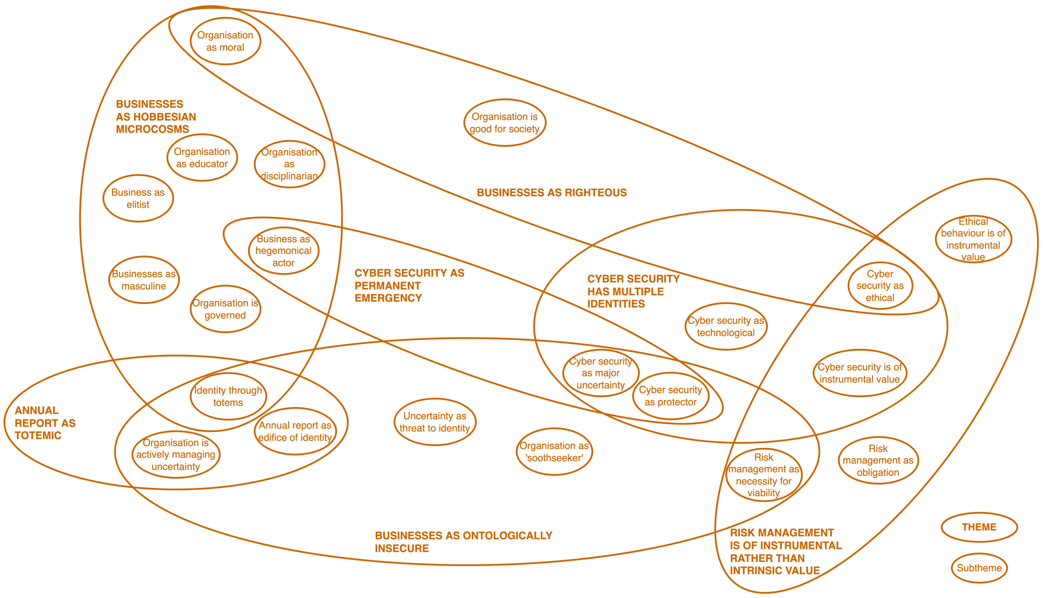

Organisation as moral
BUSINESSES AS HOBBESIAN MICROCOSMS
Organisation is good for society
Organisation as educator
Organisation as disciplinarian
Business as elitist
BUSINESSES AS RIGHTEOUS
Ethical behaviour is of instrumental value
Business as hegemonical actor
CYBER SECURITY AS PERMANENT EMERGENCY
CYBER SECURITY HAS MULTIPLE IDENTITIES
Cyber security as ethical
Businesses as masculine
Organisation is governed
Cyber security as technological
Cyber security as major uncertainty
Cyber security is of instrumental value
Identity through totems
Cyber security as protector
ANNUAL REPORT AS TOTEMIC
Uncertainty as threat to identity
Annual report as edifice of identity
Organisation is actively managing uncertainty
Organisation as 'soothseeker'
Risk management as necessity for viability
Risk management as obligation
THEME
BUSINESSES AS ONTOLOGICALLY INSECURE
RISK MANAGEMENT IS OF INSTRUMENTAL RATHER THAN INTRINSIC VALUE
Subtheme

Figure 3.5: High level diagrammatic summary of annual report thematic analysis

This figure provides a high level summary of the thematic analysis performed on the annual report data.

3.5.3 Meta-thematic analysis

Next, a meta-thematic analysis was performed in order to explore connections, as well as a means of rationalising what was a broad set of initial themes. This method was particularly beneficial in refining the analysis and connecting the different theoretical insights I had developed in my analytic memos. The meta-themes synthesised through this process form the foundation of Chapters 4, 5 and 6. A diagrammatic summary of the meta-analysis is shown in Figure 3.6, with more detailed diagrams contributing to its development included in Appendix B.

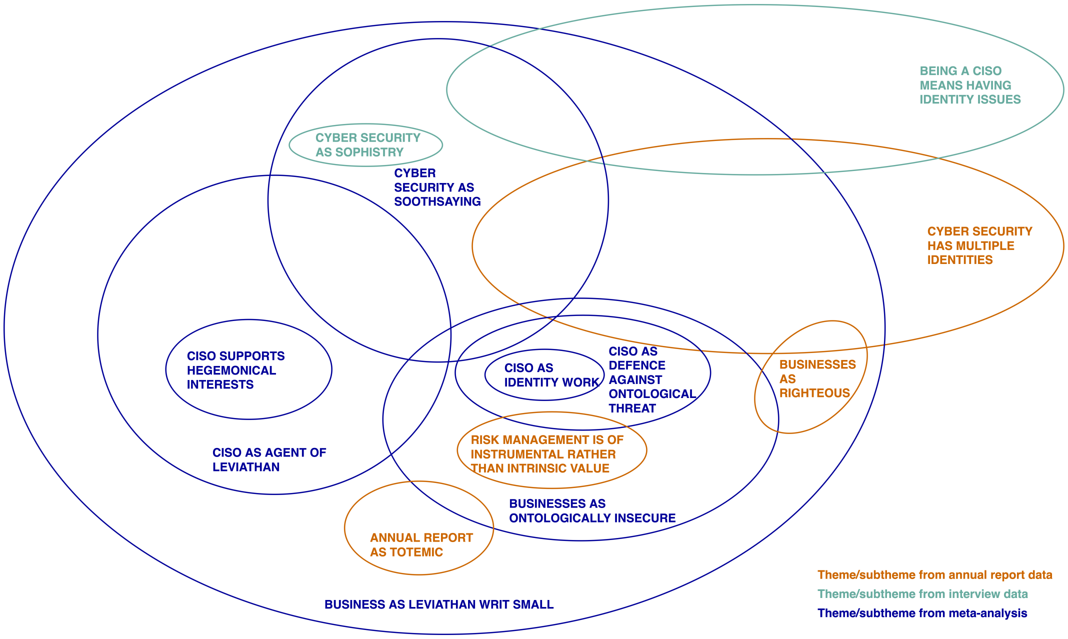

BEING A CISO MEANS HAVING IDENTITY ISSUES
CYBER SECURITY AS SOPHISTRY
CYBER SECURITY AS SOOTHSAYING
CYBER SECURITY HAS MULTIPLE IDENTITIES
CISO SUPPORTS HEGEMONICAL INTERESTS
CISO AS IDENTITY WORK
CISO AS DEFENCE AGAINST ONTOLOGICAL THREAT
BUSINESSES AS RIGHTEOUS
RISK MANAGEMENT IS OF INSTRUMENTAL RATHER THAN INTRINSIC VALUE
CISO AS AGENT OF LEVIATHAN
BUSINESSES AS ONTOLOGICALLY INSECURE
ANNUAL REPORT AS TOTEMIC
BUSINESS AS LEVIATHAN WRIT SMALL
Theme/subtheme from annual report data
Theme/subtheme from interview data
Theme/subtheme from meta-analysis

Figure 3.6: High level diagrammatic summary of meta-analysis

This figure provides a high level summary of the meta-thematic analysis, including themes and subthemes that were retained from the thematic analyses of the interview and annual report data.

3.6 Ethical considerations

I conducted an ethical self-assessment before conducting interviews or engaging with participants and agreed my approach with my supervisor before completing the University's self-certification process. I observed ethical principles throughout the research project and maintained compliance with a pre-defined approach to data capture and maintenance as described below. Participant information sheets and consent forms[46] were emailed to participants two working days before each interview. Consent forms were physically signed by both myself and the participant prior to each in-person interview and securely stored[47] at my base location. For those interviews conducted remotely, consent was sought via email and either an electronically scanned physically signed form[48] or an email message confirming consent were received. These docu-

[46] See Appendix D.

[47] In a locked safe.

[48] Subsequently also physically signed by me.

ments were securely stored, in a locked safe and, in the case of the email messages, on encrypted media.

The devices used to record the interviews encrypted recordings at point of capture.[49] While modern smartphones have the capability to record audio, a separate device provided greater security[50] over what were confidential recordings. It was made clear to participants that recording of interviews was solely to aid the production of a transcript and that, once this was complete, the recordings would not be retained [405, p. 496].[51] This conversation also enabled me to explain the specifically encrypted nature of the equipment that I was using and functioned as an "ice-breaker" [798, p. 270], a benefit identified by previous researchers, e.g. [405, p. 497]. I had anticipated the possibility of a discussion regarding the encrypted device as being useful in building rapport with the CISO participants in particular, given they were likely to share a professional interest in encryption and data security, but I found it was also useful in building rapport with the elite participants, possibly because they found it reassuring that the security of the interview was being carefully considered, and possibly because it helped put me at ease as it was something I could speak about with relative authority, given my professional role. Indeed, it may have helped cement the impression they had of me as a specialist, demonstrate credibility, and could also have aided their ability to categorise me [363, p. 36]. Furthermore, as a "prop" [363, p. 32], which allowed me to a certain extent, to "control ... the setting" [363, p. 98], the device may have supported my identity as a researcher. Therefore, the combined nature of a recording device that had a data security element enabled a dual identity that I wanted to achieve with all participants, namely to be seen as both a cyber-security professional and a researcher.

The recordings were transferred to encrypted storage at my base location,[52] with an additional encrypted backup performed using a strong password [33, 437] and stored in a locked safe, following which recordings were deleted from the portable recording device. Backup recordings were deleted once the effective capture on the primary recording device was verified. Once interviews were transcribed (verbatim [669, p. 148]) and anonymised, and those transcriptions were also backed up, all recordings were securely deleted from both primary and backup storage. Annual reports, as downloaded from

[49] Olympus DS7000 as the primary device, with an Olympus DS5000 as a backup.

[50] For example, a mobile phone is much more likely to be lost or stolen due to its frequent use in multiple settings (and, in the case of theft, its inherent value) versus a digital voice recorder.

[51] No participants objected to the use of the recording devices; the closest to an objection I got was "I suppose that's OK" when I asked if I could record the interview. This was from a non-CISO participant.

[52] The University's cloud storage option (Microsoft OneDrive) was not utilised for storage or backup of recordings due to its weak security – for example, at the time of conducting the interview there was no multi-factor authentication in use, which increases the risk of data leakage. OneDrive was, however, used as a backup for the completed, anonymised, transcripts.

each company's public website at the time of the interviews, were securely stored in the same manner as the transcripts.

All interview data was anonymised. Challenges regarding effective anonymisation of qualitative interview data have been identified by a number of researchers, e.g. [658, 667, 765, 783]. Communications scholar Craig Scott describes how "anonymity may be thought of as existing on a continuum from highly anonymous to highly identified" [667, p. 255] and others have noted that "guaranteeing complete anonymity to participants can be an 'unachievable goal' in qualitative research" [658, p. 617]. My efforts at anonymisation involved the use of pseudonyms for participants. Each organisation was referred to by a national capital city,[53] assigned at random using a spreadsheet.[54] Participants were referred to by that capital city and their role, e.g. London CISO. Alongside this mapping of participant to capital city and role, the company that they represented and the industry sector (using both ICB industry and ICB 'super-sector' [5, 48]) applicable to that company were also captured. This spreadsheet was encrypted using a strong password and stored on an encrypted storage medium that only I could access. Participants were referred to only by their pseudonym from the point of transcription forwards. I redacted any sensitive or potentially identifiable information during transcription. Effective judgement in this regard this was dependent upon knowledge of what could be considered sensitive, as highlighted by healthcare researchers Benjamin Saunders et al. [658, p. 629], who also raise the importance of reflexivity regarding this throughout the interview process [658, p. 628]. My (ongoing) professional experience facilitated this and I was conscious throughout transcription and analysis of the decisions I was making with respect to redaction. Reflections on these decisions were captured in my analytic memos.

Although participants will not be directly identifiable to readers, there is a risk of identification through what sociologist Martin Tolich refers to as "internal confidentiality" [739, p. 101] and health researcher Karen Kaiser calls "[d]eductive disclosure" [457, p. 1632]. This relates to the potential for members of a group to identify each other through particular knowledge that they hold, which could include personal knowledge of specific events discussed or even turn of phrase. The existence of in-groups within this research has already been discussed, particularly the active and close-knit community of CISOs,[55] and, therefore, it is possible that anonymisation may not be effective where direct quotations are used. Saunders et al. [658, p. 619] suggest this may be exacerbated by the use of snowball sampling, as used in this research. Further, any narratives used by participants could have been replicated previously, or may be

[53] The list of cities was taken from Wikipedia [54], comprising 260 entries at time of compilation.

[54] Using the Microsoft Excel RANDBETWEEN functionality.

[55] The "small population" problem referred to by Saunders et al. [658, p. 619].

so in future, in attributed form such as media interviews [659, p. 128]. This was considered to be a higher risk with non-CISOs who could reasonably be expected to have a higher media profile, although CISOs are also regular interview subjects in the specialist press. In addition, participants could have chosen to share narratives or other comments via social media [659]. Verbatim quotations, however, are seen as a key component of qualitative research texts [383, p. 182], particularly in supporting theory development [362, 561] and in demonstrating the appropriate quality of the research [326, 669]. Therefore, I saw these as a crucial inclusion in this thesis, despite alternatives being explored by other researchers, e.g. [531].[56] In order to address the potential for identification through direct quotations, a number of mitigating steps were performed. First, although public documents, i.e., company annual reports, were used as data sources, no direct quotations from these sources have been used.[57] Second, this risk of identification was explicitly articulated in the Participant Information Sheet (see Appendix D) provided in advance of each interview. Additionally, participants were asked explicitly at the end of each interview whether they consented to anonymised quotations being included in the final thesis, acknowledging the theoretical potential for them to be identified by them in the event that they repeat (or have repeated) any narratives quoted. This aligns with Kaiser's recommendations regarding "extend[ing] confidentiality conversations beyond the signing of the consent form" [457, p. 1638]. Third, where I deemed it relevant, and where possible, multiple pseudonyms have been used for attribution of quotes [659, p. 131]. Notably, all of the participants agreed to the use of verbatim quotations, although two participants did request upfront visibility of any of their quotations that were used. I agreed to and have complied with these requests.

3.7 Summary

This chapter has described the methodology followed in developing this thesis. It has covered my epistemological position, my positionality as a researcher and the methods followed in gathering and analysing data. In the following three chapters, I present my interpretation of the findings that arose from these activities.

The themes developed through the meta-analysis described in Section 3.5.3 form the basis of the three findings chapters that follow. In each of these chapters, these themes, and the data associated with them, are brought into conversation with the literature.

[56] Although it is also possible that the 'fabrication' method suggested in this reference did not resonate with me due to my background and a latent positivist bias, as discussed earlier.

[57] Such documents are easily searchable, and, therefore, direct quotations from them would allow identification of both organisations and participants.

In so doing, insights and provocations are achieved that advance the understanding of the CISO role and the context in which they operate. Each chapter begins with a clear presentation of the themes that are discussed within each section, which maps back to the diagram shown in Figure 3.6.

Chapter 4

Identity work

This is one of three chapters that interpret the findings through multiple analytical lenses. This chapter focuses on identity work.

4.1 Introduction

The chapter is structured into five main sections. First, in Section 4.2, I explore how cyber security related to the identities of the organisations in this study, including the identity work that they performed. Next, in Section 4.3, I discuss the identity work performed by CISOs, including the motivation behind such work. In Section 4.4, I develop moral and mystical associations of cyber security that were present in the data before discussing the rewards that accrue from the identity work in Section 4.5. I then employ a metaphor of soothsaying in Section 4.6 as a conceptual framework that allows a deeper understanding of the purpose of the CISO, whether explicit or implicit, than has been achieved by previous literature. This provokes further discussion and reflexivity for businesses, cyber-security practitioners and researchers. Finally, I summarise my contributions in Section 4.7. Throughout, I present key additional literature that supports the conceptual grounding for the discussion, building on that already introduced in Chapter 2 and bringing this into conversation with the findings. The literature is also employed to support the interpretation of the data, for example, where other researchers have reached a similar conclusion or applied a concept in a similar manner, or where I myself borrow a concept or phrasing from previous work. Quotations from participants[1] and paraphrases from annual reports[2] are included where relevant to exemplify or support a theme or interpretation from the analysis.

[1] Indicated by double quotation marks.

[2] Indicated by single quotation marks.

4.1.1 Why identity work?

In this chapter, I apply a lens of identity work to the findings from this research. This is due to the prevalence of identity-related themes that were identified during the analysis of the data. This study has been reflexive in nature, in that through the analysis, themes that were identified were then subsequently subjected to further analysis, which includes bringing them into conversation with the literature relating to those themes. Figure 4.1 highlights the relevant themes from the meta-analysis mentioned in Chapter 3 that are predominantly covered in this chapter. This diagram, which is based on Figure 3.6 in Chapter 3, is intended to provide context and aid navigation through the thesis.[3]

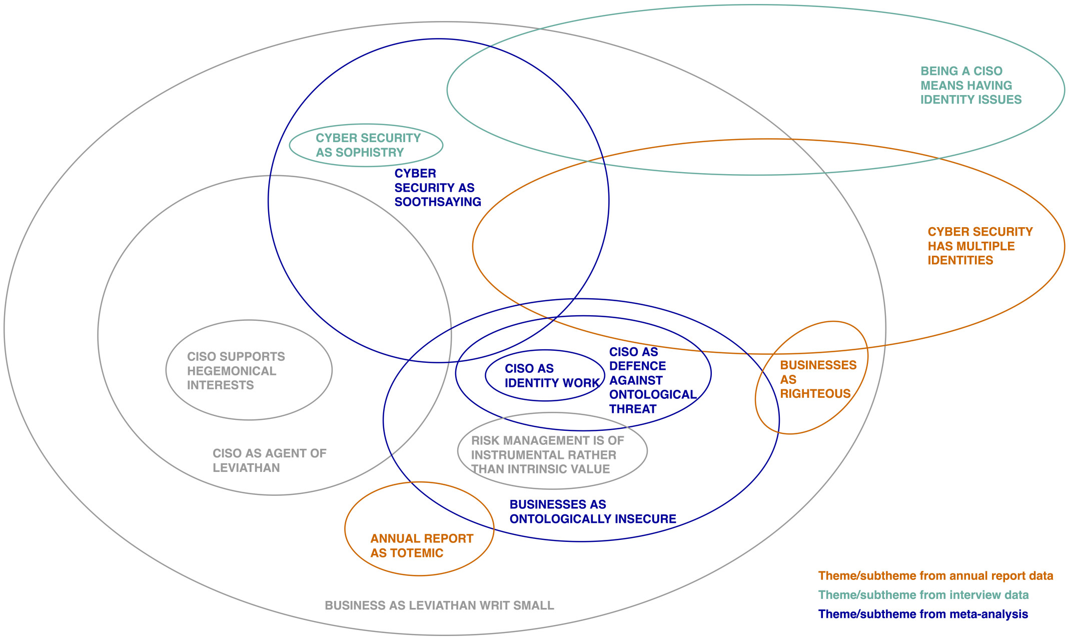

BEING A CISO MEANS HAVING IDENTITY ISSUES
CYBER SECURITY AS SOPHISTRY
CYBER SECURITY AS SOOTHSAYING
CYBER SECURITY HAS MULTIPLE IDENTITIES
CISO SUPPORTS HEGEMONICAL INTERESTS
CISO AS IDENTITY WORK
CISO AS DEFENCE AGAINST ONTOLOGICAL THREAT
BUSINESSES AS RIGHTEOUS
RISK MANAGEMENT IS OF INSTRUMENTAL RATHER THAN INTRINSIC VALUE
CISO AS AGENT OF LEVIATHAN
BUSINESSES AS ONTOLOGICALLY INSECURE
ANNUAL REPORT AS TOTEMIC
BUSINESS AS LEVIATHAN WRIT SMALL
Theme/subtheme from annual report data
Theme/subtheme from interview data
Theme/subtheme from meta-analysis

Figure 4.1: Meta-analytic themes covered in this chapter. Themes not covered in detail are greyed out.

This diagram demonstrates the multiplicity of identity-related themes that were present in the data, including those that refer to the closely-related concept of ontological security. The identification of these themes inspired the use of identity work as an analytical lens and map onto the sections in this chapter as shown in Table 4.1. As can be seen from the diagram, identity-related themes were present in the analysis of both the annual report data and the interview data, with multiple categories and

[3] Similar diagrams are presented in the two further discussion chapters that follow.

codes of data contributing to those themes. This motivated an in-depth exploration of the literature relating to identity, which resulted in the subsequent development of broader themes of identity during the meta-analysis, and the application of a lens of identity work. Hence, this chapter discusses the findings through this lens, bringing into conversation the literature on this topic that was discussed in Chapter 2.

Table 4.1: Mapping of meta-themes to sections in this chapter

Section	**Meta-themes**
Section 4.2	Businesses as righteous CISO as identity work CISO as defence against ontological threat Businesses as ontologically insecure Annual report as totemic
Section 4.3	Being a CISO means having identity issues Cyber security has multiple identities CISO as identity work CISO as defence against ontological threat
Section 4.4	Businesses as righteous CISO as identity work Risk management is of instrumental rather than intrinsic value
Section 4.5	Being a CISO means having identity issues Cyber security has multiple identities Cyber security as soothsaying Cyber security as sophistry
Section 4.6	CISO as identity work Cyber security as soothsaying Cyber security as sophistry

A summary of the themes that are represented in each of the core sections of this chapter.

Table 4.1 further demonstrates the reflexive nature of this work. This shows that the themes developed from the analysis are each reflected throughout the different sections of this chapter, where they are discussed in the context of existing theories of identity and identity work.

As well as providing a useful theoretical perspective with which to unpack and derive meaning from my findings, identity work also provides a valuable additional benefit in encouraging reflexivity for both participants and researchers, as identified by Cunliffe, particularly as such reflexivity may be rare [253, p. 368]. Reflexivity offers a means for participants to challenge or modify their identities through different discursive means. Therefore, an identity work perspective can have more value, and more impact, than simply being an analytic lens. It prompts a reflexive engagement with the identity of self (and other) that enables individuals to consider that aspects of their discourse, and possibly behaviour, can be modified in order to achieve different outcomes.

4.2 Cyber security and organisational identity

In this section, I discuss how cyber security related to organisational identity for the businesses represented in this study. This includes the identity work that they performed in response to perceived identity threats that related to cyber security, as well as identity work that indexed moral aspects of cyber security.

4.2.1 Cyber security as an identity threat

Cyber security, or at least the risk of a cyber-security incident,[4] was considered by these organisations to be threatening to their identity. A strong sense of cyber-security threat as being existential came through in the analysis of the data. For CISO7, cyber-security incidents were the "biggest risk to the viability of the organisation", and words such as "catastrophe" (CISO11), "debilitating" (CISO4) and "disastrous" (CISO9) were commonly used in reference to cyber-security events. CISO5 stated that "[in] the worst case ... your business is over".

Non-CISO participants in particular considered a cyber-security incident to be a survival-level threat to the organisation. For example, CEO1 described cyber risk as "potentially catastrophic", stating that "it could destroy the business". NED1 believed that a major cyber-security incident would "bring the company to its knees ... [and] drive us to bankruptcy". CFO1 positioned the reason for addressing cyber-security risk as "[because] you want to be able to continue in business". Not all non-CISO participants agreed however, with CEO2 stating that although a cyber-security incident would be "incredibly disruptive" and would require "alternative ways of operating", they did not consider it as something that could put them out of business.

The majority of the annual reports acknowledged cyber-security incidents as being threatening to the business's viability, which included articulating the risk of data breaches and other security events, as well as system failures and regulatory actions, as existential. Associated risks of operational impairment were mentioned, as well as loss of revenue and impacts to reputation, either directly or indirectly, e.g. through regulatory action, including fines. These businesses needed to be 'protected' and 'defended' against cyber-security threats in order to meet obligations, deliver their strategies, and maintain trust. Trust was articulated across the annual reports as a significant factor in

[4] Considered to be an event that negatively impacted the organisation which was related to an aspect of cyber security, typically either the loss of data, unauthorised access to systems or infection by malicious software.

organisational identity, from the perspective of customers, suppliers and partners, with cyber security being a common component of this. Trust in the organisation was also articulated as an existential concern, along with reputation.[5] In the annual reports, cyber security was positioned by many organisations as a continuum, necessitating a prioritised and risk-based approach. Some organisations suggested that they were concerned primarily with cyber-security risks that were 'significant', but neither the criteria for reaching that threshold nor the process followed in determining whether it had been reached were described. However, in some cases, the number of 'significant' cyber-security risks that had materialised was the sole cyber-security measurement referred to in the annual reports. All organisations mentioned the existence of cyber-security risk and, to a greater or lesser extent, how the organisation mitigated that risk.

Whether cyber-security threat was considered to be existential appeared to be related to the industry that the business operated within. For example, one participant within the real-estate industry described how it was "quite difficult to steal a building" and how cyber security was "not a big issue [here]".[6] A sizeable number of participants, both CISO and non-CISO, made reference to the banking industry as an implied 'gold standard' with regard to cyber security, with 'we're not a bank' being prevalent throughout the data. Typically this was used from the perspective of arguing for a looser set of security controls and may represent a naïve perspective of those who work outside of the banking industry. One participant who did work for a bank indicated that this characterisation may be misjudged, which I explore in more detail in Section 4.2.2.

Cyber-security practice as protection

Many participants described cyber-security practice in their organisations as a form of protection, of being kept "safe" (NED1).[7] For CFO2, cyber-security practice was "[a] framework … to protect the company", which they defined as "the protection of company assets in the online world akin to the protection of physical assets in the real world". A number of participants made reference to this activity as protecting the organisation's "crown jewels" (CISO3, CISO4, CISO14, CISO15, CFO2). Other objects of protection included "our brand … our share price and our shareholders … the good name that we've got" (CISO14) and "reputation" (CISO4).

[5] Trust and reputation were explicitly linked in a number of annual reports. As well as cyber security, reputational impacts were also articulated in relation to other risks, including health and safety, legal compliance and ethical behaviour.

[6] Not attributed to limit the risk of identification.

[7] CISOs were characterised, by both themselves and their stakeholders, as 'protectors', as I discuss in Section 4.3.2.

For CEO1, "the purpose of [the cyber-security function] is to protect our networks and data from intrusion and from damage" and this sense of protecting an 'inside' from an 'outside' was particularly common. This included "shut[ting] the doors" (CFO1), "stop[ping] people getting through the door" (CISO7) and "protect[ing] our perimeter" (CISO4). This involved using "protective barriers" (CFO2), with "layered defences" (CISO14) like "an onion" (CISO5) in order to "stop it [i.e., a threat] from getting in in the first place" (CISO11). The organisation needed to be "sound at the core" (CFO1) from a cyber-security perspective. However, CISO9 suggested that such a model was outdated, describing how

> "before you had this kind of idea of a bastion ... a kind of a castle with a moat around it, all your data was inside and ... the bad guys had to get in, whereas now ... bad guys don't need to get into your environment anymore".

As well as protection from something fearful, as described in this section, CISO9's comment also indexes a sense of morality in connection with cyber security. This conception was common, as I explore further in Section 4.4.

In order to achieve the level of protection they sought, organisations implemented different controls, including education, policy and technological controls. CFO2 observed that the controls in their organisation were "very tight and, therefore, likelihood [of a cyber-security incident] is low" and NED1 expected controls to "get tighter and tighter". CEO1 also linked this to fear, stating that "the more that we go and scare ourselves ... the more the organization becomes willing to tolerate some inconvenience in what it does ... because people become safer". This balance between security and convenience was also indicated by CISO9 who expressed a need for "making sure that security is applied and usable" and NED1 who explained that flexible working makes cyber security "tougher". Similarly, there was a perceived dualism between security and freedom indicated. CISO4 described how "there's gotta be an amount of, you know, disruption that is necessary in order to do the right thing". CISO8 alluded to the potentially problematic nature of achieving "a balance between inspection and surveillance" and how this may impact upon "free speech", with different views held by their stakeholders ranging from "absolutely no problem [with monitoring]" to monitoring of activity being "abhorrent". There were a number of references made in the interview data to the monitoring of technology system usage by staff for cyber security and IT reasons. This included the ability to see "what's going on" (CISO5), using "live operational dashboards ... [that show] the number of emails being blocked ... the number of viruses being detected" (CISO11). Such capabilities were also mentioned in a number of annual reports.

As well as surveilling staff, there were also examples of organisations surveilling their customers in terms of how their products and services were used by them, although with an acknowledgement from CISO8 that "it is a tough balance, not everybody wants it [monitoring of product usage] ... some people are really paranoid". A small number of the annual reports mentioned the existence of a CISO or a cyber-security function. These functions were expected to provide protection against these harms, to act as 'guards', to 'defend' the organisation and 'counter' them. This type of phrasing was common throughout many of these reports. This protection needed to be 'strong' and, in some cases, was articulated using militaristic terminology, which was also observed in the interview data, as discussed further below.

Cyber emergency. The majority of participants indicated an ongoing 'emergency' with regard to cyber security, which echoed the concept of permanent emergency identified from the literature, as discussed in Chapter 2. For example, CFO1 described how "the [cyber-security] threats will only increase", also referring to cyber security as an "ongoing challenge". CEO2 stated that "[cyber attacks] have been increasing and they've been increasing in ... sophistication". CEO1 agreed that "it's a constant ... everyone is trying the whole time to do better whether you're a defender or an attacker" and CFO1 articulated the need to deal with "a continuing moving goal post" with regard to cyber security. Multiple CISOs referred to 'ongoing' or 'increasing' aspects of cyber-security threat, including the need to be "cognisant of the new threats or new attack types" (CISO6) and having to deal with something that was "sophisticated, [it] changes almost on a daily basis" (CISO14). One CISO concisely expressed that there were "troubled times ahead" (CISO4), articulating a sense of foreboding.

Cyber warfare. A number of participants made specific references to cyber warfare, another concept that was discussed in Chapter 2. CISO3 observed that "if we do have some form of war between nations, it's probably going to be a cyber-attack isn't it?". Participants worried about threats from "rogue states" (CFO2), with cyber security being "an easier way to cause havoc in an enemy country" (CFO2). CISO3 agreed that cyber security was likely to be "the method of attack against the nation [i.e., the UK]". CISOs had even been asked by senior leaders "how do we retaliate?" (CISO8). Multiple examples of militaristic language were observed throughout all the interviews, ranging from the relatively mainstream, e.g. "attack", "defence", "threat" to more specialist examples such as "attack surface" and "red team" (all from multiple participants). An association of cyber security with militaristic practice was also indicated by references to “war games” (CISO11) and “war stories” (CISO3). Less overtly militaristic language was also observed when describing cyber-security risks. For example, CISO5 described articulating to their stakeholders “who it is that’s trying to do us harm”. CISO1 made reference to “trying to keep up to pace with security threats”, implying a ‘cyber arms race’ aspect that was also alluded to by other participants, although not explicitly stated. There were also references to established geopolitical ‘enemies of the West’, including the need to “protect against China” (CISO8) and have “heightened awareness of Iran” (CISO8). CEO1 was concerned about being “attacked [by] somebody sitting in Siberia ... the Chinese ... North Koreans”, providing an almost clean sweep of (currently) perceived foes. There was also, in one instance, a different form of ‘othering’, where CISO8 referred to the cyber-security risks posed by “a 14 year old in an internet cafe in Lagos”.

4.2.2 The relative importance of cyber security to organisational identity

Organisational identity, at least in terms of ‘who we are’ and ‘who we are not’, appeared to be factors in these organisations’ attitudes to cyber-security risk, both from the perspective of organisational identity being ‘something to be secured’, and also determining how much effort was expended in securing it. This was seen as particularly important from a perspective external to the organisation, because “the perception of trust or the perception of solidity is very important” (CISO15) with regard to cyber security. CISO11 referred to the need “to demonstrate that we behave like a FTSE[number redacted] organisation and take it [cyber security] seriously”[8] and a number of references were made to maintaining publicly disclosed cyber-security certifications such as ISO27001. CISO10 described having “accreditations that we have signed up to” in relation to cyber security, with CISO1 reporting the existence of a team member whose “sole job is to keep on top of [cyber-security certification]”, indicating not just the perceived importance of such certifications but also the volume of work involved. A considerable number of annual reports mentioned cyber security as a feature of their identity, including references to cyber-security accreditations as well as claims of excellence and achievement regarding both internal cyber-security activity and the security aspects of their products. In one case, cyber security was associated with an organisation’s innovation efforts.

[8] Many of the businesses in this study made reference to their market index position in their annual reports. This included membership of a particular index, e.g. being a FTSE100 or FTSE250 company, as well as, in some cases, their specific rank within that index. In certain cases, there was clearly an element of pride associated with this membership, and, where present, the rank, implying that this was also something that they valued.

CISO12 referred to maintaining “the overall cyber-security posture” of the organisation, implying both a public identity and a performative aspect, a sense of ‘keeping up appearances’. This was indicated by CISO13, who referred to cyber security “as something that they [the board] have to be concerned about and that they have to show that they’re concerned about”. Public statements relating to cyber security contained within company annual reports were mentioned by a number of participants, including CISO7 who described using these with their internal stakeholders to say “look, that’s what it says, that’s what we’re publicly telling people so you need to start doing it”, suggesting that these public pronouncements could be weaponised.

Trust was articulated as a significant factor in organisational identity across both the annual report and interview data. NED1 made this connection in relation to a cyber-security incident, stating that “if we broke that [customer] trust our reputation would just be killed because that’s what our business is based on”. Similarly, CISO14 referred to a major security incident resulting in a “material impact . . . [from] loss of reputation”. CISO10 also expressed a “reputational” demand from their customers in relation to cyber security, in the sense that those customers’ own identities depended on the security of the products and services that they consumed. Broader than cyber security, many of these businesses used their annual reports to position themselves as being ‘strong and stable’. Words such as these were commonly repeated throughout many of the reports, with multiple synonyms employed. These businesses wanted the audience of their annual reports to consider them as disciplined, effectively governed and well-behaved. They used various statements of sincerity to support this impression, including describing various practices being taken ‘seriously’ or being ‘cultural’, i.e., embedded within their ways of working and performed by default. These included, in some cases, cyber security.

Cyber-security practice appeared to be contingent on both the organisation’s business sector and its identity. CFO2 considered that there were “different challenges” in being a business-to-business (“B2B”) organisation rather than a business-to-consumer (“B2C”) one, something also articulated by NED1, CFO1 and CEO2. This included not being “known like a [well-known social media company] or a [major UK supermarket]” (CFO2). They derived “certain advantages” in relation to cyber security as a result of this. CFO1 echoed this, stating that they weren’t “a household name”. They described how “the bigger you are, the bigger target you are”, something also articulated by CEO2 who described cyber-security threat as being relative to both the size and type of a business.

In the context of their “cyber-security posture”, CFO1 referred to the organisation as “not a financial services company”. As mentioned briefly in the previous section, this was a common refrain, with banking and financial services held up as a gold standard of cyber security and suggesting that organisational identity affected where on the continuum of "good practice ... [to] best practice" (CISO7) the organisation sat. For example, CISO2 described how "some of the processes aren't quite as robust as you might get in a bank" and CISO11 stated that their business "probably don't focus in on enterprise risk management as much as, say, a global bank". Not being a bank was explicitly stated by a number of participants, including CISO1, who said "we're not the Bank of England", which meant that they had to "be pragmatic" about cyber security, and CISO11 declaring "we're not going to be like a bank". CIO1 also stated "we're not a bank" but added to this by saying that, also, they were not "a pharmaceutical company", relating this to the need to protect intellectual property (IP). Another participant described how they were "a high IP organisation", and this fact resulted in them "recognis[ing] the importance of [cyber security]". One participant who did work in a financial services business found the gold standard of banking in relation to cyber security amusing, considering how that must mean that they had "no excuse" in relation to having an effective cyber-security programme. They pointed out that further delineation within that industry was common, with distinctions being drawn by those within financial services between working in "a retail bank [versus] an investment bank". They concluded by saying that "there's always someone else who should have better controls than you, right?", suggesting that such comparisons were predominantly used as excuses.

A further aspect of identity that affected cyber-security practice related to those organisations that provided services to governmental or defence customers. This resulted in a need "to protect information to a level that is significantly higher in some of our areas than any other commercial company" as a result of handling "official-sensitive top secret information".[9] These organisations used this customer base to justify their investment in, and explain their attentiveness to, cyber security.

CFO1 considered that "the profile of cyber risk etc has gone up ... significantly in the last two three years", something that CISO6 indicated by saying that "10 years ago, the amount of airtime I got with the exec was very limited ... and even then they weren't really that interested". For CEO2, cyber security was something that "we absolutely can't take for granted". However, they also stated that "in our business, cyber security I hesitate to say is not a big issue". It was explicitly not something that they considered as being able to put them out of business. CFO1 referred to a "disparate and hence somewhat low level" nature to cyber-security risk in their

[9] These quotations are from two different participants and are not attributed to limit the risk of identification.

business. A similar point was made by CIO1 who described a distributed nature to their business that meant that "the likelihood of something bad happening . . . is probably quite low", again indicating a limited concern in relation to cyber security. While it may not have currently been a high priority, for a number of leaders, cyber security would become more important over time.[10] CFO1 described how "as you digitise . . . the end product or the customer experience . . . the cyber-security piece becomes more and more important". CEO2 thought that "[cyber security] is going to become a much more important subject going forward" and considered that the focus on security would escalate in line with increases in "size of [the] organization . . . the size of the challenge".

Organisational "maturity". The relative "maturity" (multiple participants) of the organisation, and of their industry, was articulated as a factor affecting cyber security. For example, CISO11 explained that their "industry is not necessarily hugely focused around maturity in risk" and CFO1 described their industry as "relatively immature" in relation to cyber security, with their own organisation being "behind the game" and "need[ing] to catch up". CISO4 had "demonstrated significant maturity improvement [in relation to cyber security] and that's been evidenced independently", the latter point indicating a normative aspect to the concept. Some non-CISOs wanted to see such "a mature framework" (CFO2) for cyber security in their organisations.

According to CISO2, maturity was also a factor in how the leadership of the organisation received information relating to cyber security, stating that it was "an indication of maturity . . . [as to whether] that board or any leadership group can appreciate it's better to know something even if you can't do anything about it right away". For CISO1, maturity was a factor in the reporting line of the cyber-security function, with a more mature organisation being more likely to have a reporting line for that function that was outside of IT.

4.2.3 Responding to identity threats

I now present some examples of how the organisations in this study performed identity work in response to the identity threats they associated with cyber security.

The presence of experts

These organisations made it clear that they employed experts, both in relation to cyber security and to other areas of specialism. In the annual reports, a number of businesses

[10] Other temporal factors relating to cyber security are described further below.

articulated cyber security as a specialist domain that relied upon experts. It was considered to be a complex area that required expertise to exist within the organisation, and for organisations to 'invest in people' that were responsible for cyber security. Descriptions of these internal capabilities varied, from names of departments and teams, e.g. 'cyber-security team', through to specific functions within those departments, e.g. 'security operations centre' and role titles, e.g. CISO. In a small number of cases, responsibilities of different elements within that internal capability were described. In some cases, a cyber-security capability was still in the process of being developed. External expertise was also mentioned in relation to cyber security, including the use of third-party outsourced services, consultants and threat intelligence, as well as external auditors.

Several participants, both CISOs and non-CISOs, referred to external standards such as NIST-CSF, ISO27001 and ISO31000.[11] For example, CFO2 explained how they would "like us [i.e., the organisation] to have a more mature ISO 27001 environment". As well as the incantation of standards, participants also referred to accreditation against them. This provided a further means of cementing cyber security as an expert system;[12] not only was there an external standard, agreed upon by external experts and branded with/by a recognised external authority, compliance with that standard can be assessed by further experts, i.e., auditors.

Non-CISO participants also appeared to consider cyber security as a specialist practice. CFO2, for example, referred to how their CISO is "bringing real-time expertise to the organisation". NED1 described how "we're [i.e., board members] not going to have the deep expertise" and CFO1 expressed that they are "never going to be a cyber-security expert". For them, cyber security itself was "a topic ... where you're always going to be looking to genuine experts". CIO1 articulated the need for any individual who was responsible for cyber security to have "the credentials in place to do that first" and described how their staff have "incentives to gain qualifications quickly"; these references suggest a perceived need not just for experts but also for proof of that expertise.

The existence of expert advisers within a business is a form of identity work, in response to ontological insecurity, that allows that business to "[know] which dangers to confront" [551, p. 345], as noted by Mitzen in her description of ontological security. This can be considered not just from a perspective of knowing which domains could pose dangers, e.g. cyber security, but also which specific dangers *within* those domains

[11] These are cyber-security specific standards that define frameworks and 'necessary' controls in order to achieve a 'best practice' level of security for an organisation.

[12] Here, I am I using Giddens' meaning of expert system [358] rather than in the artificial intelligence sense.

need to be addressed. Providing this expertise may be the intended purpose of a CISO within a business, i.e., objectively evaluating risk, based on knowledge and experience, to address the fear of specific threats to the business's viability. By employing a CISO, the business may be amassing information pertaining to the options they have available, in order to make a rational choice [312]. Without such expertise, those choices may be made based on limited information, or perception rather than objective analysis. However, evaluation of risk is inherently subjective [560] and, therefore, although a CISO and their team may be *intended* to provide expertise and the ability to objectively evaluate a situation, providing evidence to support security decisions, it may not be possible to provide that. However, these businesses appeared to trust their CISOs, as I now explore.

Trust in expert systems. An organisation must trust in the experts that it uses to interpret the "abstract principles" [358, p. 34] of risk that Giddens refers to. CISO6 commented on the importance of trust, but suggested the possibility of abusing that trust:

> "I like to make sure that we are very honest about the risks because it's very easy to mislead ... they [the board] don't know enough ... so they have to have some faith and trust in me and obviously my boss for representing that."

Other participants also indicated opportunities to take advantage of that trust. CISO15 referred to being asked "to educate [the board] on how to hold me [i.e., the CISO] to account", acknowledging that was "a bit backwards". NED1 suggested a similar situation by describing how board members needed to "understand the right questions to ask to make sure ... someone like you [i.e., a CISO] is doing your job appropriately", but when asked how they knew what the right questions to ask were, responded "I generally rely on someone like you". Other potentially Machiavellian opportunities were presented by interactions with senior leaders whereby the CISO would "pick the scenario to influence stakeholders" (CISO8) and the articulation of cyber-security risk as having been reduced to "perceived acceptable levels" (CISO11). In some cases, this included using "a lot of analogies" which provided an opportunity "to spin it [i.e., the message being delivered]" (CISO14), and these aspects of "spin" will be discussed in more detail in Section 4.6.2 below.

The level of trust placed in the CISO as indicated by the non-CISO participants appeared to be variable, with some expressing a high level of trust, and others suggesting that they were less trusting of their CISOs. For example, CFO1 suggested a lack of confidence in their cyber-security function, describing having "got lucky" with regard to some specific cyber-security incidents, and wanting to "not leave as much to luck next time". They also expressed a preference for an external view on their capabilities, how they would "rather [have] someone who actually would look at it [cyber security] properly and … knew what it should look like". The experience that people have regarding their interaction with experts affects their attitudes towards the overall domain, with the potential for disengagement from the domain as a result of negative experiences, as described by Giddens [358]. If an experience is not necessarily negative but is viewed in a particular way, then a degree of disengagement may result. For example, the perception that a cyber-security team is a blocker or operates as a form of 'police', as I discuss further below, could result in other employees seeking to avoid engaging with them.

Risks of cognitive bias. As articulated above, senior stakeholders in this study considered their CISOs to serve a protective purpose. However, the existence of such a role could contribute to the cognitive bias of illusion of control.[13] Illusion of control has been identified as a factor relating to perceived susceptibility to cyber-security threats [628] as well as to organisational decisions regarding recruitment [467].

IT researchers Mark Keil et al. cite prior research suggesting that "illusion of control tends to occur more often in individuals with a prior history of success" [467, p. 397]. A "history of success" could be considered from the point of view of an organisation not having suffered a successful cyber attack. A lack of cyber-security incidents as a measure of success, as observed in some of the businesses in this study, may result in those businesses having an illusion of control, providing affirmation that supports the continued employment of a CISO. For example, CISO4 referred to being "in the position where we're able to show … no breaches, no losses of confidentiality", with this being a metric by which the organisation measured its success in relation to cyber security.[14]

Another relevant cognitive bias is the "availability" heuristic as described by Tversky and Kahneman [743, p. 1127]; if an organisation is not aware of data breaches having occurred in their industry, they may view the likelihood of it happening to them as lower. This may have been manifest in the comment made by the participant who regarded cyber security as being of limited importance in their industry.[15] This

[13] Which is related to, but distinct from, optimistic bias [724].

[14] Equally, if an organisation doesn't employ a CISO, such success may cement their decision not to appoint one. Either way, it is notable that history of success has previously been identified as a factor in hubristic decision making by executives [395].

[15] "It's quite difficult to steal a building".

suggests an availability heuristic; as the participant was not aware of specific threats against their industry, they assumed that the nature of their business meant that cyber security was less of a threat than it would be in another sector. Conversely, if an industry, or a business itself, does suffer a data breach, the availability heuristic could lead that business to conclude that (further) investment in cyber security was required.[16]

As discussed in Chapter 2, "just as the anticipation of fear motivates behavior, so too does anticipation of its end" [72, p. R86]. Such anticipation may be sufficient motivation for employing a CISO in situations where an organisation considers itself at risk. Conversely, a CISO may be "moving people to protect themselves against harm" as described by Baron et al. [113, p. 426], whether through fear or otherwise. Projecting an *undesirable* future state may itself be a form of identity work; rather than a "coping strategy" as suggested by management researchers Sumati Ahuja et al. [75, p. 1002], it may present an opportunity to construct or reinforce an identity that resolves that undesirability, as I discuss further in Section 4.3.2. Emotional talk regarding a future state in which a cyber-security breach occurs, as expressed by a number of participants,[17] with an associated (emotional) impact on a business's reputation, supports the construction of an identity that is being defended against such a breach. This talk may also have the disciplinary effect of motivating an organisation to maintain the existence of a defender role, such as a CISO. However, while uncertainty may motivate identity work, there may be a limit to its motivating ability, as suggested by Giddens [359], and, therefore, deliberately constructing an identity as a resolver of uncertainty may be a flawed strategy.

Semiotic displays

A cyber-security function or CISO may serve a totemic purpose, publicly signifying the organisation's identity as being one that is responding to cyber-security threats. Although some annual reports mentioned the existence of a CISO, none of them named the occupant of that role, in contrast to a number of other senior, and in some cases less senior, individuals who were named in the report, supporting the idea that the existence of the role is more important than the person who performs it, as suggested by cultural theorist Dominic Pettman [601]. The presence of this totem, with the additional legitimation arising from an associated external certification such as those mentioned by a number of companies in this study, may be intended to convince the audience observing those signs that there is no need for them to make their own judgement on

[16] Increases in staffing following compliance breaches have been observed by other researchers, e.g. [133, p. 436].

[17] For example, the "shit!" response of CEO2 in relation to the mention of a cyber-security breach which appears in Section 4.3.2.

the organisation's expertise.

Such signs can also be seen as "status differentiation" [116, p. 63], and provide a visible sign of consumption, motivated by what Baudrillard describes as "*salvation by works*" [116, p. 62] (italics in original). Visibly signifying that an organisation is 'consuming' with regard to cyber security constructs an identity that is somehow virtuous, if cyber security is seen as a 'righteous' ideology in terms of its indexing of existing narratives of (supposed) right and wrong.[18] The organisations in this study made it clear to their stakeholders that they were investing in cyber security, particularly through their annual reports.[19] The majority of these made explicit reference to areas in which they were investing, often including cyber security as well as, more broadly, references to technological spending. Many of the annual reports described the need to invest in both internal and external 'expertise' as well as associated cyber-security technologies. In a small number of cases, there was a subtle but distinct positioning of cyber security not as an 'investment' but as an increasing cost to the organisation, a distinction I will discuss further in Section 4.3.

As introduced in Chapter 2, Baudrillard suggests that "violence" [116, p. 160] drives consumption. I argue that cyber security represents a form of this violence, particularly through its associations with warfare and fear. As violence, cyber security contributes to ontological insecurity for an organisation, and is also a factor in its relief by "stimulating consumption" [116, p. 163]. Baudrillard describes how the need to drive consumption (in a society that depends on it) "*fetishis[es]*" elements that can drive consumption; not just "objects ... [but also] ideas, leisure, knowledge, culture" [116, p. 62] (italics in original). Neocleous also discusses the "*security fetish*" [568, p. 153] (italics in original) associated with the "commodification of security", linking this further to "the ideology of security" [568, p. 153]. Baudrillard considers the use of these 'fetishistic' elements "as signs" used to signal an identity, including that of "status differentiation" [116, p. 63]. Borrowing a theological concept, he suggests that, in a consumption-driven society, status differentiation indicated by visible signs of consumption is motivated by a desire for "*salvation by works*" [116, p. 62] (italics in original). In other words, visibly signifying what an individual or an organisation has consumed constructs an identity that is somehow virtuous, something I return to in the next section. This sense of identification through signs is also suggested by Baudrillard to have a socially hierarchical dimension; "needs and satisfactions trickle down" [116, p. 64]. If governments and the military are at the top of that hierarchy, then their

[18] Baudrillard goes further, describing consumption itself, and by extension anything that can be consumed, as righteous [116]. These righteous aspects are developed further in Section 4.4.

[19] Although such statements were not necessarily in concordance with what CISOs experienced, as I discuss in Section 4.3.

signification of the importance of a cyber-security capability may 'trickle down' to businesses, and indeed, at least in the UK, this is demonstrated by government messaging about the role that businesses play in national cyber security [747]. Different types of businesses may occupy different roles in that social hierarchy of needs. Those that form part of critical national infrastructure or are part of the financial system, for example, may feature more prominent signs of cyber-security capability than other businesses, whether directly through public statements in their annual reports or through indirect means such as advertising.

An organisation's annual report, a document primarily intended for investors but available to the general public, also represents a form of semiotic display [170] and can itself be seen as a totem, articulating the organisation's identity through a narrative, using both words and images [635]. While not explicitly referring to organisational identity, management scholars David Campbell et al. apply signaling theory [707] to statements in annual reports, suggesting that "companies that believe they are 'better' than other companies signal this to investors in order to attract investment and a more favorable reputation" [197, p. 71]. This suggests that certain perlocutionary effects are expected by businesses in relation to the content of their annual reports, i.e., as a result of the narratives they construct, they anticipate, or at least hope for, further investment. One narrative that was consistently identified throughout the analysis was that of the organisation being, not necessarily "better", but of being righteous, which I now explore in more detail.

'Doing the right thing'

A considerable amount of ethical identity claims were identified in the annual reports of all organisations. These included references to ethical 'commitments' and intolerance for any deviation from these, as well as a large number of ethical assertions. The latter ranged from environmental achievements, employee diversity improvements, and human rights aspects of product and materials sourcing, through to the existence of roles dedicated to monitoring and improving ethical aspects of their businesses. The majority of organisations also supported their ethical claims with evidence. This ranged from certifications and awards through to the provision of externally verifiable data and case studies.

Businesses in this study constructed an ethical identity through their annual reports and wanted to appear as though they were 'doing the right thing' as well as being 'good for society', in some cases, 'essential'. This sense of keeping up appearances was related to a concern regarding the organisation's reputation, something that was considered to be of high value, and that was threatened by cyber-security failures. Ethics appeared to be a threat to these businesses, who were concerned about being punished if they transgressed, particularly in relation to the associated impact on their (highly valued) reputations, and, therefore, their identity, as established by management scholars Russell Abratt and Nicole Kleyn [64], which is fundamentally linked with morality [250, 388]. The motivation to act morally is, at least in part, based on a concern about the opinions of those external to oneself [370, p. 14] and these opinions may operate as what management scholar Stephen Fineman refers to as "felt pressures" [330, p. 36] that motivate the development of "working, or enacted moralities" [330, p. 37]. That is, the identity of these organisations as 'moral' may not have represented a deeply held position, but rather may have been a deliberately purposive construction.[20] Businesses themselves may even be inherently amoral, as suggested by Heath [396]. Ethical behaviour may, therefore, have been considered by these businesses to be of instrumental, rather than intrinsic, value.[21] However, that does not prevent the outcomes they achieve as being of ethical merit [399]. Statements made by these organisations in their annual reports in relation to continued adherence to governance principles and legislative requirements could also be viewed as moral commitments, at least from a shareholder perspective. Corporate governance can be argued as ensuring that governed organisations 'do the right thing' by their stakeholders, and, on this basis, can be seen as having a moral dimension.[22]

'Doing the right thing' was a common refrain, observed in the majority of annual reports, and in some cases, this was articulated as a 'core value' of the organisation. The concept of values was indexed by many of these businesses, including explicit references to both 'moral' and 'ethical' values. These adjectives were also applied to behaviour, with associated 'commitments' needing to be made by employees within a number of organisations. Some organisations referred to maintaining their ethical positions through staff discipline, including governance forums, remuneration-related objectives and employee contractual commitments as well as other, in some cases undefined, penalties. Additionally, the references to national security made by a number of these businesses, both in interview data and annual report data, enabled a moral identity

[20] A small number of instances were identified whereby businesses described performing actions that were positioned as ethical but were also strongly self-serving. These included descriptions of products and services provided by the organisation as being somehow ethical where that categorisation could be considered debatable. There were also some instances of very carefully worded descriptions of events and actions that could be perceived as Machiavellian.

[21] There is an established, although debated [325], distinction between instrumental and intrinsic value in moral philosophy. The distinction between the two is that intrinsic value relates to inherent "goodness" [325, p. 340], whereas instrumental value relates to utility, i.e. good *for* something. I return to these concepts in Chapter 5.

[22] The UK Corporate Governance Code also mentions the importance of "contributing to wider society" [243, p. 4].

to be created or maintained by association [705], something I develop further in the second part of this chapter.

Rights and wrongs of cyber security. Participants consistently indexed aspects of morality when describing cyber security, with 'doing the right thing' being a constant refrain in both CISO and non-CISO interviews. For example, CISO3 described having a desire to "make it easier for the business to do the right thing", CISO11 believed patching of systems was "do[ing] the right thing" and CISO4 mentioned the need to "do the right thing by the customer, by colleagues, by shareholders". CISO7 referred to "holding [third parties] to account to make sure they're doing the right thing". CISO2 described their board's perspective on their purpose as being "to make sure that we do the right thing", with that "right thing" being "keeping them within a best practice tolerance". They added that those stakeholders "do appreciate that there are trade-offs ... our role is to help with those trade-off judgements". CISO6 stated that there was a need to be "constantly challenging yourself to say 'are we doing it right?' ". CISO5 believed that their reporting line, which was not within the IT function, made it "much easier now to hold the right line ... [and] ensure that the right things are done at the right time", suggesting the potential for a conflicting moral position. They described how "when you're working into the [IT] design team, it's much harder to hold the line when the design's going wrong ... it's easier on the outside". CISO4 suggested that a reporting line that was outside of IT "kinda almost keeps you honest".

A right-versus-wrong dualism in relation to cyber security was indicated by CFO2, who described how breaches in cyber security can "cause nasty accidents" and can be "cruel", with CIO1 using similar language when referring to "nasty things happen[ing]" in relation to cyber security. Value-laden language was also observed in CFO2's description of the CISO having "a duty to communicate risk" and CISO1's articulation of their role as partly "making sure systems are built properly". A value judgement was implicit in the positioning of cyber security as hygiene [329] by a number of CISOs, including reference being made to "basic information security hygiene" (CISO14) and "general hygiene of the estate" (CISO12). The right-versus-wrong dimension was also indicated by a number of participants who implicitly indexed these aspects when describing negative cyber-security related consequences as being 'in trouble'. For example, CISO9 stated that "stopping the business getting into trouble is kind of one of the things that we do". CISO8 referred to having "an army [of staff] ... trying to find [employees] doing wrong". Their department was "the moral police force of the company" and, as will be discussed in Section 4.3, many CISOs enforced discipline.

The articulation of cyber threats in moral terms was also consistent. This included references to cyber-threat actors as “bad guys” (CISO9, CEO1) and a statement that “the mission [of the cyber-security function] really is to protect against crime” (CISO8). CEO1 wondered “how much would a big gang be prepared to invest in the efforts to do that [hack into one of their core systems]”, indicating that they were conscious of being targeted by criminals.

Additionally, the references to national security made by a number of these businesses, both in interview data and annual report data, enabled a moral identity to be created or maintained by association [705]. Entities with whom an organisation or an individual has a relationship can affect identity by association. If those entities have a moral dimension, then these moral aspects can also be transferred. Examples of such morally-implicated entities include law enforcement, national intelligence services and governments, as well as regulators, trade organisations and charities, all of whom were manifest within both interview and annual report data. It is not uncommon for law enforcement and intelligence services to be referenced by organisations experiencing cyber-security incidents, e.g. [50], and their invocation may serve a purpose of assuring stakeholders that the organisation is ‘doing the right thing’, but also indexing a broader narrative that the organisation is ‘a victim of crime’, further implying morality through the good versus bad, right versus wrong, dimension. The victim of crime position may even be referenced explicitly, e.g. [32]. Although no explicit ‘victim of crime’ statements were observed in this study, there were multiple references to being menaced by criminals as well as engagement with law enforcement and intelligence services, clearly placing the organisations concerned on the side of ‘good’ rather than ‘bad’.

Cyber security was perceived as resulting in punishment from external actors,[23] including references to “sanctions from government” (CFO2) and needing to have “a defendable position” (CISO15) against regulatory action. CISO9 referred to how cyber-security related “massive” regulatory fines had the effect that “suddenly boards sat up and took notice”. As well as fines, the risk of imprisonment relating to certain cyber-security failings was also highlighted by CISO15 who made reference to “personal liability” of senior leaders. Non-CISOs were aware of their obligations in relation to cyber security, with CEO2 describing how “the board under our legal system in the UK has responsibility for everything, good, bad or indifferent”, and NED1 making a similar comment, stating that “there’s a big role of the board relative to security and risk” and referring to their “fiduciary responsibilities”. This association with punishment implies a certain morality, as punishment is apportioned to those doing wrong. Further, there was a sense of these businesses being conscious of not being ‘caught’ doing wrong, as I now discuss.

[23] Discipline and punishment will be discussed in more detail in Section 4.3.

Cyber security under the spotlight. Several annual reports made it clear that these businesses considered their approach to cyber security to be something that was being watched by others. This was primarily described in terms of regulatory and legal oversight. These businesses were conscious that there was an external spotlight on them with regard to cyber security and that failures or omissions would be noticed. Cyber security was more prominently mentioned in the sections of the annual reports devoted to governance than in those focusing on strategy.[24] In a very limited number of cases, cyber security or data protection were mentioned in the "non-financial information statement", indicating that they were considered as social or community issues. Ethical behaviour more broadly was also described in terms of external focus. It was clear from a number of annual reports that businesses were conscious of being watched in relation to whether they were 'doing the right thing'. This was not just described in terms of a regulatory or legal focus, but also that of other stakeholders such as investors and customers.

For CISO13, their senior stakeholders saw cyber security "as something that they have to be concerned about and that they have to show that they're concerned about", suggesting both obligatory and appearance-related drivers. In CISO9's experience, "most of the time I would say that they're [i.e., the board] not particularly interested [in cyber security]". CISO13 echoed this sentiment by saying "I don't think they care deeply about it". CISO15 considered that the purpose of their role, as seen by their executive team, was "[to] keep the non-execs at bay", which suggests a lack of engagement with, even a lack of ownership regarding, cyber-security risk for those leaders but also reinforces a sense of obligation to external parties, in this case, the independent role of the non-executive directors. This external gaze suggested, in many cases, that certain activities were performed because the business felt that it was obligated to do them, either through something specific such as a regulation or, more implicitly, through being watched and judged. Cyber security appeared to be one of those activities for a number of these businesses.

The majority of the annual reports indicated that cyber security was also under a spotlight internally. This included many references to non-executive directors reviewing cyber security and, more broadly, cyber security being a board-level concern. CISOs were, in a limited number of cases, described as regularly presenting to the organisation's board and non-executive committees with regard to cyber-security ini-

[24] Annual reports of UK-listed organisations are subject to provisions defined by the Companies Act 2006 [4] which include the necessity for a "strategic report" [4, Ch. 4A] as well as a financial report and statements on corporate governance. The strategic report must include a "non-financial information statement" [4, Ch. 4A §414CA] containing information on relevant "social, community and human rights issues" [4, Ch. 4A §414C].

tiatives. Sometimes, the annual reports referred to senior leaders making judgements regarding the progress of the latter, and, in some cases, supporting those judgements through independent assessments. The majority of references to internal oversight were in connection with the audit committees of those businesses. There were notably fewer references to executive review of cyber security, with only a very small number of reports mentioning such an occurrence.

Ethical identity beyond cyber security. 'Ethics' itself was positioned in a number of ways by these businesses in their annual reports, including as an obligation and as a threat. Threatening aspects were articulated from the perspective of failures to maintain their ethical commitments and the associated impact on the organisation's identity, particularly through reputation. A number of organisations referred to ethics as a continuum, or indicated an interpretive aspect to the subject. As mentioned above, these businesses felt that ethics was a topic that received a lot of external attention, with references in annual reports to multiple stakeholder groups that were interested in, and were monitoring, ethical performance. In one case, the lack of any penalty for unethical behaviour was positioned as evidence of having behaved ethically.

An ethical identity construction may also be an attempt to legitimate an organisation. Organisational identity is associated with legitimacy [175, 793], a concept I introduced in Chapter 2. An organisation that positions itself as 'doing the right thing' in relation to cyber security is asserting that it is normatively compliant with what wider society considers to be what it is expected to do, what it 'ought' to do, as described by Suchman [719]. Importantly, such a positioning is crucial for ensuring what Brown describes as "easy access to resources, unrestricted access to markets, and long-term survival" [175, p. 38], survival and viability being key organisational concerns, as discussed earlier, and, hence, an ethical identity construction that indexes the moral category of cyber security is a means of maintaining an organisation's ontological security.

By establishing a legitimate identity, an organisation can also assign a legitimate identity to those individuals who form part of it. As well as legitimating its staff, an organisation can maintain legitimacy for all concerned by "caus[ing] them [i.e., staff] to forget experiences incompatible with its righteous image, and ... bring[ing] to their minds events which sustain the view ... that is complementary to itself" [294, p. 112]. This may involve the use of "symbols ... totems" [294, p. 113],[25] as well as specific language. Invoking sociologist Emile Durkheim, Douglas describes how these become "sacraliz[ed]" [294, p. 112], and, therefore, unchallengeable. They support the

[25] As introduced above and which will be further discussed below.

legitimate identity of the organisation and continually recreate it, but also maintain normative conventions, hierarchies and power structures [294]. This maintenance of hierarchy and power is a form of regulatory effect, a concept I now explore in more detail.

4.2.4 Regulatory effects

As introduced in Chapter 2, identities can be regulated and one identity may have a regulative effect on another, whether intentionally or not. This includes the creation, or assignment, of identities to one party as a result of another party's identity construction. These effects can be repressive and act as a form of control [86, 124, 129], particularly within organisations [86, 203].

Regulatory effects may arise from the (self-)positioning of an organisation's identity as being one that is committed to cyber security, through, for example, its public statements in annual reports or press releases, or through the appointment of a CISO. This may function as a 'normative control' that conditions or prepares its staff to be surveilled, supporting a wider metanarrative from government.[26] Indeed, governmental narratives were present in the analysis, including references to punishment from government as mentioned above, but also a national security perspective. Both CISOs and non-CISOs made reference to threats from "rogue states" and "cyber war", as well as related expectations from government. CEO2 described how "the UK government has been ... quite vocal [on cyber security] in recent years" and CISO8 mentioned that "the UK has an aspiration to be the safest place to do digital business", which refers to the UK's National Cyber Security Strategy [411, 412].

Many participants explicitly referred to the role that their businesses played in national security. This included participating in national security working groups as well as other interactions with national intelligence agencies in relation to cyber security. CEO1 referred to the UK government requiring certain minimum standards of their suppliers and CISO3 explained that "governments see the supply chain as their weaker link". One of the CEOs described being specifically obligated by government to take certain actions in relation to national security. Other participants also mentioned these minimum standards, with one CISO articulating that their approach to cyber security had to be verified by a government department before they were permitted to tender for a contract; this included "the quality of the cyber-security team ... [being] the litmus test", suggesting that individual people as well as organisational capabilities were being assessed. It appeared that there were double standards regarding evaluation by government, with government departments charged with assessing these businesses

[26] As will be discussed in more detail in Chapter 6.

responding with “oh Lord no, we would never achieve it” when asked if they complied with the same requirements. There were also references to invitation-only and industry-specific information exchanges with representatives from state security services where specific threats were shared with attendees, as well as indications of more indirect governmental influence. The latter included senior leaders being invited by government departments to participate in “roundtable discussions” and being encouraged to utilise certain frameworks. There were also indications of deference to wider surveillance occurring at state level, with CEO1 describing how various governments “keep an eye out, which works in ways that neither you or I need to know how it works”, suggesting that not only should such surveillance be accepted and unquestioned, it should also remain unexamined.

Similarly, the annual reports indicated political, and geopolitical, influences affecting a number of these businesses. In some cases, this was suggested by the presence of senior leaders who either currently or previously held positions within the UK or US military or government, or with quasi-governmental organisations.[27] More commonly, this was in relation to the role that the business played in supporting broader interests. Some of these businesses articulated their role in national security and in providing services to governments, both defence oriented and non-defence oriented. Governmental demand for products provided by these organisations was also mentioned, with this being a ‘critical market’ in a number of instances. A number of annual reports alluded to potential negative impacts on revenue if the focus of their government customers moved away from security-related products and services. Security in this context included, but was not limited to, cyber security. A number of businesses also referred to meeting various obligations relating to security and governance defined by their governmental customers.

In addition to the role that they played in national security, some participants also mentioned the role that their organisations played in wider society. This included those who referred to their organisations as being critical to the functioning of the UK economy, with cyber-security failures at a single organisation having wider societal impacts. One participant described their company as “the soft underbelly” for their customers, who themselves supported wider societal goals such as distribution of food.

Such narratives, originating from a position of power, can be seen as “mobiliz[ing] discursive resources . . . [that] get others to acknowledge or take seriously a position that is being proposed” [124, p. 69], in this case, the position that businesses need to take action with regard to cyber security, particularly as it is a significant threat

[27] E.g. intergovernmental organisations, trade organisations, law enforcement organisations, among others.

to the country. Further, by performing identity work that positions the organisation as one that is committed to cyber security, and, by extension, implementing cyber-security controls, the organisation regulates the identity of its staff such that they are 'the surveilled'. In addition, this public identity work may have a regulatory effect across industries, as other organisations consider a need to also adopt the identity of 'organisation who takes cyber security seriously'.

Identity regulation can also be seen from the perspective of the cyber-security industry. By defining the identity of cyber-security professionals in a particular way, including the hierarchical nature of the profession with the CISO role at the apex, the industry creates a metaphorical "iron cage" [465, p. 149] of identity. The existence of a CISO role within an organisation may also act as a form of identity regulation by defining who is and who isn't responsible for cyber security; by appointing a role that is, or at least appears to be, explicitly responsible for it, an organisation may implicitly be stating that others within the organisation are not, an established feature of bureaucracy [772]. However, this may have unintended consequences in the sense that those who have the identity of 'not responsible' may make decisions or display behaviours that are detrimental to the overall security of the organisation.[28] Further regulatory effects may result from masculine aspects of cyber security, which I will discuss further in Section 4.5 below. Beforehand, I turn to a broader discussion of CISO identity that is grounded in the data from this study.

4.3 CISO identity work

As discussed in Chapter 2, the existing literature suggests that the role, and purpose, of the CISO is unclear and multifarious. In this section, I provide an in-depth discussion of how CISO identities are constructed. I begin by exploring the ontological insecurity that was experienced by the CISOs I studied.

4.3.1 Motivators of CISO identity work

CISOs in this study indicated concerns with their continued existence within their organisations, being both explicitly concerned about the precarity of their roles as well as implicitly indicating anxiety regarding how they were perceived. CISO12 summed this up by stating "we know that it's implicit with our role, if something goes wrong . . .

[28] As Benwell and Stokoe describe, there is a "prevalent dualism" [129, p. 10] in discussions of identity as to whether agency or structure has the greatest influence. It is outside the scope of this thesis to explore these debates in detail, however, I follow Giddens [357] in considering that each may have a role to play in identity construction, and that the relationship between them may be fluid and dialectical [444] rather than there being a binary division.

you're the guy [that gets fired]". The importance of cyber security itself was, however, not questioned, suggesting that what was under threat was not the existence of the function or the role itself, but the incumbent's occupation of that role. For example, CISO3 described how the cyber-security function is "going to be there for the long term that's for sure" but they themselves were "not under any illusions [as] to where accountability sits". CISO2 believed that "if we had a terrible security failing here . . . I wouldn't escape the spotlight", also expressing that their relationship with their board could change if they "drop the ball really hard".

Non-CISOs also implied a threat to the CISO's position. For example, NED1 described the role that their board had with regard to cyber security as including the power to "hire [and] fire people" and their need to determine whether "whoever is accountable for it [cyber security] has the right level of expertise". CEO1 stated that "you have to make judgments on the fly about whether you think somebody is bullshitting or not", indicating not just an awareness that this was possible, but also that they were leaving open the option of removing anyone that they considered to be "bullshitting". As well as their senior leaders, CISOs also had to be concerned about regulators. For example, CISO15 described how "if one of those regulators raises their eyebrow at something I say, that's the end of my job", indicating that they needed to satisfy multiple stakeholders who could impact on their employment status.

Detachment and 'othering' of the CISO

CISOs in this study indicated feelings of detachment and vulnerability, partly related to inhabiting a precarious role, as well as isolation and exposure. CISO3 stated that "it can be very lonely in security" and CISO13 described how "you can never win really". The experience of being a CISO could be "a little overwhelming" (CISO1). CISOs also experienced frustration. CISO14 had "found it a really, really hard slog to get . . . stakeholders to just engage with security and understand the value" and CISO7 referred to "spend[ing] too long doing run of the mill kind of stuff which doesn't add much value". CISO15 seemed resigned to "roughly a third of the people [i.e., their internal stakeholders] to be complaining at any given moment".

Many CISOs felt undervalued, even to the extent that "if none of us turned up for a week or a couple of weeks, no-one's gonna notice, nothing's gonna happen" (CISO7). CISOs felt that senior leaders "don't see the risks, they don't understand the risk that the whole of [company name] faces" (CISO7), "they wouldn't understand . . . the threat that they're under" (CISO6). CISO2 experienced there being "a lot of different variations of understanding about security in the business generally". However, this may be partly because "the hardest thing . . . is being able to articulate what is actually a cyber team ... [it's] a really difficult thing to describe" (CISO5). Because of this, they felt the need to "to give them [i.e., senior leaders] a feel for what we're dealing with" (CISO4). CISO7 felt that a (hypothetical) move out of IT would result in them having "a bit more clout ... a bit more perhaps respect within the organization".

In CISO9's experience, "most of the time I would say that they're [i.e., the board] not particularly interested [in cyber security]". CISO13 echoed this sentiment by saying "I don't think they care deeply about it". CISO2 believed that their senior leaders "don't realise how bad it gets when it's really bad". When asked to describe the responsibility of their CISO, CFO2's response was "[pronounced outbreath] ... that's [laughs] I can't believe I can't answer that question".[29] Their reaction here was one of surprise, self-reflection, and even embarrassment. They may have considered that someone in their position should have been able to answer such a question easily, but may also have considered that not being able to answer it was insulting to both their CISO and myself, as I perform the same role.

CISOs felt anxious about how they were seen, which included "try[ing] not to be too much of a pain" (CISO13). They needed to be "credible" (CISO4), to have a strong "reputation" (CISO4), which may be partly because, in some cases, senior leaders were judging "whether it looks like they are masters of their brief" (CEO1). Related to this, CISOs also experienced aspects of 'othering' within their organisations. For example, CISO2 referred to being "treated like a body that needs to be negotiated with ... rather [than] as something intrinsic" and CISO15 described how they were viewed as being "of a different tribe".[30] A CISO who had recently changed reporting line, such that they were no longer reporting into IT, described how that change had affected the relationship with their previous colleagues, with the result that those colleagues had now been "put ... on their guard". CISO15 suggested something similar, how it might feel to their stakeholders like they were "an auditor".

As well as their perceived precarity, CISOs in this study also experienced identity threats from the perspective of being seen as a particular 'type' of individual. This was partly because the CISO identity itself was unclear, multiple, and conflicted, as I now explore.

Conflicted identities of the CISO

CISOs inhabited a multitude of different roles, which appeared to be in conflict in some cases. One conflicting identity was whether cyber security was, or was not, an

[29] This participant described having been asked this question, and their reflections on their response to it, as a notable benefit to them of having taken part in the interview.

[30] One senior leader referred to me, a CISO, as "people like you" (CEO2).

element of IT. CISO6 stated that "everyone sees it [cyber security] as IT but it's not" and CISO5 agreed that "cyber [security] ... is much more than [IT]". CEO1 described cyber security as "an element within IT reporting" and the other non-CISO participants all associated cyber security with IT. While this study does not explore reporting lines in detail, it is notable that there were multiple and varied reporting lines of the CISO participants, with some reporting to an IT function, some to a General Counsel, and some to a Finance function. For CEO2, cyber security was "part and parcel of our technology team" but they acknowledged that "[a] standalone security and assurance function ... does make sense, otherwise people are marking their own homework aren't they?". IT reporting lines did cause some friction for CISOs including "a problem around separation of duties" that could lead to them "drop[ping] [their boss, the CIO] in the shit" (CISO14). CISO11 described something similar, referring to the need for

> "independence and separation from IT because if the CIO wants to drive a different agenda, then you know, there's the risk that you could have some of the data and information either suppressed or masked".

However, the conflict of interest angle was, for CISO2, "often overplayed". CISO6 stated "I don't think [reporting line] really matters providing you have the right governance ... without governance you can get some real conflicts of interest". A CIO who did have responsibility for cyber security described being "quite happy ... to move it [i.e., responsibility for cyber security] on, pass the baton, that's fine [laughter]" (CIO1). Their laughter here suggested a disinclination towards having that ownership, and perhaps even a lack of interest in cyber security itself.

CISO1 believed that a non-IT reporting line would result in "less leverage to be able to work" and also "less visibility of what's happening on the inside of IT". CISO7 agreed, saying that "because I'm in IT, I can get a lot more stuff done". CISO9 referred to organisational power, stating that "if you're separate from IT, it's all well and good saying you must do this but you have less clout" with CISO11 similarly acknowledging a benefit of an IT reporting line as "safety in numbers ... if I have to go to the board, I go with the CIO". CISO10 felt very strongly about not reporting to IT, saying that they had "refused to do that in any role that I ever went to". CISO6 described being "tarnished" by association due to "IT ... [having] a pretty poor reputation in the organisation". However, CISO2, who did not report into an IT function, described how "delivery is much harder when you're not in the same hierarchy as the people that are ultimately probably going to be doing a lot of the work".

Technical versus non-technical. A related finding was an apparent distinction between technical and non-technical security staff. CISO13 positioned themselves as "a non-IT person", CISO15 portrayed a part of their security organisation as being "where our deep techies live" and CISO14 referred to a particularly technical member of staff as being someone who "you might not put in front of the board of directors". CISO12 described having "a couple of guys that are kind of technical" and CISO1 distinguished non-technical aspects as the "fluffy side" of cyber security, a feminisation that will be discussed further in Section 4.5. CISO9 referred to having a "background [in] IT, so I feel comfortable being in IT" but, in their situation, advancement within the organisation could involve "moving from a role that still has very much a technical aspect to it to a pure *management* role" (emphasis captured in original transcript). CISO11 described the need for certain security staff to not be "the geeky dudes that sit in the dark room and eat mushrooms and hack and break things", preferring instead "vibrant engaging smiling tolerant resilient people" to engage with their business stakeholders.

The majority of CISOs stressed that their primary focus was on "the business" (multiple CISOs), by which they were referring to the commercial, non-IT aspects of the organisation.[31] This included "stay[ing] in touch with the market" (CISO3) and "partner[ing] with the business" (CISO2) to ensure it continued to be "making money ... [and] getting more business through the door" (CISO1). CISO4 emphasised their business focus by describing how they spent the majority of their time "with business and operating board and audit stakeholders ... [rather than] technology stakeholders". CISOs wanted to be seen as being "interested in the security of business rather than the business of security" (CISO15). Security personnel needed to understand that "the business has to run, without a business, there's no security team because they can't get paid" (CISO1), which provides a more prosaic view of the role.

Barrier versus enabler. A large number of CISOs were concerned about being seen as "an impediment" (CISO4). They described their functions being characterised variously as "the ministry of no" (CISO8) or "the people who put the no into innovation" (CISO7). Cyber-security personnel might "stop people having fun" (CISO1) or "slow things down" (CISO5), with cyber-security improvements being seen as "an adjunct ... or an annoyance" (CISO2).

CISO6 was "not a naysayer"; they were "try[ing] not to be a blocker and mak[ing] sure my team are the same". CISO5 acknowledged the risk of their function "inhibit[ing] the business and stop[ping] it from working". CISO2 admitted that "security professionals, or practitioners often aren't *that* flexible" (emphasis captured in original

[31] Similar language has been identified by previous researchers e.g. [273].

transcript) and CISO13 commented that "there's always this sense that you don't want to create too much burden on people", stating that their internal customers "will be quick to complain".

However, some CISOs saw themselves as "help[ing] solve problems rather than close doors" (CISO6), "helping [their business to] make better decisions about how the business runs" (CISO10). CISO14 had "always been a very strong believer that security has to be seen as an enabler for the business", with CISO13 seeing themselves as "more of an orchestrator". CFO1 saw the security function as "a behind the scenes but core plank" within the organisation, with a similar conception articulated by CISO9 who described how

> "there is a certain appreciation, of what it is you do ... [but most of] the time, I would question whether or not they even know [we're here] ... that's not necessarily a bad thing ... [if] things are running well, nobody worries too much about how they are running well. When IT works it works, if IT is secure it's secure and nobody worries about it too much ... it's only when it all goes wrong that they start jumping up and down".

This underlines the sense of the CISO as enabler but also suggests a background role, one that the organisation would only miss if it wasn't there.[32]

CISO12 referred to the Covid-19 pandemic as stimulating a shift in their approach, with more of a focus on enablement. The pandemic had "made us pause and think ...how can we enable [staff] to work and to be productive ...without worrying how to do it", suggesting that, were it not for the pandemic, they would not necessarily have considered how to facilitate productivity in the same way.

Some CISOs were arguably both barrier and enabler due to acting as gatekeepers, particularly in "allow[ing]" (CISO15) the organisation to take certain risks. Similarly, they were brokers of information. For example, CISO14 described how "very often we will get a piece of threat intel and if I think it's relevant to share with a stakeholder we will actively do that". CISO6 referred to removing information from certain reports as their stakeholders "don't need to know the detail" and CISO2 articulated their role as "surfacing ... things that matter, matter more, so they [the board] understand what matters". The latter included "severity but also relevance or whether or not there's a bigger picture message or an opportunity to educate", providing a link to pedagogical aspects of the role that will be presented later in this chapter.

[32] This suggested, to me, the metaphor of a bass player. Admittedly, I am also a bass player, but am not the first to use this analogy, e.g. [544].

4.3.2 How cyber security is positioned

In this section, I discuss how cyber security itself was both presented and understood by the participants. Such an understanding provided a foundation for the CISOs' subsequent identity work and is, therefore, important to appreciate.

Cyber security as not-science

Several CISOs described cyber security as 'not-science'. CISO2 passionately stated that "although much of ... cyber security ... is kind of positioned as almost a science, you know my own approach is that it's not **at all**" (emphasis captured in original transcript). They added that they rely on "judgement and gut feeling and stuff like that". CISO2 further highlighted how they determine "the right course of action" based on both "data" and "gut feeling", but that often a lack of empirical data meant that they must rely on their own "experience". In line with this, several CISOs invoked the 'art not science' motif by describing the immeasurability of cyber-security risk set against pressures from their stakeholders for measurability and quantification. CISO13 believed that their stakeholders did not appreciate that "there isn't a clear answer", which resulted in them experiencing frustration. Similarly, CISO7 admitted to "the subjectiveness" of their interpretations and referred to part of their role as "wordsmithing things", indicating an 'art' to what they do, as well as the opportunity for sophistry, which is discussed further in Section 4.6.

Several CISOs either explicitly labelled themselves as pragmatic or as not-dogmatic, or implicitly invoked that label using similar words, e.g. "I think they appreciate I'm pretty candid and also realistic" (CISO2). The invocation of 'pragmatic' (identified in 13 out of 15 CISO interviews) implies a sense of interpretation; in order to be pragmatic or realistic, both an analysis and a judgement are required. This also helped to position the CISO role as one of expertise. Expertise, pragmatism and interpretation are all themes that I develop further throughout the chapter. First, I explore the conception of cyber security as fearful.

Cyber security as fearful

The association of fear with cyber security was observed throughout the interview data. For example, words such as "scary" and "worried" were commonly used by both CISOs and non-CISOs. The perception of senior leaders in particular was that a cyber-security incident was something to be afraid of, summarised by the following exchange:

Interviewer: "When you hear about things like the Travelex incident,[33] how

[33] A reference to the then-current ransomware attack experienced by Travelex in early 2020.

> does that tend to make you feel, how do you tend to react?"
>
> *CEO2:* "Shit! [laughter]".

The participant's laughter here perhaps indicated an underlying nervousness in relation to a cyber-security incident, but also a level of rapport with myself as the interviewer.[34] NED1 described how increased knowledge regarding cyber security, as provided by their CISO and also from what they had observed in the media, had "got me a little scared".

The annual report data also indicated that impacts arising from cyber-security risks were feared by these organisations. There were multiple references to cyber criminals, geopolitical cyber-threat actors such as nation states, and cyber terrorists.[35] Cyber-security threats were 'sophisticated' and 'complex', and were growing in both of these dimensions, as well as in frequency. These organisations were conscious of the existence of cyber-security threats targeted against them specifically, and against businesses more generally.

CISOs deliberately utilised fear in their communications with stakeholders, including making reference to cyber-security incidents affecting other organisations. CISO4 indicated a 'usefulness' of associating cyber security with fear, stating that "if there's an incident or a breach or a loss event that is topical ... you want to use that ... it will resonate with [board members]". NED1 believed that "you don't do it [improve cyber security] because of fear of being fined, but you have to, you know, take all of those things into account". CISO14 referred to fear being "coupled with 'so what are you doing about it' ", indicating that they generated a fear response in order to position a sense of assuagement of that fear. CISO14 was more explicit regarding assuagement, describing how they saw their role as "giving my senior stakeholders ... [a] level of comfort". CISO6 used similar language when referring to reporting on cyber security to their senior stakeholders, stating that "a lot of it's about a comfort factor". CISO14 had "tried to drive the message that ... it's when not if [a cyber-security incident occurs]", adding that their stakeholders "accept that the likelihood is that we will suffer some form of cyber event over the ... short to medium term". Multiple references were made to "sophisticated" threats that were "increasing" and "ever-changing". CISO4 described articulating "why it might not happen to us" in their communications relating to cyber-security incidents affecting other companies. CISO13 stated that "until [a major incident] happens, they'll [i.e., the board] feel confident about it", suggesting that a lack of bad news was indicative of good news.

[34] Findings related to rapport and other, predominantly methodological, aspects of the interviews can be found in Appendix A.

[35] Non-cyber related terrorist threats were also mentioned in some cases.

Cyber security as bad news

Cyber security was characterised by many participants as bad news, and the CISO as a 'bad-news merchant'. CISO3 described how "our job is to point out there's a problem here", while CISO13 referred to activities aimed at "flush[ing] out some of the issues". CISO2 positioned the role of the CISO as "turning over rocks and doing discovery and showing how bad everything is, so things appear to get worse". CISO12 provided an example of being a 'bad news merchant', saying that they would only be present at a board meeting "if it's something going wrong". CEO1 expected "to be told quickly . . . if something serious happened [in relation to cyber security]". However, CFO2 implied that they did not want to be told bad news, and CISO9 relayed how their CEO was, at one stage, "very angry" when presented with cyber-security risk.

According to CISO5, there was "only so much [that] people can put up with", which may indicate that bad news relating to cyber security results in fatigue. This statement also suggests a level of frustration and resignation on behalf of the CISO in relation to being a bad-news merchant. CEO1 stated that "what we try to avoid is shroud-waving at ourselves the whole time because people then don't take it seriously", indicating again that cyber security has a negative association and suggesting the risk of 'cyber fatigue'. The interview data also included a number of references to the high cost of cyber security, which may contribute to a conception of the subject as bad news.

Cyber security as cost centre. CISOs were conscious that cyber security was a significant cost for their organisation and the majority described being under cost constraints. Additional investment was "often hard to justify if not impossible" (CISO11) and cyber security was "expensive" (CISO6), with cyber-security functions being "by nature quite expensive to run and you need some powerful tools to do stuff" (CEO1). Cost seemed to be inherently associated with security practice. CISOs were hearing phrases such as "we seem to be spending a lot of money on security" (CISO8) from their senior stakeholders. CISO10 referred to senior leaders having "doubts that we just seem to be costing money, I get that occasionally, I think everyone in security will do". Those senior leaders would be "worrying about how much it costs", because "security . . . doesn't make the business any money, it's an overhead, you know, you're an overhead" (CISO7). In some cases, business leaders would decide "well actually we'll take the risk and we won't spend the money" (CISO9). There was a need to manage cyber-security risk "from a cost-effective standpoint" (CISO11), and "being roughly as safe as your peers, but at lower cost and faster" was "a competitive advantage" (CISO15). However, as a CISO, it was "hard to say you've got a strategy when you don't have money" (CISO5), suggesting that they felt their value was undermined by a lack of funding.

CISO10 described being subject to "budgetary squeezes" but insisting that certain security costs were "red line[s]", not least because the organisation's "reputation depend[ed] on" them. CISO13 referred to security projects being postponed due to budget reasons and also explained that "there is always that tension because ... obviously the organisation doesn't want to spend money on it". Cost constraints were particularly associated with spending on technology to support security objectives, as there were "only so many tools that the business is prepared to buy and pay licenses for" (CISO5) although it was possible to have invested heavily in information security tooling without deriving value from it, resulting in a situation of having "all the gear and no idea" (CISO6), which would contribute to a sense of cyber security as a never-ending cost.

Temporal and spatial factors

The majority of CISOs described their cyber-security capability as incomplete, either in temporal or spatial terms. For CISO14, they had "still got a quite a way to go", with an almost identical statement being made by CISO10. The concept of being on a cyber-security "journey"[36] was expressed explicitly by CISO2, CISO3, CISO4 and CISO15 as well as CFO1 and CFO2. This concept was implicitly referred to by a number of other participants, including CISO13 who characterised cyber security as "a marathon as opposed to a sprint", but they were "ultimately get[ting] them [i.e., the organisation] to a better place". A concept used in tandem with spatial elements was that of "maturity". For example, CISO2 was "on a maturity path" with regard to their cyber-security programme and CFO2 used similar phrasing. CISO11 described the organisation needing to "take a step up in terms of maturity" and CIO1 described their organisation's cyber-security maturity being "miles apart" from "its aspirations", expressing not just a spatial gap but one that was sizeable. Some of the annual reports similarly described cyber security as a 'work in progress'. This included references to historical and planned maturity improvements. These were, in many cases, positioned as long-term improvements, in some cases, 'continual'.

As well as spatial metaphors, temporality was employed by participants. CISO11 stated that "a maturity and cultural shift [with regard to cyber security] ... takes time" and, similarly, CISO13 described how improving cyber security "just takes a bit of time". This time period was measured in years. CISO6 had "laid out a three year plan ... we're two years in ... I'm just in the process of writing what [years] four, five and six will look like". CISO7 expected that it would take "five years ... [to get]

[36] Admittedly a common metaphor in business.

ourselves up to a level of three and a half maturity".[37] CISO15 considered that the cyber-security function would "become more and more important", in relation to both future pace of change in their business and also "as the regulations continue to pick up". In particular, the latter meant that "the potential to get it wrong and the impact of getting it wrong increases". This also indicates the sense of foreboding in relation to cyber security identified in Section 4.2.1.

However, the goal, whether measured in temporal or spatial terms, may never be reached, as demonstrated by CISO3 who described how "the journey's never complete". CFO1 indicated some frustration with this, describing how

> "it's a continuing moving goal post so you'll never [complete the journey] . . . if you set yourself a goal for a year . . . the goal has moved in a year's time so yes, you'll be better than you were but you wouldn't have got to quite where you want because the goal's moved".

They did acknowledge that "having said that, you will then get to a good level hopefully . . . [then] it's a gradual improvement from there as opposed to having to make a step change". Their concept of "a good level" was echoed by CISO2 who described having a target of "good enough" but also expressed that the definition of this was fluid. CISO2 referred to having a "goal" to "make ourselves [i.e., the cyber-security function] as redundant as possible" but acknowledged that they were "definitely not there yet". When asked how far away that goal was, they stated that "we'll never get there", indicating that this may have been a hollow aspiration.

Cyber security is experienced emotionally

As well as fear and anger, other emotions were articulated by participants in relation to cyber security. CEO1 was "incredibly upset" when "ethical hack[ers] . . . seemed to get in", and CISO8 expressed how "the inevitability of [a cyber-security incident] upsets a lot of people". CISO12 described such incidents as having "psychological effects" on their staff, particularly shame, if "a hack on my computer allowed this to happen". Other emotions associated with cyber security included "panic" (CEO2) and even love, with CISO11 explaining that they employed people who "love security".

Viewing cyber-security threats as potentially existential to the organisation, as discussed earlier, may motivate the organisation to construct, through dialogue, both internal and external, an identity that is protected against those threats. Articulation of this identity feeds the organisation's sense of ontological security and it becomes

[37] Where maturity measurements were referred to by participants, whether CISO or non-CISO, it was always on a five-point scale, similar to established technology industry maturity models.

self-sustaining, unless something happens that contradicts or undermines that identity. Articulating or demonstrating that they employ someone in a role that helps defend the organisation against cyber-security threats is an example of this identity work at an organisational level, which then sustains the identity of the person employed in that role, giving them a greater sense of ontological security, both as a person who has a clear identity as a 'defender'[38] but also as a person who is valued and necessary, and, therefore, likely to continue to be employed. Identity work that relates to cyber security can be seen as beneficial to both parties, organisation and CISO; this can of course be extended to other interested actors, such as governments and the cyber-security industry, as will be discussed in Chapter 6. Using Sims' model of an individual's identity being distributed [685], if an identity depends upon being 'present' in other people's minds, then there is a risk to that identity if those people stop thinking about it. In Figure 4.2, I summarise the interplay of phenomena identified in this study that relate to ontological security and cyber security.

[38] Which arguably has a moral dimension, as I discuss shortly.

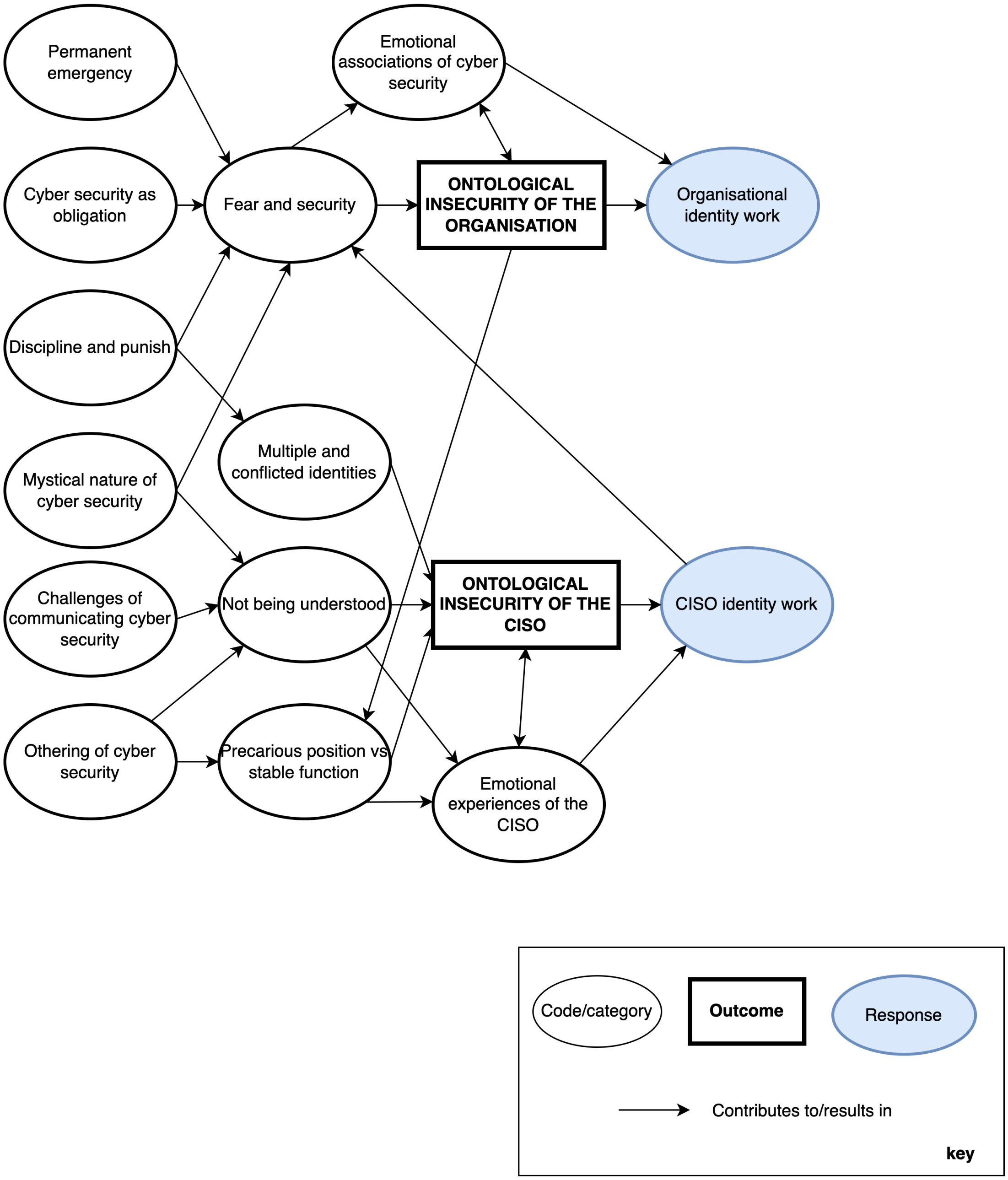

Permanent emergency
Emotional associations of cyber security
Cyber security as obligation
Fear and security
ONTOLOGICAL INSECURITY OF THE ORGANISATION
Organisational identity work
Discipline and punish
Multiple and conflicted identities
Mystical nature of cyber security
Challenges of communicating cyber security
Not being understood
ONTOLOGICAL INSECURITY OF THE CISO
CISO identity work
Othering of cyber security
Precarious position vs stable function
Emotional experiences of the CISO
Code/category
Outcome
Response
Contributes to/results in
key

Figure 4.2: An operational model diagram (following Saldaña [653, pp. 226-7]) summarising the links between ontological security and identity work from both organisational and CISO perspectives.

This diagram[39] suggests the existence of a complex cycle with regard to ontological

[39] Which reflects codes and categories of data from the analysis. More detailed diagrams are provided

security, cyber security and identity work. Of particular note is that the identity work performed by a CISO may indirectly contribute to the ontological insecurity of the organisation through the use of fear appeals. The use of the latter supports continued presence in the minds of others, through the use of a narrative that is exciting [685, p. 100]. Exciting cyber-security narratives, such as nation-state attacks, threats to critical national infrastructure, and media frenzy were observed in the present study and, as discussed in Chapter 2, are common elsewhere. These help to maintain the existence of a cyber-security professional's identity, particularly when that professional experiences ontological *in*security, as observed in this study.

Having explored how cyber security itself was presented, I now explore the different forms of identity work performed by the participants in this study.

The CISO as protector

CISO15 had "positioned" themselves with senior stakeholders as a protector by saying "my promise is to keep you safe", with their responsibility being to "pick out the kinds of data that can cause the most harm and pick out the kinds of people that can cause the most harm". CISO7's role was to "ensure the business understands the risks to their systems and data and can take appropriate action to protect them". CISO4 described providing "safeguards and protective measures" and helping business stakeholders to "deliver the outcomes that they're trying to deliver in a safe controlled and protected manner". Employees needed "to tolerate some inconvenience ... because people become safer" (CEO1). CISO15 had made a "promise to keep [the board] safe" and CISO11 stressed to their stakeholders that it was "better to be safe than sorry", invoking concepts of both protection and fear.

The CISO as expert

The analysis of the interview data suggested that the practice of cyber security was highly specialised, requiring expert knowledge and capability. This was indicated across the data, and took many forms. CFO2 described how "the cyber team recommend to us as a management team what they think they need to do because it's quite specialised", which may suggest that this "cyber team" actively position themselves as specialists. This participant also referred to needing to "unpick" the information they are provided, in which "there are quite a lot of acronyms". CISO3 believed that their board "still struggle a little" and explicitly positioned themselves as an expert, explaining how "you'll come in [to a board meeting] as a subject matter expert". Through this narrative

in Appendix B.

construction, they were not only the expert but also the solution to a problem. CISO15 suggested a similar narrative:

> “when I turned up, it was management by anecdote ... the board didn’t know which question to ask ... I think I’ve turned that around”.

CISO4 described “dealing with ... a particularly sophisticated set of attack activity”, adding that “cyber-security is a dark art ... most people won’t understand it”, their narrative suggesting a problem that is both fearful and incomprehensible.[40]

As mentioned earlier, there were several references in the data to external security standards such as NIST-CSF, ISO27001 and ISO31000. CISO7 stated that their board “quite like the fact that I’ve based us around the NIST cyber-security framework” and described referencing this standard in their reporting, using it to frame their activity. The use and presence of standards may serve to legitimise their activity but also suggests a position as an expert. CISO15 suggested that if a provider of a service is regulated, that fact “slightly obviates” the consumers of that service “from having to make a judgment”. Similarly, the reference to a standard by a CISO may “obviate”, at least in part, the need of their audience to make a judgement on the CISO’s legitimacy or expertise. CISO9, however, partly challenged the use of standards, saying that “ISO27001 is often seen as a bit of a panacea” and that they were “not necessarily convinced that ISO[27001] is the sort of ... big sticking plaster that everybody thinks it is”. They suggested a ranking of accredited standards, that some are considered “lesser certifications or qualifications”, but thought that “actually ... they all have a place”.

References such as these to the ‘professional’ nature of cyber security and the indexation of standards help to construct an expert identity for CISOs. This is supported by the existence of professional associations relating to cyber security, e.g. [18]. Goffman points out how these “require practitioners to absorb a mystical range and period of training ... in part to foster the impression [of difference and status]” [363, p. 55] and, as discussed further below, many professional bodies also require attestation by their members to particular behaviours. Goffman’s point about a “mystical” aspect of specialist knowledge is important to reflect on; this suggests that the positioning of a role as professional may depend on the specialist nature of the knowledge required, its unknowability by those outside of the profession, regardless of whether that is actually the case [359, p. 30]. As well as possession of specific knowledge, it could also be the ability to interpret that knowledge. Therefore, it may be in the interests of professionals to position their work as “mystical” in order to maintain the identity of the group.

[40] This aspect of cyber security being a ‘dark art’ is explored further in Section 4.4 below.

Such positioning may also serve the purpose of "dramatizing one's work" [363, p. 42], selectively making certain elements visible while concealing others, as also described by Goffman [363].

Referring to earlier work by cultural theorist Gayatri Spivak [708], Benwell and Stokoe point out that "the membership of a specific, named collectivity may be a *marked* and politically motivated strategy to make oneself and one's interests 'visible' and 'included'" [129, p. 28] (italics in original). Discussing, and critiquing, historian Christopher Lasch's work [495, 496], Giddens summarises his point that experts may "have invented the very needs they claim to satisfy" [359, p. 173]. Therefore, as well as providing an identity with which to associate, a group of experts may, wittingly or unwittingly, perpetuate claims that support their existence, something I explore further in Section 4.6.

Expert superiority. CISO3 stated "it's like children isn't it", when referring to communicating cyber risk to their stakeholders. They described how "people don't like to be told what to do . . . unless they understand". This suggests not just the construction of an expert identity but also one of superiority, a more knowledgeable and well-meaning parent explaining something to a less knowledgeable, naïve child. A different aspect of superiority was expressed by CISO14 when referring to one of their team members who they described as someone that "you might not put in front of the board of directors". As well as being superior, this may suggest that a particular 'type' of person is required in order to interact with senior leaders and also links to the distinction between technical and non-technical identities discussed in Section 4.3.1.

Other indications of constructing cyber security as an expert system in the data included references to the subject itself being demanding. For example, CISO11 stated how "it's not simple and it's not easy, it's not straightforward". CISO4 stated that "most people won't understand it [cyber security]". This implies not just the specialist nature of the subject, but also the specialist nature (in the sense of *being* 'special') of the person who does understand it. By delineating between those who do and those who do not understand there is also a suggestion of superiority, that having that understanding sets them apart from "most people". CISO1 alluded to this when describing how they "want to give them [their senior stakeholders] an idea of the scope of what we're trying to do". By giving their stakeholders the idea that they were dealing with something that was difficult, CISOs constructed (or maintained) an identity as an expert. This was further developed by the commonly expressed need for cyber security to be interpreted, as I now discuss.

Cyber security as an interpretive practice

Multiple participants articulated a need for cyber-security decisions to be made based on interpretation. For example, CISO8 described their role as involving "a whole lot of translating threat landscape into reality". These did not solely originate from CISO participants. For example, CFO2 needed cyber-security information to be "expressed in a way that is understandable to a lay person". This indicates both a sense at the senior leadership level that such information needs to be interpreted, or at least translated, but also that such information is specialist. CISO14 suggested that they met the needs expressed by CFO2 when they stated that:

> "I don't just say that there's this flavour of ransomware and it's really bad and it could hit us, that means nothing, you know, I try to articulate that in a balanced risk-based way so that they can understand how vulnerable we are ... what the consequence would be perhaps in financial terms, yeah, and what we need to do and how much it might cost to mitigate that risk."

Not only have they interpreted the information from the perspective of its relevance to the organisation and its exposure, they have done so, according to them, in a balanced way, using language that they consider to be more understandable by their audience. This suggests a role for the CISO as an interpreter and translator, who also holds a position of power as a gatekeeper of information, as discussed earlier.

The CISO as advisor. The CISOs for these organisations performed a role as advisors to the organisation. This was summed up by one non-CISO participant who described the need to be told "no you don't need to be worried about that, yes you do need to be worried about this" (CEO1). Many CISOs articulated this role explictly, such as being "a trusted advisor to the business ... to provide guidance, provide advice" (CISO12). As advisers, they were trusted to provide "judgements" (CISO2) and had "shown ourselves to be discreet" (CISO10). They "worked with the board to make sure they understand the risk" (CISO3), or helped "the business understand ... its risks better" (CISO2), providing "assurance" (CISO4, CISO5) and "the advice and the guidance and the frameworks" (CISO7). An advisory role was contrasted with that of an enforcer by CISO8 who wanted to be seen as "more guide dog, less guard dog". CISO15 described being the person who

> "draws the goal posts for them [i.e., their internal stakeholders] and I will coach them to shoot and score, and I will keep score, but ultimately I have a very clear direct incentive to make sure ... that they score".

This suggests a variant of the advisory role, that of being a coach, although a coach that is also apparently a form of referee.

Cyber security as a foreign language. As well as information needing to be interpreted, there was a need for it to be relayed in words that its audience could understand. CISO4 described how they "speak in a language that actually is very business-specific rather than technology-specific", they "keep it as simple as we can ... as monosyllabic as we can". CISO8 noted how they wanted to "find a common language for talking to the board about security"; this common language was financial in nature, similar to the explanation given by CISO14 above.

CISO5 made an explicit reference to cyber security being a foreign language, expressing how "when you try to talk to anybody in another language you should at least know how to say please, thank you, order a beer" and stating that it was

> "incumbent upon a CISO or any head of security in whatever guise to teach the recipient how to speak pidgin cyber or pidgin IT or something that gives them a fighting chance to understand".

The same participant described how cyber-security professionals "almost speak in you know, hieroglyphics or we speak in ... language that nobody else speaks in".

Several references were made to cyber security being difficult to understand. Multiple CISOs described the necessity of analogy and metaphor in their communications, particularly with senior leaders. The CISOs also indicated that their stakeholders had a limited understanding of the subject, across all levels of the organisation. Senior leaders expressed the need for cyber-security messaging to be kept "as simple as possible" (CEO2). However, CISO5 expressed some frustration with having to explain cyber security to senior leaders in their organisation, as "no-one ever moans about having to be taught about engineering jargon".

The CISO as educator

A key role of the CISOs in this study was educating staff. References to cyber-security education were made by the majority of participants. This involved not just "making sure they're [staff] educated well" (CISO3) but also "[making] cyber-security meaningful for them ... on a personal level" (CISO11). There was a need to "educate" because, as above, cyber security was "another language" (CISO5). CISOs saw their role as "getting the business to be able to understand that security is important" (CISO1), suggesting that there was a need to counteract a pre-existing ignorance.

Education involved explaining “what we’re trying to protect and why” (CISO3) and relating security messages to “to things they might experience in their home life” (CFO2). CISO3 described how “if you can relate it to our business . . . what could go wrong and if you explain it to them, that makes a huge difference”, indicating both a contextual approach to their education as well as the value they perceived that context to add.

Various methods used by these organisations to educate staff and stakeholders on cyber security were mentioned, including “visual breakdowns” (CISO2) and “games” (CISO11), as well as testing of staff, particularly through simulated phishing attacks. Education covered all levels of staff, with senior leaders noting how they were “all being educated much more about cyber-security risks” (CEO2). There were indications of the deliberate use of fear in cyber-security education, such as the use of “war games [with senior leaders] . . . and you watch them shit themselves” (CISO11). CEO1 believed there was value in using fear, stating that “[when staff] see the art of the possible and it’s scary . . . they say okay, I’m gonna whine less”. CISOs acknowledged that “it’s very difficult for a conversation [about cyber security] not to gravitate back to being scary and inevitable” (CISO8) but were conscious of the risk of “scaremongering” (CISO5). Consequences relating to cyber-security incidents were also used as an educative tool. Publicity regarding other companies being subject to fines for cyber-security breaches were part of security messages, as “things like that have not done us any harm . . . that’s a big fine, so we need to start thinking about that” (CISO7), such incidents helping to underpin the CISO’s instruction.

Similarly, a large number of annual reports described mitigating cyber-security risk through the provision of training and education to staff. This was, in many cases, articulated as encompassing all staff. In some cases, specific mention was made of providing dedicated cyber-security training for senior management, including the recency of such education. In some cases, specific types of educative interventions were described in the annual reports, such as simulated phishing attacks.

Disciplinary aspects of cyber-security practice. As well as an educative role, CISOs appeared to have a disciplinary one. CISO5 described how “security’s job is to hold their [the IT department’s] feet to the fire” and CISO3 positioned their role as being to “hold IT to account”. There were “cowboys out there and that’s where you get the risk” (CISO1). Other CISOs articulated their role in enforcing controls, including “drawing the line” (CISO11), ensuring that instances of non-compliance were brought “back on track” (CISO12), and applying a “penalty” (CISO14). In one case, one CISO described "forc[ing] the company to shut down all the factories and do all their patching".[41] The role of the CISO as a form of organisational police was observed in the majority of interviews, although many CISOs explicitly resisted this identity. For example, CISO14 stated that they "hate the term police" but acknowledged that they do "act a bit more like the policeman". CISO3 referred to attempts to circumvent cyber-security controls resulting in "a disciplinary", adding "that's known". CISO12 referred to individual members of staff having "to face disciplinary action if they've done something wrong or even if they've done nothing wrong" in the event of a cyber-security breach. CISO8 explicitly referred to being "the moral police force of the company", and to being a "guard dog".[42] CISO1 described being "perceived probably as stop[ping] people having fun", and was concerned about this identity and its impacts on their relationships.

CFO2 believed that part of the CISO's role was to "raise the whistle" if there was "any poor behaviour". CISO7 referred to having this responsibility, identifying risk in one area of the business "that is endangering the rest of the organisation", and making it clear to the leader of that area that they did not "have the authority to ... accept the risk". CISO12 stated that "it's in their [individual business units] best interest for us to be aligned ... [because] every three months I report to the audit committee", suggesting a consequence arising from conduct that they considered to be risky, with an associated, implicit, threat.

The disciplinary aspects of cyber security within organisations, both in terms of discipling staff and in terms of organisations themselves being subject to discipline from governments and regulators, provided a further indication that cyber security was, in part, something to be feared. As explored in the first part of this chapter, this was associated with a sense of right and wrong, a theme I develop in further detail in the following section to establish how these moral aspects featured in CISO identity work. This provides a further foundation for the final section of the chapter, where I propose a metaphorical identity for the CISO that acts as an assemblage of the concepts explored thus far.

4.4 Morality and mysticism in CISO identities

In this section, I develop themes of morality in relation to cyber security which, as presented earlier, were consistently indexed throughout the data in this study, including right and wrong as well as harm and safety. References to crime and warfare also featured, contributing to the establishment of a moral aspect. Subsequently, I discuss

[41] Not attributed to limit the risk of identification.

[42] Although, as described earlier, their preference was to become more of a "guide dog".

aspects of mysticism which also featured.

There was also considerable positioning of cyber security as being good for society, with altruistic elements being explicitly called out by some participants. For example, CISO8 referred to cyber security as having "an altruistic element", both within the organisation and in wider society. This included "making it safe for children to use the internet ... making it safe for consumers to buy bus tickets ... be[ing] able to use the internet without fear" (CISO8). CISO12 expressed how they "try to improve for the benefit for the many". These comments implied that cyber security was a 'cause', that CISOs believed in what they did because it was 'right'. References were also made to changing "mindsets". For example, CISO4 described how they had "changed ... perception ... and actually created a much more open, enabling mindset" for their stakeholders within the organisation.

Several CISOs considered their role as being edifying for the organisation. For example, CISO13 stated "I see it on myself to ultimately get them [the organisation] to a better place and improve it". CISO11 described "dragging [the company] out of the dark ages of security into the modern contemporary security daylight" and CISO6 suggested that, without them, the organisation "would wander round blindly", both of these CISOs positioning themselves as providing some enlightenment to the organisation. CISO2 believed that their business would "live with a kind of ... fig leaf" if they were absent, and this would eventually lead to "a pretty serious failing". Similarly, CISO12 considered that, without them being there, "the businesses [within the organisation] would suffer ... because of some of the things I see". A number of these metaphors have, arguably, religious associations, an impression which I develop further in Section 4.4.2. These CISOs appeared to see themselves as saviours, and, in at least one case, as 'lone rangers', with CISO13 describing how they alone had "drive[n]" cyber-security improvements within their business and implying that, without them specifically, those improvements would not have occurred.

As described earlier, dialogue is of key importance in identity construction, including external discourse, with both the re-use and appropriation of specific language being of note, as described by Beech [124]. This is important to consider from the perspective of positioning cyber security as a moral concern, particularly where militaristic and value-laden language (such as 'cyber criminals' and 'gangs') is utilised. The repetition of terms such as 'arms race' and 'nation state hackers' within the cyber-security industry, e.g. [486] and within businesses, can be considered part of a process whereby this moral identity is continually reinforced and reconstituted. The use of value-laden language in particular is highly productive in identity construction, as noted by Cunliffe [253], and, therefore, the application of value-laden terms by CISOs, as observed in this study, is constitutive of a broader identity construct whereby cyber-security professionals are associated with aspects of morality.

Some organisations described cyber-security failings in terms of social impact, as well as reputational and financial impacts, which contributed to the positioning of cyber security as virtuous. In some cases, cyber security was implicated in organisational responsibilities for supporting wider society, such as through the distribution of food. Social aspects of cyber security within business were also observed, including a number of indications that these CISOs were acting as a form of social worker, encouraging the 'right kind of behaviours' within the communities they operated within. The external focus on ethical behaviour, and the threat of punishment, motivated these organisations to implement governance in order to maintain an ethical position. This governance included punitive controls, as well as the assignment of governors. As presented in the previous section, one particularly common cyber-security control observed in the data was that of education, an activity which has a strong moral tenor, as I now discuss.

4.4.1 Cyber-security education and morality

Education has a moral dimension, with an inherent association of right and wrong, as described by Foucault [336]. Education is also associated with both punishment and edification [336]. The CISOs in this study operated as a distributed judicial function, representing both the organisation's 'laws' as well as those defined by wider power structures, such as governments (via regulators), and the wider cyber-security industry (via standards). CISOs may be operating as one of the "judges of normality" [336, p. 304] referred to by Foucault, and as the "specialized personnel" [336, p. 174] required for discipline.

Heath argues that there is a need for moral education in business [397] and that this needs to focus on consequences. The CISOs in this study were following this approach, encouraging 'right' conduct by explaining the harm arising from 'wrong' conduct, such as the consequences of cyber-security breaches. Taking philosopher Kurt Baier's definition of morality as "following rules designed to overrule self-interest whenever it is in the interest of everyone alike that everyone should set aside his interest" [104, p. 314], risky cyber-security behaviours can be considered as amoral. A decision taken by an individual employee that is in their self-interest, for example, choosing to use a weak system access password that is easy for them to remember, may increase risk for the rest of the organisation. It is in the collective interest of everyone in the organisation for that employee to use a strong password that is less convenient for them, as this will reduce the likelihood of their access being compromised and, therefore, impacting on the organisation as a whole. Cyber-security education in business may result in what Heath describes as “neutralizing the neutralizations” [397, p. 611] used to justify amoral behaviour.

As introduced in Chapter 2, moral decisions require interpretation [220, 397]. As described earlier, the CISOs in this study functioned as interpreters, utilising expertise in order to enable the organisation to make decisions, similar to findings from other cyber-security researchers, e.g. [385]. The requirement for cyber security to be interpreted was clear, with its perceived complexity and specialist nature serving to support this need. Additionally, the references to cyber-security standards, such as ISO27001, and the incantation of these, further underpins the conception of cyber security as an interpretive practice. By calling out the existence of technical standards, there is an implication that those standards need to be interpreted. That interpretation must be carried out by experts, and only an expert interpretation would be legitimate as a result. Participants indicated that cyber security was an expert system, comprising technical aspects, e.g. software vulnerabilities, that could not just be taken at face-value; they required interpretation in order for risks to be related to the organisation.[43] These CISOs constructed an identity as an interpreter, but also as being *necessary*, with an implication that, without their role (or perhaps without them specifically), the organisation may under- or over-react to a threat. From the perspective of these CISOs, this role was not simply about evaluating threats however; it was about determining right and wrong. The moral aspects of cyber security enabled the CISOs to construct an identity of moral expertise. CISOs were positioned, both by themselves and by their stakeholders, as being arbiters of morality, as moral experts.

4.4.2 The CISO as moral expert

The CISO occupies a privileged position in being able to determine what is right and wrong with regard to cyber security. Cyber-security professionals more broadly enjoy a monopolistic domination of this authority, as with legal experts [156]. As experts, their interpretations are legitimised [156]. Their interpretation may also be influenced by additional factors such as geopolitics and mass media, which themselves index concepts of morality in relation to cyber security.[44] These moral dimensions of cyber security suggest that the purpose of a CISO may be to act as a moral expert [299, 388], to advise a business on what is right with respect to cyber security, particularly where determining what is right may not be intuitive or discernible due to the specialist nature of the subject. The existence of this moral expertise supports the business’s own identity as virtuous. However, as introduced in Section 4.2.3, this may be a “working

[43] Cf. the comment from CISO14 in Section 4.3.2.

[44] I return to these aspects in more detail in Chapter 6.

morality" [330] rather than a moral position that is firmly held by an organisation. The employment of a CISO may be "window dressing" [782, p. 16], providing what Goffman describes as "academically-trained experts who provide an aura of thought and respectability" [363, p. 239]. This may be in response to governmental messaging relating to cyber security, which may represent a "felt pressure" [330, p. 36]. Such pressure may result in shame avoidance, and motivate the organisation to take an instrumentally valuable view of cyber-security practice.

Cyber-security practice and value conflicts

In addition to the obligatory aspects of cyber security presented above in Section 4.2.3 and Section 4.2.4, an instrumentally valuable aspect of cyber-security practice for these organisations was also indicated by references that were made to cyber security being seen as burdensome. For example, CISO13 thought that their board saw cyber security "as something that is a bit of an inconvenience but we just need to manage [it] on the side and, therefore, we'll be creating a bit of noise about [it] every six months". They added that "they just see [it] as a problem that has to be kind of dealt with ... they just want the problem to go away basically". Similarly, CIO1 described how, "the chairman ... [is] not interested in it, he's pleased to know that the risk [has] gone away but thanks very much". CISO10 explained that they were trying to "find tools and capabilities that enable them [i.e., their executive leaders] to do their job with a minimum interference and that's a challenge". Similarly, CISO5 stated that "there's only so much people can put up with" with regard to cyber-security improvements, both process- and technology-based. This may have been exacerbated by an understanding that cyber security was "dull, it's boring" (CISO1),[45] with CISOs feeling the need to "make it a little bit more exciting and engaging" (CISO11) in order to counteract that impression.

An instrumentally valuable view of cyber security may conflict with a CISO's own view of cyber security as being intrinsically valuable, as indicated by the edificatory and altruistic aspects described earlier, motivating them to perform further identity work to counteract the instrumental view. This mechanism of conflict and identity work is summarised in Figure 4.3 below.

[45] A characteristic that has previously been identified by other researchers [385].

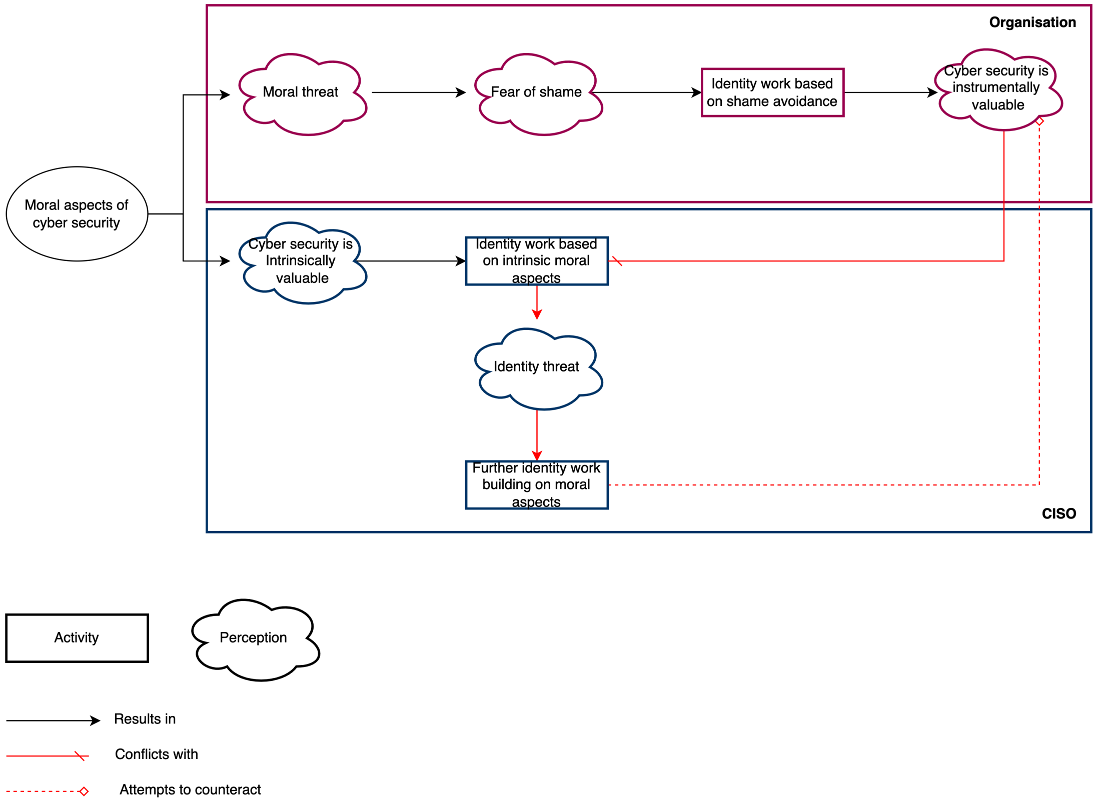

Organisation
Moral threat
Fear of shame
Identity work based on shame avoidance
Cyber security is instrumentally valuable
Moral aspects of cyber security
Cyber security is Intrinsically valuable
Identity work based on intrinsic moral aspects
Identity threat
Further identity work building on moral aspects
CISO
Activity
Perception
Results in
Conflicts with
Attempts to counteract

Figure 4.3: A summarised view, based on this analysis, of how moral aspects of cyber security may be perceived differently by organisations and CISOs.

As shown above, an organisation's view of cyber security as instrumentally valuable, that is, as an obligation and, potentially, as a burden, conflicts with the CISO's own view of it as being intrinsically valuable. The latter perspective is a factor in the CISO's identity work, who constructs an identity as someone that is associated with something that is, intrinsically, morally 'right'. However, the organisation considers the moral 'rightness' of cyber security as being determined by external perception and being *seen* to be 'doing wrong'. It, therefore, only does what is 'right' with regard to cyber security as a form of working morality. The result of this conflict is experienced by the CISO as an identity threat, who performs further identity work that indexes an intrinsically moral perspective of cyber security, in an attempt to counteract the organisation's perspective of it as being primarily of instrumental value. This cycle of conflict is one of the sources of organisational disengagement experienced by many CISOs in this study.

Contrary to a conception of cyber security as a technical discipline, and, by extension, the CISO as a technological expert, the most valuable feature of a CISO may, in fact, be their (perceived) moral expertise. This would suggest that, contrary to the views of some, but not all, participants in this study, a cyber-security professional's primary utility from the perspective of the organisation is socially focused. This may be a source of conflict or dissonance, both from the perspective of any professionals who see themselves in a particular way, but also from the perspective of other stakeholders, who consider the discipline to be a predominantly technical one and yet experience, and derive most value from, its social aspects. Having a moral identity, whether based on intrinsic value or otherwise, helps the CISO maintain their position; this may be a stronger or more stable identity than one that is solely based on a job title. If so, it serves the CISO's interest to maintain a moral aspect to the subject but, as will be discussed further below, it also serves wider interests at a societal level; positioning cyber security as moral reinforces existing narratives regarding those who are 'wrong', i.e., enemies.

Spiritual identity. Morality is not equivalent to spirituality, however, as there is often an implied connection between morality and religious belief, it is relevant to briefly consider spiritual identities. Theologian Chris Kiesling et al. identified in their study that "role-related spiritual identity is important in constructing ego identity" [471, p. 1276], referencing earlier work by Erikson [317] that suggested the same. They concluded that "spirituality offered … a profound sense of connection [for people] – through a relationship with their deity, with a spiritual community, *or with their most valued aspects of self*" [471, p. 1276] (emphasis added). As psychologist Douglas MacDonald states, "research involving spirituality as a whole is characterized by a pervasive and persistent shortcoming – namely, the problem of adequately defining what spirituality is in the first place" [519, pp. 533-534] and, given the "murkiness and inconsistencies in its definition" [519, p. 534], research in this area may be of little use. However, the connection between belief systems and identity is worthy of consideration, given the potential for a strong linkage between what an individual believes and how this influences how they see themselves, and indeed how they interact with others. References or implications to 'rights and wrongs' may also demonstrate an indexing of master societal narratives relating to religious myth, which can include emplotment of heroic characters [256, 348], as described in Chapter 2.[46] In the next section, I further explore aspects of belief systems that are analogous to cyber security, and to introduce this, I begin with a related discussion of how mysticism is indexed within cyber-security practice, again, grounded in the data from this study.

[46] The use of myth in organisational narrative has been explored by many other scholars, e.g. [349].

4.4.3 Cyber security as mystical or arcane

As well as having moral dimensions, this study suggested that cyber security was mystical. Beyond simply being a complex subject, it was “a dark art” (CISO4), “another language” (CISO5), “almost . . . hieroglyphics” (CISO5). It was “opaque and . . . pervasive” (CISO15), impenetrable and everywhere. Senior leaders considered it to “feel quite intangible” (CFO2) and relied on CISOs to interpret signs for them. CFO2 believed that cyber-security specialists “have a depth of knowledge and a smell and a sense for their particular area”, suggesting something beyond knowledge, an intangible “sense” for the subject. As a subject that was complex and mysterious, it required a specialist to make sense of it. If positioning cyber security as mystical benefits the conception of it as an interpretive practice, which, therefore, requires an interpreter, then this may motivate CISOs (and others with a vested interest in cyber security) to position the subject in this way, that is, to express it as a dark art. There was a common conception of those outside of cyber security being “lay-person[s]” (CFO2). One example was provided by CISO2 who described cyber-security risk as being “quite complex to convey to, you know, a lay-person”. The use of this language positions cyber security as a specialist subject, but also as something mystical, possibly even clerical in nature, a concept I now explore further.

Cyber security as a system of belief

Building on associations of morality and edification with cyber-security practice, as well as the mystical associations presented above, there were indications from a number of participants that cyber security was analogous to a system of belief. Besides the implicitly religious metaphors described earlier, such as ‘out of the dark, into the light’[47] and “fig leaf”, the use of metaphors such as “lay persons”, and the perhaps evangelical aspects of ‘changing mindsets’, there were a number of references that suggested cyber security was a cause for CISOs. For example, CISOs wanted to be “mak[ing] a difference to people” (CISO3) in their organisations and also saw themselves having “a responsibility to drive the next kind of generation of CISOs through” (CISO6) because “there’s not many of us around, and not many that kind of get it properly” (CISO6). This sense of ‘getting it’ with regard to cyber security was also articulated by CISO8, who was concerned about a change in organisational leadership where “the new guy doesn’t get it”, meaning that they would have to “start again”. Several CISOs articulated a need to ‘sell’ the concept of cyber security to the rest of the organisation, including the promotion of positive security behaviours, a need also found by security researchers

[47] This is a motif that, traditionally, has a spiritual dimension [264, p. 165].

Julie Haney and Wayne Lutters in their study of cyber-security advocates [385]. This may motivate not just edification, but also evangelism.

Working in cyber security meant being part of something bigger. CISOs wanted to "give back to the broader cyber community" (CISO11), to "share [cyber-security knowledge] with others" (CISO3), including "unofficially ... to friends and family" (CISO8). Cyber security was more than just a job, CISOs were emotionally invested in it. For example, CISO15 "worr[ied] that people [i.e., the organisation's customers] are placing trust in me without knowing whether they should or not".

The implicit associations of cyber security with belief systems also reinforce its moral dimensions. As a system of right and wrong, with an established doctrine that is seen as arcane and cryptic, even mysterious, that requires exegesis by specialists, cyber security can index the moral aspects of belief systems. These associations may also provide additional societal benefits in that there may be a perceived higher social status associated with being moral. The arcane aspects of the discipline could even be viewed as deliberate, enabling the maintenance of what Hobbes describes as "worldly Riches, Honour, and Authority" and keeping people "more in awe of their Power" [414, p. 708].[48]

The multiple references to cyber-security standards such as ISO27001 and those from NIST, as referred to earlier, suggest an almost doctrinal aspect to cyber security, an idea supported by the references to 'lay people'. More prevalent were references to pragmatism versus dogmatism, which also index belief systems. The majority of CISOs either explicitly labelled themselves as pragmatic, e.g. "I'm pragmatic" (CISO10), "you have to be very pragmatic" (CISO13), or were concerned about being seen as dogmatic, e.g. "they thought we were just being kinda dogmatic" (CISO3). This phrasing, as well as having ideological implications, also suggests an aspect of personal identity, in the sense of resisting a characterisation that may be perceived as negative. I now explore this resistance to dogma in more detail.

The CISO as heretic. Being associated with a domain that has aspects of an established belief system does not preclude resistance against this system. Resistance against orthodoxy can be a response to bureaucracy in such a system [488, p. 104] and, notably, being heretical does not necessarily result in less mysticism; heresies can claim greater mysticism than the dogma they are positioned against [488, p. 104]. Being heretical supports both the conception of cyber security as an interpretive practice, and as 'art not science'. Moreover, as mentioned above, many CISOs in this study either explicitly

[48] These quotations are from Thomas Hobbes' *Leviathan*, which is explored in more detail in connection with cyber security in Chapter 6.

labelled themselves as pragmatic or as not-dogmatic. The use of the word 'pragmatic' (seen in 13 out of 15 CISO interviews) implies a sense of interpretation; to be pragmatic or "realistic", both an analysis and a judgement are required. By suggesting the existence of dogma, a practical application of knowledge can be positioned as an alternative.

There was a strong aversion from CISOs to not being categorised as dogmatic, suggesting that there was a fear of this label being seen as the default with regard to cyber security. This is a form of identity work, an expression of being *not-X*. Even though they may be heretical, they may still be tainted by the association with something that is seen as a dogmatic belief system and the 'I'm pragmatic' protestation can be seen as an attempt to counteract that. This may also relate to a separate finding from the analysis regarding the conflicted identity of CISOs. One particular conflict was whether cyber security was, or should be, considered as part of IT. In some cases, this conflicted identity was observed regardless of the CISO's actual reporting line. If the IT discipline is associated with dogma then performing identity work to position oneself as pragmatic may be a reaction against being seen to be part of an IT function, serving to create an identity that is not just discrete, but specifically is *not-IT*. As mentioned earlier, being *not-X* can be an important factor in the creation and maintenance of identity [401] and *not-IT* and *not-dogmatic* are manifestations of such identity work.

The invocation of dogma lends support to the notion that cyber security is akin to a system of belief. Not only does it have a sense of right and wrong, there is also a sense of authority and accepted practice. CISOs in this study resisted the call of dogma, actively positioning themselves as heretical. I speculate that heretics are more acceptable, particularly in a society (considering an organisation as a society) that is more secular, and claiming to be heretical may be a response by CISOs to their being seen as outsiders, as observed in this study. I now discuss in more detail benefits that may accrue to CISOs from such identities.

4.5 Identity rewards

In this section, I discuss two principal categories of identity rewards that accrue to CISOs from the identity work described above. First, I begin with rewards that relate to the moral associations before discussing rewards associated with masculine associations of the domain.

4.5.1 Moral identity rewards

CISOs, and other cyber-security professionals, accrue a number of benefits from the positioning of their domain as moral. As discussed in Chapter 2, a role that is positioned as a 'defender' may offer "identity rewards" [174, p. 321], particularly if that defence is against threats that are morality-laden. Being associated with rights and wrongs, good and evil, may qualify cyber security as a "prestigious 'glamour industr[y]' " [75, p. 997] that offers "emotional rewards" [75, p. 997] for those that work within it. Cyber security may be arguably less glamorous than professions where identity rewards have been identified, such as advertising and magazine publishing [574], or film production [649], and may even be seen as boring by some [385]. However, given its associations with national security [570] and organised crime [570], as observed in the data, as well as with high salaries [345], it is not unreasonable to suggest an element of allure.[49]

Through the moral associations of the domain, those who work in cyber security may consider themselves as virtuous, as being on the 'right' side, and possess an identity as defenders, heroes, prophets, or missionaries [686]. This identity may be supported through undertakings they make to professional certification bodies, which include commitments to "[p]rotect society, the common good, necessary public trust and confidence ... [a]ct honorably, honestly, justly, responsibly, and legally" [3].[50] Such "commitments to ... moral principles" are linked with establishing and maintaining a moral identity [388, p. 499]. Additionally, cyber-security communities, and the wider cyber-security industry, which were both referenced in the data, provide support and foundations for moral concepts and ethical codes [409, p. 521]. Further, the cyber-security activities of 'threat hunting' [562] and 'insider threat management' [731], which were alluded to by some participants,[51] can be seen as what Sims describes as 'seeking out demons', providing a level of satisfaction[52] for those who are seeking them out. While the moral association of the role may also be considered to provide some job security, this was not the perception of a number of the CISO participants who were particularly concerned about the risks of scapegoating, as discussed in Section 4.3.1.

Cyber security, particularly in an organisation, may, like "[m]uch of everyday morality ha[ve] as its goal the prevention of collective action problems", as suggested by Heath [396, p. 365]. That is, amoral behaviour results in negative consequences for the

[49] However, negative consequences may also arise from an association with morality. Virtuousness can be associated with being "self-righteous, sanctimonious" [36], or be derided [20].

[50] The organisations in this study also made similar commitments to principles of governance and legislation in their annual reports.

[51] For example, CISO8 referred to having "an army [of staff] ... trying to find [employees] doing wrong".

[52] A "warm glow" [686, pp. 1637-1638].

wider population. If there are people doing wrong, then solutions are needed in order to protect against those people, which may require "costly investments in security and protection" [396, p. 365]. As a result, the cyber-security industry also derives benefit from the moralistic dimensions of the subject. Moralistic aspects of cyber-security discourse may, as Clegg et al. describe in their study of organisational identity work, establish "discursive norms and structures that will enable the market to be both created and exploited" [219, p. 510]. Moralistic narratives relating to being in trouble, e.g. [34], and being attacked by criminals, e.g. [27, 51], or by malicious, disgruntled or coerced employees [731], can lead to investments in security, even if such investment is "grudge spending" [245, p. 1197] [507]. This may be a factor in the cyber-security industry's continued growth, where consumption appears to be increasing at a significant rate [15].[53] Cyber-security crises have been reported as leading to increases in budgets [31] with a public breach affecting one firm leading to increased investment in other, unaffected, businesses [394].

4.5.2 Masculine identity rewards

Militaristic language has a traditionally masculine dimension and should be viewed in this light. Wider security discourse suffers from a masculine bias which perpetuates gendered language and concepts [769]. The cyber-security industry suffers from a lack of representation of women [479, 594, 621] and cyber-security discourse, both in mass media and in academia, commonly utilises masculine tropes; for example, the positioning of cyber-security workers as "shadow warriors" [795]. This bias contributes to the traditionally masculine and arguably paternalistic notion of being a 'protector'.

As discussed earlier, metaphors of war were observed throughout, including "attack" (CISO2, CISO3, CISO4, CISO14, CEO1), "defend" (CISO3, CISO15, CEO1), "war stories" (CISO3) and "war games" (CISO8, CISO11). Militaristic language relating to cyber security was also observed in a small number of annual reports. The close associations of cyber security with warfare may encourage, or lead to, an aspirational identity construct within cyber-security professionals to cast themselves in a heroic and therefore moral, and masculine, role.

An individual's identity work may also affect the identity of others, as they adopt, or adapt, what they have heard or otherwise experienced [253, 353]. References to cyber criminals and nation-state attackers, for example, whether "real or imagined" [353, p. 71], may function as what Gergen describes as "social ghosts" [354] that result in the

[53] Industry research suggests a marketplace valued at over $120 billion between 2019 and 2020, an average 10% increase year on year between 2017 and 2018 [15], with cyber-security spend growing significantly more than that of overall IT spend and a total number of cyber-security vendors estimated at over 1200 [10].

identities of organisational leaders being developed as both 'the attacked' but possibly also as 'commanders',[54] responsible for ensuring that appropriate defensive measures are taken.

As mentioned in Chapter 3, the majority of the participants, and all of those in CISO roles, identified as male.[55] Beyond militaristic aspects, other stereotypically masculine language and concepts were observed throughout much of the analysis. Some participants referred to their businesses being like a "bearpit" (CISO6), needing to avoid being "too soft" (CISO13) and being "browbeaten" (CISO1). Other stereotypically masculine metaphors were also used, such as cyber security being "those good six piston calliper brakes" (CISO12).[56]

Identity, including gender identity, requires ongoing construction and maintenance through performances [177, 187], and these performances rely on both structural and agentic aspects [129, 187]. The former includes disciplinary mechanisms in society such as policing and armed forces, while the latter can be seen through the deliberate self-labelling observed by a number of participants in this study. Aspects of punishment related to cyber security, whether enacted by regulators or by CISOs within organisations, may also be considered performative, as suggested by Foucault [336], and contributive to a masculine identity. Another performative aspect of identity construction in relation to cyber security can be seen by the references by one participant (CISO1) to the "fluffy" side of cyber security. This quote has parallels with a study by organisational scholars Caroline Clarke et al., where the phrase "pink and fluffy" as a descriptor of an individual was used disparagingly [218, p. 333], providing an example of how an anti-identity can be used both to define one's own identity as well as that of others, and to diminish them in the process. Such discourse may also help establish "a hierarchy", as suggested by Ybema et al. [793, p. 307]. I now develop the associations between cyber security and morality, masculinity and power to suggest several implications.

4.5.3 Wider implications of these associations

The association of cyber security with harm and safety, as well as with hygiene, that was observed in the analysis of the data provides moral legitimation, as these concepts

[54] A highly masculine identity.

[55] As do I. I caveat the statement regarding the CISO roles as not all participants provided the optional demographic information requested. For those that did not, I have made a (potentially inaccurate) judgement on their gender identity based on how they presented.

[56] Unrelated to cyber security, both annual report and interview data also featured multiple references to competition, another masculine archetype. A large number of the annual reports also utilised language that invoked other conventionally masculine concepts, such as aggression, conflict, strength, and even penetration.

have moral undertones [329, 344]. As morality is an established normative concept, an association with it makes cyber security more acceptable, perhaps even more 'real'. Positioning cyber security as moral also facilitates the implementation of controls, with moralisation historically being an instrument of domination [336, p. 285] and, as Heath describes, having a "primary function ... to impose constraints" [396, p. 360]. Where restrictions or controls are needed, or desired, a moral association may ease their acceptance by those being controlled.[57] If cyber security is a moral enterprise, there may be an unquestioning acceptance of actions taken in its name.

Cyber security can be used to wield power, through both repression, e.g. cyber-security controls, and influence, e.g. cyber-security education, each of which are methods of exercising power as described by Gramsci [371]. Cyber-security discourse may be "indexing different sources of power" [129, p. 269] through references to national security and intelligence agencies, as observed in this study. Further indexation from a moral perspective can be seen through references to nation states that pose a cyber-security risk. Both mass-media reporting and government rhetoric in relation to cyber security is consistent in portraying both a "growing and evolving threat" [21, p. 9] and known 'villains', e.g. [238, 597]. The nation states referenced in the data were existing Western enemies, providing a link to historical meta-narratives (and possibly indicating "hidden transcripts" [668]) relating to threats to the Western way of life arising from communism (in most cases) and also terrorism, supporting Neocleous's arguments relating security to a wider narrative with respect to the superiority of Western cultures and ideologies [568, p. 172]. These may be identity performances that are being "informed by the authority of historical, anterior voices" [129, p. 33] and hegemonic interests [375]. This indexation creates an identity of being on the 'right side' but also of actions taken against those threats as being morally justified, even morally necessary, as described by Bogain [145].

Cyber-security professionals in businesses may serve to support, and repeat, messages relating to a broader security agenda [568], both among a company's employees and their customers. The moral dimensions of cyber security, including the sense of being 'at war', supported by regular use of militaristic terminology, justify actions such as surveillance and policing of staff; as Bogain notes, along with morality, "[f]ear and danger are powerful legitimation strategies" [145, p. 487].[58] These actions have a regulatory effect, inuring employees, who are also citizens, to the existence of these controls,

[57] This also has implications in broader society as I discuss further in Chapter 6.

[58] Surveillance was positioned in a number of cases in this study as not just necessary for security, but also as itself contributing to ethical outcomes, as being beneficial from the perspective of 'the greater good'. This may suggest a utilitarian moral position [620], although exploring that debate is outside the scope of this thesis.

normalising their use in their personal lives and supporting a wider meta-narrative in relation to the questionable dualism of security versus privacy [568]. This also makes cyber security "highly visible", reinforcing power structures [375, p. 360].

Further, the positioning of cyber security as a geopolitical and military, and, by extension, moral, concern encourages spending. As a "military expenditure ... [it is] more reliable, easier to monitor and more effective in achieving the survival and goals of the system [the "industrial or capitalist systems"]" [116, p. 59]. The industrial society demands unending growth, and through growth, accumulates power [94]. Cyber-security risk presents ever-present and insoluble problems that require continued and increasing spending, driving growth and, therefore, power. Cyber security may provide a means through which demons can be not just maintained but made Legion,[59] plural and opaque, providing an inexhaustible well [379] of shadowy threats that solves the problem of ever "running out" [37]. The moral association, combined with the intractability of the subject, facilitates not just the conjuring of these demons, but also makes them less tangible, less reckonable – and, therefore, less verifiable; "the exorcism must never end" [379, p. 19]. CISOs may be inadvertently "colonis[ed]" [129, p. 31] by ideas that "serve hegemonic ends and preserve the status quo" [129, p. 31]. They may, as anthropologist Carol Greenhouse describes in relation to the politicisation of security, "fail to see the hidden transcript ... [and therefore] see like a state" [375, p. 366]. The heroic aspects of cyber security that index morality may also act as a form of control on CISOs and other cyber-security professionals by creating a "desired identity" [89, p. 203]. Political aspects of cyber security will be explored in greater detail in Chapter 6 and, to conclude this chapter, I synthesise a number of perspectives explored above to suggest a specific identity, and indeed possible purpose, of the CISO.

4.6 The CISO as soothsayer

In this section, I conceptualise the CISO as a soothsayer. This concept was developed based on multiple codes and categories from the analysis that suggested the fulfilment of this role, and it provides an overarching metaphor that brings together many different aspects of the analysis.

Soothsaying should not necessarily be viewed in a negative light. For example, it is notable that some mythical prophets have become more recognised as "lawgivers rather than magicians" [186, p. 35]. Historically, soothsayers have been "prophet-consultant" [264, 748] and totem [601], as well as "scapegoat" [748]. They are associated with 'reading' signs and interpreting information that would be unintelligible to a non-

[59] A biblical reference that connotes both plurality and the military [713].

soothsayer, e.g. animal entrails [228] or patterns in the stars [640]. As well as 'reading' information and assimilating data, they make judgements and advise their stakeholders on the path to take, even including which path is permitted. Some of this judgement is based on 'gut feeling' and soothsayers, as prophets, may have self interest in the realisation of their prophecies [748].[60] Soothsayers occupy a position of some jeopardy; if their stakeholders are displeased with their interpretation, or if they are seen to have failed, a soothsayer may lose their job, e.g. [11, 672, 688] or worse, their life e.g. [69]. In more modern times, nation states have employed the analogical role of 'futurists' to predict military threats, which include those related to cyber security; those nation states may take a futurist's predictions seriously, even when based on their own works of fiction [572].

Participants in this study articulated narratives wherein the CISO performs a specific role of responding to, or providing protection from, threats. This is what Czarniawska describes as a "*modern story*', in which "society and nature cause disequilibria, and science restores equilibrium" [256, p. 86] (italics in original). These stories, as expressed by both CISOs and non-CISOs, position the CISO and their discipline as the "science [that] restores equilibrium" [256, p. 86]. Without a CISO, senior leaders may look at data – i.e., signs – and make their own, inaccurate, interpretations. Such judgement based on signs is analogous to soothsaying practices of divination, an interpretive practice performed by "specialists" [228, p. 320]. References that non-CISOs in this study made to the capabilities of the CISO, such as CFO2 referring to cyber-security professionals having "a smell and a sense for their particular area", suggested something beyond knowledge, an intangible, arguably mystical, *sense* for the subject, possibly akin to divination.

The implicit associations of cyber security with systems of belief are also mutually reinforcing of the role that CISOs play as soothsayers, as is the existence of qualifications and professional associations regarding cyber security, e.g. [9, 18]. These are similarly analogous to soothsaying, in which "membership of a prophetic association" [157, p. 130] provided endorsement and validation.

Soothsayers or oracles were historically consulted for motives of politics [530] and warfare [233]. Tropes of warfare were used by participants in this study, including references to militaristic attack-defence concepts in relation to cyber security which are common in the cyber-security industry, e.g. [70, 289]. Such narratives are also seen in mass media, e.g. [55, 238], some with governmental origins, e.g. [147], and in academia, e.g. [463, 504]. In particular, the existence of a permanent emergency that necessitates specific attention being paid to cyber security appears consistent in security discourse.

[60] This point is explored in more detail later in this section.

Through the existence of a CISO, and statements that make its presence public, a wider narrative of cyber security as "permanent emergency" [568, p. 66] is supported, specifically as something that is a threat which needs to be addressed by businesses.[61] In order to be seen as defending the organisation from that threat, it is helpful to make that organisation *feel* like it is under attack. Using militaristic language enables the CISO to maintain this narrative but, crucially, as presented above, the nature of the attack is positioned as mystical or specialist, requiring a certain capability in order to be successfully defended against.[62] This enables the CISO to position themselves as a soothsayer; if there is war, then an advantage would be gained by going 'into battle' with a soothsayer on one's side, particularly to advise on aspects of that war that are not well understood.[63] This narrative, therefore, benefits from the existence of opaque threats that require interpretation.

4.6.1 The CISO as totem

The CISO as soothsayer also performs a semiotic function, particularly if viewed as a form of totem, as suggested in Section 4.2.3. CFO2 described how "having a particular person [as a CISO] gives us a focal point and makes sure that we do get much more rapid and frequent reminders of what is an important function", suggesting a partly symbolic role for the CISO in their organisation, and modern totems can include "oracles, experts" [601], the latter being a role that was clearly assigned to the CISOs in this study. Pettman describes how "totemic semiotics [are used to] ... frame, and make sense of, a largely hostile and uncertain world" [601, p. 8]. Organisations in this study articulated considerable uncertainty in relation to cyber security, associating this with threats to the continued viability of the organisation.[64]

Totems provide assuagement [601], a function I found to be provided by CISOs, as discussed briefly in Section 4.3.2. As totem, they function as an instrument of ontological security [601], and, as "medicine-man or wizard[65] ... ensur[e] the prosperity of the tribe" [186, p. 5]. As with soothsayers, totems are also used to predict the future [601]. In addition, the CISO as totem serves to indicate group membership [601, p. 22] and to indicate to observers the moral position of the organisation [241, p. 7].

Being a totem also contributes to the othering of CISOs, as identified in this study;

[61] Permanent emergency will be discussed further in Chapter 6.

[62] Given the masculine association of militaristic language, as discussed above, it is notable that soothsaying historically was a profession that was dominated by male practitioners [186].

[63] But also to act as a totem, indicating to anyone observing the warring party that it is defended against such threats. These totemic aspects are developed further below.

[64] Uncertainty is explored in more detail in Chapter 5.

[65] These gendered terms unfortunately borne out by the gender imbalance in this study, and the wider CISO community.

a totem may be “a ‘frenemy,’ who could turn on the subject at any moment” [601, p. 9] and may have a disquieting effect [601, p. 10]. Othering may result from an impression that totems are “tricksters” [601, p. 27], something I now explore.

4.6.2 Cyber sophistry

The CISO plays a role in not just interpreting, but also relaying information. They hold a position of power, and that power provides opportunities for sophistry. As presented earlier in this chapter, a number of participants, both CISO and non-CISO, were aware of these opportunities. It is not just in the interpretation and the associated judgement but also in the communication of that judgement where the CISO can exert influence. This influence may be self-serving or may serve to support others within the organisation. Regardless, there is a suggestion from the analysis of the data that their interpretations may not be entirely objective. This may result in undesirable outcomes of reduced security due to ineffective allocation of resources [334].

The positioning of the CISO as a soothsayer may be performed by the incumbent as a response to perceived threats to their own identity, as identified in this study and similar to identity issues identified by other researchers, e.g. [97]. Ethnographer and scholar of folklore Natalie Underberg describes how “a prophet, a figure at times not at the center of social life and who sometimes delivers prophecies that will not be well received, can be in danger of becoming a scapegoat” [748, p. 148], and security itself often carries associations of blame [479]. As discussed in Section 4.3.1, the CISO role is one that is at risk of scapegoating. As modern soothsayer, they may even lose their job as a result of proclamations which displease their masters [672, 688] as well as for perceived failures [11]. The risk of displeasing their audience may be high as “credibility of oracles depends on their apparent wisdom, and apparent wisdom is defined by the beliefs and opinions of those to whom it must appear as wisdom” [157, p. 126]. Their proclamations may also be impenetrable and ambiguous, something observed historically, e.g. [530].

As with soothsayers, CISOs can have a self-interest in the realisation of their own prophecies, a position that may motivate unscrupulous behaviour.[66] The CISO’s role in regulating information provides them with significant influence and potentially allows them to help secure their own future. Predicting an ever-increasing number of ‘sophisticated’ threats may deter their stakeholders from considering their replacement or removal, and multiple CISO participants made reference to development of long-term cyber-security plans, perhaps indicating an attempt to secure their positions for longer.

[66] Perhaps being aware of the precarity of their role, CISOs are like other prophets who “are said to know the time and place of their own deaths” [748, p. 152].

A dynamic may exist whereby the greater the perceived threat to their position, the greater the effort in securing their future. Cyber-security threats play multiple parts in this dynamic. The greater the threat, the more likely a breach is to occur that could ultimately cost the CISO their job, if they are scapegoated for it. However, the greater the threat, the more weight the CISO can put behind their own agenda. Therefore, although it may be in the CISO's interest to articulate the existence of such threat, it may be more in their interest for those threats not to exist.

Self-serving aspects of the cyber-security industry

A CISO could have an "obsession with security" [190, p. 37] that results in negative outcomes for a business, perhaps due to over-provision of information [312]. As suggested earlier, identity threats may be deliberately constructed by individuals [177] and extended by others, becoming established narratives within a collective [177]. Identity threats may, therefore, be advantageous to an individual or group, such as the CISO community and the wider cyber-security industry, which may lead to their deliberate construction and continued usage.

The wider cyber-security industry may also be motivated to perpetuate discourse that positions the discipline as requiring interpretation by experts, but also the consumption of goods. As well as benefiting the industry [568], this benefits a consumption-driven society more generally [116]. Cyber-security predictions made by other modern-day soothsayers such as so-called 'futurists' can be seen to be influenced by purely commercial desires, e.g. [572], which may motivate predictions of a worsening security climate [334]. Further, narratives of permanent emergency and associated threats, as repeated by CISOs and the wider cyber-security industry, serve to maintain a position of power for that industry and also support broader societal agendas which benefit from an ongoing sense of insecurity [568], as will be explored further in Chapter 6.

The benefits of a soothsayer identity

Business narratives that consider security as a necessity can be indexed by cyber-security professionals in order to construct identities of protectors, of being 'on the right side', and of being necessary. As mentioned earlier, identity can depend upon being present in other people's minds [685] and, therefore, not being present, i.e., not being thought about, poses a risk to that identity. Exciting narratives relating to cyber security abound, particularly in the media, including nation-state attacks and threats to critical national infrastructure. These narratives help to maintain the continued presence of cyber security in the minds of others and, by extension, help to maintain the CISO's identity within an organisation [685]. As suggested above, cyber security has an element of glamour which is emotionally rewarding to be associated with [75, 649], and such rewards may motivate identity work, both by practitioners and by businesses, in order to be associated with such glamour. The (perceived) opacity of the subject, and its mystical nature, further support that appeal.

The positioning of cyber security as 'art not science', alongside its positioning as 'a dark art' may be attempts by CISOs to modify or enhance their identity in order to maintain their position. If they consider themselves to be in a precarious position, then cyber security being considered a science, i.e., as repeatable, methodical, established, is threatening, as that would imply the relative ease of their replacement. If cyber security is a 'dark art', on the other hand, i.e., mystical, arcane and requiring interpretation, then their replacement is more problematic. In other words, it is easier to replace a chemist than a soothsayer. This conception as not-science and the need for a soothsayer may be facilitated or underpinned by the lack of an established scientific basis to cyber security [334, 404] – or even vice versa. These narratives may, therefore, have a perlocutionary effect on cyber-security stakeholders, both inside and outside of an organisation.

4.6.3 Implications of the CISO-as-soothsayer

My intention here is not to position cyber security in the same category as either astrology or haruspication, however, soothsaying offers a rich metaphorical resource with which to view the role of the CISO. Cyber security is an interpretive practice, as others have argued, e.g. [404], and, therefore, should not be approached as a binary, 'are we secure?', determination – it needs specialist interpreters to advise on the level of risk. The CISO is not employed to 'make things secure'. Indeed, as security scholars Cormac Herley and Paul van Oorschot make clear, it is indisputable that 'being secure' cannot be proven [404], if indeed it can be considered as a binary state. Rather, the role of the CISO becomes one of advising on the level of risk, at least at the most senior levels of the organisation. Accordingly, rather than being a role of 'securing' – or indeed 'policing' – an organisation, the CISO role is more akin to weather forecasting. Orienting their role away from 'securing' towards 'weather forecasting' also serves the CISO: they may be less likely to lose their job as a result of an inaccurate weather forecast (although a series of inaccurate forecasts would likely still lead to that result). Indeed, this study shows that the perceived precarity of the CISO role leads to self-serving actions. Managers and practitioners should be conscious of the potential for cyber-sophistry and the unhelpful outcomes that can result [334]. This may require additional cyber-security expertise to exist at senior levels within an organisation, possibly in a non-executive capacity, in order to identify and challenge this, particularly given the inability to disprove many security-related affirmations, as highlighted by Herley and van Oorschot [404].

The mystical associations of cyber security also have an impact on how cyber-security education is approached. Approaches to education relating to cyber security could either aim to demystify it, or, alternatively, to acknowledge the mysticism and thus reinforce the need for specialist interpretation. If adopting the latter approach, education of staff may be best approached as instruction in the use of systems in a secure way, with the security aspects of this education being implicit rather than explicit, and certain decisions on acceptability of risk being deferred to cyber-security specialists. For example, rather than training staff how to identify phishing emails, an organisation may place more focus on the cyber-security team filtering emails before they reach staff. Equally, rather than training developers on common cyber-security threats, organisations may focus more effort on specialist testing and associated risk assessment of systems before implementation. These options are, however, potentially problematic if they result in end users feeling less responsible for security and depending entirely on technological protections, becoming themselves powerless in the process. Additionally, end users will always need an element of preparedness for security-related incidents. However, as with much in security, educative approaches should be viewed as a continuum rather than in a binary manner, and a change in focus that results in secure behaviour without necessarily involving explicit articulation of security specifics may ultimately lead to a more user-centric security approach, as called for by others, e.g. [623], where employee experience is foregrounded.

The question of whether cyber security is a dark art or not is perhaps obsolete. However, if it is *considered* a dark art then systems should be designed on the basis that their security will need to be interpreted by a specialist, in order for that specialist to advise the users of that system as to the level of risk that it poses, and how it may be mitigated.[67] To make that easier, there may need to be a minimum level of information provided with a system in order to make that task simpler or more standardised. As an analogy, specialist parts for domestic goods often have a separate 'advice/information for installer' section. That is, where there is a section for the purchaser to read and familiarise themselves with, there is also a separate section for the installer. Employing this analogy, a similar approach for security systems could be considered: an 'information for CISO' section to be provided at point of purchase. Similarly, as noted above, developers should not approach security in a binary, 'is it

[67] This may even go as far as advising users whether that risk is acceptable or not. Examples of this were observed in the data, where CISOs were expected to make that decision on behalf of the organisation's leaders, conflicting with normative assumptions that executive and supervisory boards alone determine risk tolerance.

secure?', manner. They may need to appreciate, particularly in organisations, that security-risk decisions require interpretation by a specialist that the organisation has appointed.

While others have highlighted the lack of "science" in cyber security, e.g. [334, 404], and problematised its practice in organisational contexts, e.g. [97, 421, 464], I introduce a different perspective. Rather than attempting to make security "more scientific" [404, p. 114], perhaps there is greater value in acknowledging the interpretive nature of cyber-security practice, particularly within commercial organisations, and reclaiming soothsaying as a beneficial advisory profession, rather than seeing the term in a negative light. Even sophistry can be viewed positively, with "[e]ffective communication, including pedagogy and sound argument, [being] critical to prosperity" [370, p. 23], and perhaps it is especially important to distinguish between sophistry and "rhetrickery" [152, p. 7]. Therefore, rather than only exploring the 'what' of cyber-security behavioural interventions in organisations, e.g. [121, 236, 474, 571, 624, 681], there is value in future research also exploring the 'how' and identifying the most effective means of educating and communicating desirable behaviours and practices, particularly among the non-expert actors on whom effective security depends [623]. Effective cyber security may depend less on policy and control, themselves ineffective [96, 474, 479, 607], and more on communication and collaboration. This has an implication on recruitment. Others have already highlighted the need for CISOs to have effective communication skills, e.g. [421], and alongside this, the need for advisory and forecasting skills should also be considered. As well as being able to evaluate risk, CISOs need to be comfortable with providing advice regarding, and making recommendations on, the acceptability of that risk, and being clear with their stakeholders as to the implications of their advice. Such an approach needs to be followed with all stakeholders within the organisation, not just leaders, as collaborative engagement at all levels is crucial to effective security outcomes [97, 623].

Organisational leaders themselves should rely less on the CISO-soothsayer as protector, totem and scapegoat and more on them as advisor, forecaster and educator. Shifts in thinking such as this will help organisations to develop and improve their security measures collectively, rather than as the responsibility of one person or function. Unclear responsibilities, and confused, misunderstood and multifarious roles, lead to conflicts within organisations that ultimately increase their cyber-security risk. The aspiration should be to build a truly collaborative approach to cyber security [367], with multiple actors playing their part [623], and resolve the otherwise disconnected and othered state of the CISO [96, 97, 421, 464, 623], as well as improving overall organisational cyber security.

4.7 Summary

This study has shown that cyber security is enmeshed with business identity; a business's identity determines their attitude towards cyber security. Cyber security itself then is both a component of that identity and a threat to that identity. I have found that the businesses in this study experienced cyber-security threats as ontological, that is, threatening to their very existence or state of being. These organisations performed identity work in response to this ontological threat in order to assuage their feelings of insecurity and, therefore, feel protected, as well as to publicly present an identity of *being* protected. This identity was maintained through discourse and communicated to their stakeholders, in part, through public statements made in their annual reports. These businesses sought to appear as ethical or moral, with cyber security being associated with these aspects. The purpose of a CISO and their function may, therefore, be to *externally* affirm the organisation's identity and *internally* respond to a sense of ontological insecurity that they experience as a result of an emotional response to threats that exist in the external environment, including those arising from wider narratives. Their responses to such threats may support both their own drive for ontological security but also that of the society they operate within.

A business that demonstrates that they employ someone in a role that helps defend the business against cyber-security threats is performing identity work on its own behalf. However, this also sustains the identity of the person employed in that role, giving that individual a greater sense of their own ontological security, both as a person who has a clear identity as a defender but also as a person who is valued and necessary, and, therefore, likely to continue to be employed. Identity work that relates to cyber security can, therefore, be seen as beneficial to both parties, business and CISO, and this can be extended to other interested actors, such as governments and the cyber-security industry. Encouraging businesses to address cyber-security threats through the use of dedicated functions can itself be seen as identity work performed by governments in order to address the ontological insecurity they feel as a result of cyber-security threat, and may also accrue additional benefits to those governments in terms of normalising surveillance [552, 568].[68]

Cyber security as a domain has a number of moral dimensions, being associated with good and bad, right and wrong. I have not set out to demonstrate whether or not there is any 'truth' in these associations but rather to show that they are indexed by both organisations and CISOs in constructing their identities. This study of a range of UK businesses has shown that the moral aspects of cyber security were beneficial to

[68] Wider geopolitical themes of cyber security in business are explored in Chapter 6.

these businesses in constructing an ethical identity, with cyber-security risks themselves being threatening to that identity. These organisations were able to make use of cyber security's moral dimensions to help construct or maintain an ethical identity, as either being an organisation that 'does the right thing', or an organisation that is 'doing good', or both. I have also shown that cyber-security leaders index these moral aspects to construct their own identities as moral experts and derive benefits as a result. These identities, both organisational and individual, were created and maintained through discourse, both verbal and written, with moral aspects of organisational identity being communicated by these business to their stakeholders through their annual reports. Moral aspects of cyber security may support hegemonic interests by maintaining power through increased spending, encouraging acceptance of intrusive disciplinary controls, and supporting the othering of competing hegemons. The abstract nature of cyber security allows for a potentially bottomless source of evil spirits from which defence will always be necessary.

This study has also shown that the role of the CISO comprises several functions akin to a modern-day soothsayer for an organisation. The CISO sits at a nexus within that organisation, consuming opaque information from multiple sources and making decisions based on their interpretations and what they judge to be appropriate or 'the right thing' for their stakeholders. Having a soothsayer benefits the organisation, not just through the role it performs, but also how it contributes to the organisation's own identity; as a legitimate, and defended, entity. Being a soothsayer, however, has downsides. The CISO can be scapegoated or othered, and can feel detached from the rest of the organisation.

This study has implications for both those performing the CISO role and their stakeholders. For CISOs, it would be beneficial to reflect on how such an identity affects, both positively and negatively, their interactions and practice within their organisations. Such reflection can also help them to come to terms with the detachment and alienation many of them experience within those organisations. For organisational leaders, it is useful to consider whether employing a soothsayer is indeed what they have intended, and also whether this represents an abdication of responsibility in decision making. By relying on a soothsayer to 'read the signs' (i.e., to provide the weather forecast) they may deliberately be facing away from confronting a problem more directly – or perhaps they are deliberately looking for someone to blame in the event of disaster. It may indeed be beneficial for all parties if the CISO is treated as a weather forecaster instead of a security totem.

Chapter 5

Risk

This is the second of three chapters that interpret the findings through multiple analytical lenses. This chapter focuses on concepts of risk.

5.1 Introduction

The chapter is structured into four main sections. First, in Section 5.2, I discuss how cyber security represented uncertainty for the businesses in this study. Next, in Section 5.3, I explore dutiful aspects of cyber-security risk management and how these manifested in the analysis of the data. I then turn to a discussion of risk management through controls in Section 5.4 before examining value and a number of paradoxes associated with risk management in Section 5.5. Finally, I summarise my contributions in Section 5.6. Throughout I present key additional literature, to build on that introduced in Chapter 2, that supports the concepts discussed and the interpretations I make, bringing this into conversation with the findings. Quotations from participants[1] and paraphrases from annual reports[2] are included where relevant to exemplify or support a theme or interpretation from the analysis.

5.1.1 Why risk?

Concepts of, and language relating to, risk were prevalent throughout the data, both from the annual reports and from the interviews. Themes that were identified through the analysis were brought into conversation with the literature in further cycles of analysis, which demonstrates the reflexive nature of this study. Applying existing theories relating to risk and risk management as part of the analysis process has enabled

[1] Indicated by double quotation marks.

[2] Indicated by single quotation marks.

deeper interpretation of the findings from the research. As well as "form[ing] a key aspect of daily experience" in modern (Western) society [447, p. vii], risk, and risk management, is embedded within corporate business [135], which makes it particularly relevant to the present study. Further, responses to risk are closely associated with identity [447], and risks can be deployed for political motives [123]. Therefore, as well as providing a useful analytical foundation with which to derive greater meaning from research findings, risk management also provides an apposite bridge between themes of identity explored in the previous chapter, and themes of politics and control that will be explored in Chapter 6.

In Figure 5.1, I highlight the relevant themes from the meta-analysis mentioned in Chapter 3 that are predominantly covered in this chapter.

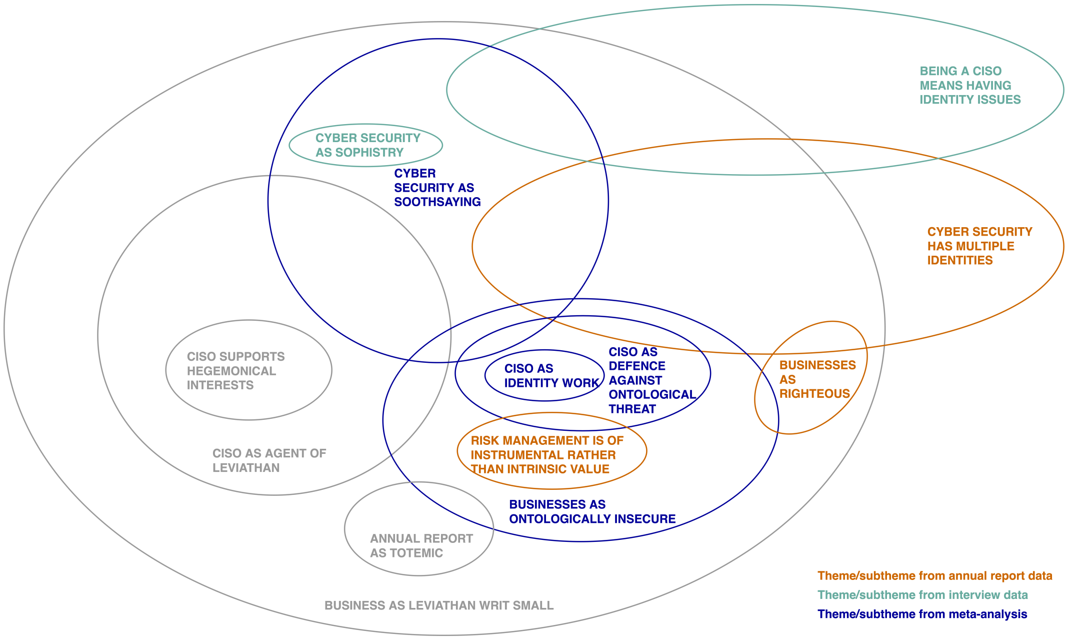

BEING A CISO MEANS HAVING IDENTITY ISSUES
CYBER SECURITY AS SOPHISTRY
CYBER SECURITY AS SOOTHSAYING
CYBER SECURITY HAS MULTIPLE IDENTITIES
CISO SUPPORTS HEGEMONICAL INTERESTS
CISO AS IDENTITY WORK
CISO AS DEFENCE AGAINST ONTOLOGICAL THREAT
BUSINESSES AS RIGHTEOUS
CISO AS AGENT OF LEVIATHAN
RISK MANAGEMENT IS OF INSTRUMENTAL RATHER THAN INTRINSIC VALUE
BUSINESSES AS ONTOLOGICALLY INSECURE
ANNUAL REPORT AS TOTEMIC
BUSINESS AS LEVIATHAN WRIT SMALL
Theme/subtheme from annual report data
Theme/subtheme from interview data
Theme/subtheme from meta-analysis

Figure 5.1: Meta-analytic themes covered in this chapter. Themes not covered in detail are greyed out.

The identification of these themes inspired the use of risk as an analytical lens and map onto the sections in this chapter as shown in Table 5.1.

Table 5.1: Mapping of meta-themes to sections in this chapter

Section	**Meta-themes**
Section 5.2	Businesses as ontologically insecure
	CISO as defence against ontological threat
	Cyber security as soothsaying
Section 5.3	CISO as defence against ontological threat
	CISO as identity work
	Businesses as ontologically insecure
	Businesses as righteous
	Cyber security has multiple identities
	Cyber security as sophistry
Section 5.4	Risk management is of instrumental rather than intrinsic value
	Cyber security has multiple identities
	Cyber security as sophistry
	CISO as identity work
	Businesses as ontologically insecure
	Businesses as righteous
Section 5.5	Risk management is of instrumental rather than intrinsic value
	Being a CISO means having identity issues
	Cyber security has multiple identities
	Businesses as ontologically insecure
	Cyber security as soothsaying
	Cyber security as sophistry

A summary of the themes that are represented in each of the core sections of this chapter.

Table 5.1 illustrates the reflexive nature of this work, showing that themes developed from the analysis are reflected throughout the different sections of this chapter, where they are discussed in the context of existing theories of risk.

5.2 Cyber security as uncertainty

As described in Chapter 2, uncertainty and risk are distinct, but related concepts [478, 563], with the latter characterised by its measurability [478].[3] Risk management, as a concept, is what Mythen describes as the attempt to "control and predict the future" [563, p. 14], which provides a crucial thread from the metaphor of soothsaying employed in Chapter 4.

For the businesses in this study, uncertainty was a common concern, as it affected their survival.[4] The annual reports made reference to various sources of uncertainty including the economic, political and regulatory environments that these businesses

[3] Aspects of measurability of risk are discussed further in Section 5.4.2.

[4] As explored in Chapter 4.

operated in, the broader international nature of their operations, merger and acquisition events, and competition. This uncertainty was considered to be growing by many of these businesses. Attempts to control this uncertainty at source were identified, particularly in relation to direct engagement with governments and regulators to influence future regulations and legislation. These businesses wanted to be able to control uncertainty and 'predict' its occurrence. Some saw that uncertainty as presenting opportunities to be exploited but most businesses wanted to 'defend' against it. Any disruptions to their businesses were considered as impacting upon their ongoing viability, and a number of these organisations graded their risks on a scale that included catastrophic impacts.

Cyber security was specifically identified as a type of uncertainty in the majority of annual reports. This was evident in conjectural statements relating to non-compliance with security standards and future breaches, as well as explicitly, albeit sometimes generically,[5] referring to cyber security as a key risk facing the organisation.[6] In the majority of cases, cyber-security risk was categorised as being highly concerning for the organisation. This included, in some cases, explicit statements relating to the level of attention that this risk was receiving from the organisation. For those businesses that indicated a direction to the severity of cyber-security risk in their annual reports, the majority described this as either increasing or unchanged,[7] with a very small minority describing it as decreasing. As discussed in Chapter 4, part of the role that the CISOs performed in these organisations was in providing assuagement that helped them cope with the uncertainty relating to cyber-security risk.

As articulated in the previous chapter, determining a response to this uncertainty required interpretation, and judgement, by experts.[8] This process was intended to transform uncertainty into risk, i.e., to make it predictable and, importantly, measurable. This is summarised by NED1's requirement to understand, in relation to cyber security, "what is our risk? what is the level of that risk? what is the reality of that risk?". For some non-CISOs, cyber security felt "quite intangible" (CFO2) and there was a need to be told "no you don't need to be worried about that, yes you do need

[5] For example, simply referring to 'cyber security' under a heading of risk without further detail.

[6] All organisations mentioned the existence of cyber-security risk and, to a greater or lesser extent, how the organisation mitigated that risk. In a very small number of cases, cyber-security risk was either shown as a low priority risk or was absent entirely from the list of key risks affecting that business. Also in a small number of cases, cyber-security risk was referred to as being 'new' to the organisation's list of key risks. In a small number of different cases, cyber security was described as a previous organisational weakness.

[7] Approximately the same number of organisations positioned this as increasing versus those that positioned it as remaining unchanged.

[8] In the annual reports, this need for interpretation was not limited to cyber security. Other areas of uncertainty were also described as requiring interpretation and these equally relied on both internal and external expertise.

to be worried about this" (CEO1). CISO4 described how determining the response to cyber-security risk was "quite complex ... there's no one size ... that we prescribe", invoking not just the language of a tailor but that of a medical practitioner as well. As discussed in the previous chapter, the CISO here is in a position of power, being able to prescribe to the organisation what its approach to managing the uncertainty associated with cyber-security risk should be.

The uncertainty associated with cyber-security risk was also evident in relation to its depiction as a continuum. CFO2 highlighted this by stating that "we don't gold-plate it I wouldn't have said, but we don't short-change it", implying that there is a 'range', a continuum from short-changing to gold-plating, with regard to security. This also implies that it is necessary to determine where on this scale an organisation should be placed. CISO7 used similar language when describing how they agreed risk tolerance with their board as "we're not going to be gold-plated". They further noted a "subtlety between 'do you want good practice or best practice' " when talking to their board about risk tolerance. By asking this question, they are both constructing the continuum and their role as an interpreter of the continuum, and of being capable of helping their stakeholders determine where on that continuum they 'should' be.[9] Further examples included CISO12 describing "a certain baseline they need to achieve and in security that's where I come in" and how, within their organisation, they set each individual business unit a "bar" to achieve with regard to cyber security. These examples indicate that the CISO plays a role in facilitating the organisation's understanding of its "risk thermostat" [68, p. 15], but also that they are influential in actually setting the thermostat. In so doing, by setting the "bar" that CISO12 described, they are able to determine the organisation's tolerance to cyber-security risk and, by extension, adjust how it responds to that risk. As well as demonstrating their power, this indicates the potential for a conflict of interest. If organisations, or their leaders, are not confident in setting their own cyber-security risk thermostats then relying on an individual who may derive benefit from the thermostat being set at a particular level could be akin to allowing one's energy provider to determine the temperature of one's house.[10] This further supports the suggestion in Chapter 4 that organisations may benefit from having independent cyber-security expertise at a senior level that can provide additional verification that the thermostat is indeed set at the correct level.

In some of the annual reports, planning for future negative events was articulated

[9] They added that not achieving best practice amounted to "just common sense stuff". This perhaps undermines the idea of there being a need for a specialist interpreter. However, it may be the case that this 'common sense' is only common to specialists.

[10] Although it may not be unreasonable for an energy provider to at least make recommendations in this regard.

as a characteristic of being a 'well run' business.[11] Part of the motivation for being a 'well run' business was associated with a sense of duty.

5.3 Cyber security as a duty

In the previous chapter, I proposed that one purpose of the CISO is to act as an organisation's moral expert. Here, I build on this concept to advance that part of their role is being a seeker, and preventer, of recreancy, a concept introduced in Chapter 2 that itself has moral associations.

As discussed in Chapter 4, cyber-security risk management was seen by many of these businesses as an obligation, and one that was being watched, and judged, externally. To recap, examples of a dutiful aspect to cyber security included references to organisations having a "responsibility" to protect customer data (CISO3), descriptions of cyber security as "something that [senior leaders] have to be concerned about and that they have to show that they're concerned about" (CISO13) and CISOs referring to organisational compliance with cyber-security requirements as being achieved "because you had to, not because you wanted to" (CISO15). In addition, several annual reports described a 'need' to meet obligations in relation to cyber security, and participants referred to this both in commercial and regulatory contexts. For example, CFO2 described how "you don't get to operate in that space or bid on that type of business if you don't have the [cyber-security] framework in place" and CISO14 referred to "a whole raft of formal compliance and government obligations". CISO4 felt that their organisation was "under a [regulatory] regime" and one CEO made specific reference to obligations imposed by the UK government that related to national security. A duty, an obedience even,[12] with regard to 'doing the right thing' in relation to cyber security was expected of organisations by not just regulators and governments, but also customers and broader society.

These organisations cascaded that concept of duty to their employees, with CISOs playing a role in establishing both what was required and how recreancy would be dealt with. The CISO had "a duty to communicate risk" (CFO2), which included identifying risks that were inadvertently distributed within an organisation.[13] This was explicitly indicated by CISO7, who pointed out to one of their senior leaders that they did not "have the authority" to accept risk that could impact the whole organisation. Where recreancy was identified, the CISO would administer punishment, such as "holding [the IT department's] feet to the fire" (CISO5) or applying a "penalty" (CISO14).

[11] I return to aspects of being 'well run' in Section 5.4.

[12] A concept explored further in Chapter 6.

[13] Applying Beck's perspectives on the distribution of risk [122, 123], as discussed in Chapter 2.

Instances of recreancy were actively sought out, as indicated by CISO8's description of the role that CISOs played as being "the moral police force of the company". This sense of recreant behaviour resulting in punishment echoed the wider narrative from government in relation to cyber security, whereby these organisations were concerned about actions taken by governments and regulators, for example, "massive" regulatory fines (CISO9) and "sanctions from government" (CFO2), if they failed to fulfil their duties.

There were also indications of duty in relation to the role that these businesses played in broader supply chains,[14] and the risk that their own supply chains posed to them.[15] Therefore, CISOs in these organisations were both identifying recreancy and reminding staff members of their duty to the organisation, and its stakeholders, with regard to cyber-security risk.

5.3.1 Trust

The importance of trust was highlighted by a number of CISOs when discussing controls, particularly with controls that could be considered surveillant. This was also implied by the deference that one CEO showed to surveillance conducted by state actors, suggesting that intrusive controls were acceptable to them if those controls were managed by actors that they trusted, and that they obtained a perceived benefit from that intrusion. They described how "[various governments] keep an eye out, which works in ways that neither you or I need to know how it works" (CEO1). A supposed dualism between freedom and security is common in security rhetoric [568]. Such dualisms were present in the data, with CISOs referring to the privacy implications of security controls, and both CISOs and non-CISOs referring to convenience impacts, both for staff and for customers. For example, CISO8 described the need for "a balance between inspection and surveillance" and CISO4 stated that a business needed to tolerate "disruption . . . in order to do the right thing".

From the perspective of a CISO, it is important that they are trusted by those in the organisation who they are subjecting to controls, not just for the sake of their own interactions and a sense of inclusivity, but also to ensure that those controls are effective in achieving the desired security outcomes for the business that employs them. If they are not trusted, employees will work around the controls that they implement, with resultant impacts upon the security of that business. Therefore, trust appears to be a crucial component of the CISO's relationship with their organisation. However,

[14] Cf. the reference that one participant made to their company being "the soft underbelly" for its customers that distributed food, as presented in Chapter 4.

[15] Such risks have been highlighted by other researchers, e.g. [160] as well as in media reports, e.g. [485].

there is an aspect of distrust suggested with regard to the 'othering' that many CISOs felt within their organisations, particularly those that felt that they were seen as auditors or similar. This included being "treated like a body that needs to be negotiated with"(CISO2) and being viewed as "of a different tribe" (CISO15).

By identifying recreancy, an organisation can assign blame. The role of the CISO in this process further indicates the moral associations of cyber security that were discussed in Chapter 4. Further, those who are recreant can be assigned an identity as wrong-doers, which enables the use, or justification, of intrusive controls, as described by Bogain [145], and even dehumanisation, as described by Joffe [447]. In order to both identify and prevent recreant behaviour in relation to cyber-security risk, the organisations in the present study implemented and operated various forms of control aimed at regulating behaviour, including mandatory training, checklists and regular attestation from certain staff with regard to policy compliance. As described in some of the annual reports, organisations sought to change employee 'mindsets' in order to achieve the desired corporate culture in relation to risk management. Deviation from the latter could result in punishment.

The trust dynamic between CISO and organisation is likely to be multifactorial, with trust seemingly needing to be negotiated, and renegotiated, with multiple stakeholders. This further contributes to their conflicted identity, as explored in the previous chapter. The CISO's role in defining and implementing controls in response to risks faced by their employer may generate fractures in trust with their stakeholders within that organisation. Therefore, in helping a business to build trust with its stakeholders, by implementing controls, the CISO may unwittingly undermine the level of trust placed in them by their fellow employees.

In the following section, I discuss the use of controls in risk management more broadly.

5.4 Management of risk through control

Risk management was commonly described in the annual reports as not just cultural but as pivotal to the running of the business. In some cases, part of being 'well run',[16] included planning for future negative events. Risk management was articulated by the vast majority of these businesses in their reports as both formalised and governed, and the activity of risk management was positioned by some organisations as an activity that was essential to their continued viability, as well as being a factor in the success of that business, with risk itself being 'intrinsic' to business. Risk management was

[16] Which links to the 'doing the right thing' construct discussed in Chapter 4.

also, for the majority of them, an obligation. However, there was again a perceived spectrum of importance implied in relation to risk management, which was associated with the industry that the business operated in, according to CISO11, who stated that their business "probably don't focus in on enterprise risk management as much as, say, a global bank".

In order to manage the multiplicity of risks that these organisations faced, they implemented different controls, beyond those relating to cyber security as described in Chapter 4. This included references in the annual reports to the penalising of staff in relation to risk management, including, in a number of cases, penalties relating to failures in managing cyber-security risk. These penalties were financial, with employee and senior leader remuneration being linked directly to both cyber security and broader risk management failings. This included the provision for 'clawback' of previously paid sums.

In the remainder of this section, I bring the literature relating to the use of controls in risk management into conversation with the data in order to achieve a deeper understanding of how these organisations responded to cyber-security risk and the implications of such responses. This focuses on three specific risk-related controls that were identified from the analysis of the data, namely education, measurement and governance.

5.4.1 Education and *Nichtwissen*

Cyber-security education was discussed in the previous chapter, particularly in the context of morality, and it will be discussed again in the following chapter, in the context of punishment, power and control at a state level. It is also relevant to discuss here, from the perspective of education being a means to reduce uncertainty [128, 414]. For the businesses in the present study, the predominant philosophy regarding cyber-security education was one of addressing perceived gaps in knowledge, in explaining what was required of staff and the reasons why they were being asked to do, or not do, certain things. Although, in many cases, CISOs utilised emotionally engaging messages and attempted to connect their education to the lives of employees outside of their work environments, this was still approached from the perspective of resolving deficiencies in knowledge. In some cases, those staff were even seen as imbecilic, for example, the reference one CEO made to "the idiocy of a single individual" (CEO1), which builds on a normative conception of employees as being inherently risky in relation to cyber security [66, 602]. A gap-filling approach was also followed by CISOs when describing how they educated their board members, as exemplified by CISO6's comment that "[the board] don't know enough".

As introduced in Chapter 2, Beck considers such an approach to be ineffective, even facile [123]. He argues that "[risk] nowadays often cannot be overcome by more knowledge but is instead a result of more knowledge" [123, p. 5]. He suggests that current modernity involves "living . . . with the simultaneity of threats and non-knowing . . . [which] cannot be overcome by more and better knowledge . . . it is the *product* of more and better science" [123, p. 115] (italics in original). Beck further distinguishes between "provisional non-knowing, unacknowledged non-knowing, wilful ignorance and . . . conscious and unconscious inability-to-know" and describes how "*Nichtwissen*", in these different forms, "permeates and transforms human conditions of life and suffering, expert and control systems, the notions of sovereignty and state authority, of law and human dignity" [123, p. 115] (italics in original). This reference to *Nichtwissen* as something that "permeates . . . expert and control systems" [123, p. 115], as well as Beck's suggestion that "experts" are as subject to *Nichtwissen* as lay persons, provides an argument that undermines Giddens' "trust in expert systems" [359, p. 83] as a mechanism to deal with uncertainty, and hence risk. As established in Chapter 4, cyber security for the organisations in this study appeared to result in *Nichtwissen*. Both the (perceived) existence of cyber-security threats and the prevalence of non-knowing were clear in the analysis of the data, with risk arising from the knowledge that such threats existed, were unknown (or at least unacknowledged), and, further, were to a certain extent unknowable, due to their arcane nature. Efforts to increase knowledge within those organisations may only have increased the level of *Nichtwissen*, which, by definition, is "ineradicable" [123, p. 115].

Nichtwissen prompts efforts of calamity avoidance [123], and, as with the examples of terrorism Beck describes, cyber-security threat is nebulous, and avoidance of risks associated with these threats "must rely on more or less fictive suppositions" [123, p. 119], as discussed in the previous chapter. Therefore, a CISO's purpose may be seen as providing an organisation with the capability to avoid cyber-security calamities, prompted by its 'cyber-*Nichtwissen*', and yet contributes to that same state of non-knowing by providing "more knowledge" [123, p. 5], especially through education. Avoidance of calamity is dependent on potentially "dubious hypotheses or mere suspicions" [123, p. 119], provided by both the CISO and the wider cyber-security industry.[17] I summarise this process from an organisation's perspective below in Figure 5.2.

[17] Cyber-security practices aimed at avoiding cyber-security threats may themselves result in the creation of novel, and larger, threats [123, p. 119], such as antivirus software that introduces new vectors of attack [791].

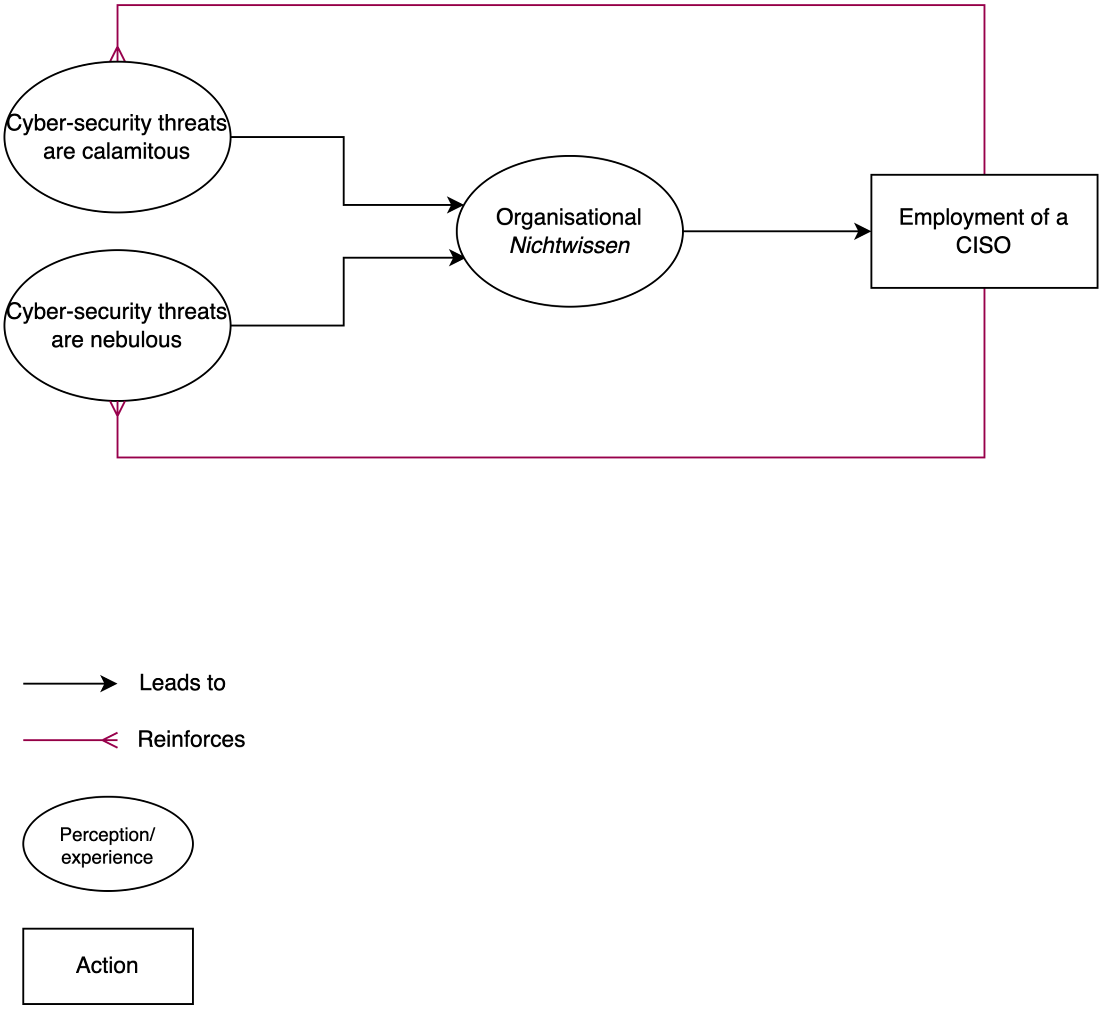

Cyber-security threats are calamitous
Cyber-security threats are nebulous
Organisational *Nichtwissen*
Employment of a CISO
Leads to
Reinforces
Perception/ experience
Action

Figure 5.2: The cycle of non-knowing with regard to cyber security in an organisation, based on this analysis.

This diagram summarises what I propose to be a vicious circle regarding organisational cyber-*Nichtwissen*. Perceiving, or experiencing, cyber-security threats as disastrous and opaque results in this sense of non-knowing for the organisation. In response, a CISO is employed, who further contributes to that sense of cyber-security threats being disastrous and opaque, which perpetuates their employment.[18]

The role of the CISO in calamity avoidance contributes to the sense of cyber security being "somebody else's problem" [67, p. 25], as discussed in Chapter 2, with cyber-

[18] However, not all avoidance of calamity regarding cyber security was prompted by the CISO. As discussed in the previous section, part of the sense of risk associated with it was due to perceived obligations.

Nichtwissen resulting in both a disconnection from cyber-security risk, as discussed in Chapter 4 and the employment of a CISO to deal with any calamities arising from that risk and to meet a perceived obligation regarding the management of that risk. As Beck describes, "authorities must continually reaffirm and re-establish their control over uncontrollable risks" [123, p. 117], with the (continued) employment of a CISO being a mechanism to "reaffirm" that control and further suggesting a semiotic purpose to the CISO role as described in Chapter 4.

5.4.2 Measurement

The annual reports included various references to measurements that related to risk management, both qualitative and quantitative. In relation to cyber-security risk specifically, some organisations suggested that they were concerned primarily with cyber-security risks that were 'significant', but neither the criteria for reaching that threshold nor the process followed in determining whether it had been reached were described.[19] However, in some cases, the number of 'significant' cyber-security risks that had materialised was the sole cyber-security measurement referred to in the annual reports. All organisations mentioned the existence of cyber-security risk and, to a greater or lesser extent, how the organisation mitigated that risk. Descriptions of the manifestation of such risks included impacts on reputation, the achievement of the organisation's strategy and its long-term growth potential. However, predominantly, impacts were articulated in terms of financial measures, such as revenue and profit, with a normative bias towards such measurements being clear and a number of reports indicating the primacy afforded to such criteria.

There were limited references to specific measures in the data, such as the total number of breaches and the existence of scorecards, which appeared to be a demand that CISOs were responding to rather than something they were driving. The annual report data indicated a stronger desire for quantification of risk however, with references to metrics associated with risk being common, both in relation to cyber security and to other risks. Only two annual reports referred to a qualitative element within cyber-security risk measurements.

CISO participants indicated that there was a drive for a statistical measure with regard to cyber security, which appeared to originate from their leaders. CFO1 indicated this desire when they stated that

> "ultimately . . . [we've] got to get to a position where there is that sort of

[19] This sense of 'significance' further suggests a conception of cyber security as a continuum, necessitating interpretation, as discussed above and in the previous chapter.

> a dashboard … what's your management information … from a security perspective, they should have formed various KPIs [Key Performance Indicators] … that's probably where we need to get to".

Similar sentiments were expressed by CFO2 and CEO1, who already received KPI reports relating to cyber security. NED1 also described a need to know "what is the level of that [cyber-security] risk?" but suggested a tolerance for a less quantitative measure, asking whether that risk was "red, yellow [or] green". However, an inability to deliver this frustrated some of the CISOs' stakeholders, who did not appreciate that "there isn't a clear answer" (CISO13). One CISO stated that the audit committee for their organisation would ask "if it's not red [the relative colour-coded importance of the cyber-security risk], why am I here?" (CISO11), suggesting that, in reality, a red-yellow-green measure was being treated as binary, i.e., either red or not-red. This was also indicated by CISO12's description of only being present at a board meeting "if it's something going wrong" and CEO1's expectation of being "told quickly … if something serious happened [in relation to cyber security]" but otherwise not having much visibility of cyber-security risk. Such statements indicate an implied quantitative measure in relation to this risk, that of 'good state' versus 'bad state'.

The desire for risks to be expressed in purely economic terms that was observed both in interview data[20] and in the annual reports[21] suggests that the "positivistic posture" [287, p. 272] of economics influences business to such an extent that, as well as economics itself ignoring social factors [287], there is a side effect of other processes within businesses being seen in a similar way. This normative conditioning [769] may lead to cyber security being seen through a purely economic, i.e., positivistic lens, with the result that its social aspects are deprioritised or ignored.[22] Cyber-security practices are then seen solely as a 'cost/benefit analysis', with the benefit being a quantifiable avoidance of risk. This influence of economics on business may be a cultural feature that is specific to the markets and geographies that these companies operated within, however, as described by O'Malley [584], this primacy also enables aspects of control, and maintenance of power structures, both those related to expert systems and, potentially, wider hegemonies.[23]

[20] For example, the need to "find a common language for talking to the board about security" (CISO8), which was financial in nature, and CISO14's description of "try[ing] to articulate … what the consequence [of cyber-security risk] would be in financial terms … and how much it might cost to mitigate that risk".

[21] The annual reports described impacts on revenue and profit associated with the manifestation of cyber-security risk, as well as less explicit economic impacts such as to long-term growth potential and reputation, and the loss of commercial opportunities.

[22] The expression of cyber-security risks in financial terms can also be observed in certain academic sources, e.g. [77, 202], and in general media discourse, e.g. [767].

[23] As I discuss in more detail in Chapter 6.

It was notable, however, that many CISOs indicated a resistance to the quantification of cyber-security risk, and were clear about the subjectivity of assessing such risks, particularly demonstrated by the 'art not science' construct that was expressed. As discussed in Chapter 4, such objections could be related to a desire to reinforce an irreplaceable interpretive expertise. This does not align fully with O'Malley's point about the positivist aspects of security, however, it does still support his idea that "experts define the problem in such ways that only their expertise can resolve the issue" [584]. Viewing cyber-security risk (and other risk) from the perspective of what Mythen describes as the "natural objectivist model", where risk is "an objective and calculable entity" which "does not entertain either the social production, or the cultural cognition of risk" [563, p. 97], results in primacy being given to attempts to measure and objectively assess risk over cultural and social aspects. If organisations expect their CISOs to objectively assess cyber-security risk, or to provide the necessary resources and knowledge to employees to allow them to do so, then, as well as not achieving an effective outcome, in the sense of fully understanding the risk and what is required to manage it, they may demotivate and alienate those individuals. This may be a source of the disconnect expressed by many of the CISO participants, as discussed in Chapter 4.

The awareness of leaders with regard to cyber security, both in terms of threats and current 'health' of the organisation, appeared to be key components of the governance practices described by the organisations in this study.

5.4.3 Governance

Many of the annual reports made reference to the governance of cyber security which included both governance of the cyber-security function and programme, and of cyber-security responsibilities that fell to others within the organisation. This was achieved via committee review, internal and external auditing and other, more vague, methods of 'assurance'. Some of the reports described regular board-level reviews of cyber-security programmes and risk reduction activities, including the provision of updates from the CISO. The CISOs utilised governance forums in order to 'stage' risk to their leaders, that is, "[making the] future catastrophe become present – often with the goal of averting it by influencing present decisions" [123, p. 10]. CISOs provided visibility of cyber-security threats and an assessment of the exposure that the organisation had in relation to them. Through this process, the organisation achieved a feeling of control over those risks; as they were being identified and assessed by an expert, then there was less need to be concerned. The perceived effectiveness of that expert was a crucial factor in the level of comfort that the organisation felt, with governance processes being key to determining that sense of confidence in the CISO. This again indicates the judgemental aspect of governance, with decisions being made not just on whether the organisation was 'doing enough' with regard to cyber security, but also as to whether the person charged with managing cyber-security risk was effective, or indeed, even the right person. Governance, therefore, played a role in the perceived precarity of the CISO's job.

The concept of governance by consent[24] was indicated by some of the CISOs in this study, who alluded to the need for those being governed in relation to cyber security to accept that fact. Johnston and Shearing argue that "the desire to promote local capacity and knowledge ... [is a] basis for effective governance" [450, p. 73], with "problem-solving governance ... [entailing] the application of any means that will promote safe and secure places in which people live and work" [450, p. 71]. The CISOs in this study certainly played an educative role, and their stakeholders expected them to "promote [a] safe and secure place ... [to] work" [450, p. 71]. In addition, security governance is motivated by the need to be ready for a future, damaging event [450] and aligns with views of risk as future-oriented. Therefore, as well as being soothsayers, CISOs were also agents of governance.

Jiraporn et al. found that "firms with more effective governance exhibit a substantially lower degree of risk-taking", with their focus being on financial risk [446, p. 111]. Extending this finding to cyber security, more effective cyber-security governance may, therefore, be expected to result in more risk-averse behaviour from an organisation. However, an associated outcome may be the loss of opportunity and reward. This was suggested by the concern that many CISOs in this study had of being seen as blockers, inhibiting organisational innovation, and also lends weight to the impression that many CISOs had that they "[could] never win" (CISO13). As agents of governance they were expected to reduce the organisation's risk but in so doing, they could limit the organisation's potential for reward. This also suggests that these organisations had an overly simplistic conception of risk versus reward that is based on a no-loss hypothesis, as discussed in Chapter 2.

A sense of CISOs walking a tightrope was clear, with the language of 'balance' again being common. For example, CISO14 described how they "try to articulate that [threat] in a balanced risk-based way" and CISO9 expressed a need for "making sure that security is applied and usable". Bowman points out that those who take risks on behalf of the companies they work for may not themselves suffer the consequences of those decisions going awry, particularly if they were confident of finding another job [159]. Chari et al. build on Bowman's work to suggest that "career concerns" [208,

[24] Which is another Hobbesian notion explored in Chapter 6.

p. 369] are a factor in both risk-taking and risk-avoidant behaviour, with “strong governance” being required which “motivates managers and aligns their interests with shareholders” [208, p. 362]. I suggest there is a particular paradox with regard to CISOs, in that the decisions they take may reduce risk for their organisations, but by potentially limiting (perceived) opportunities, they may put themselves at risk of stakeholder dissatisfaction that could impact their career security.[25] Equally, however, if they take (or fail to take) a decision that is not successful in reducing cyber-security risk then they can be scapegoated in the event that such risks manifest and impact upon the organisation. A further complexity is seen in that the job market for CISO roles may feature what Bowman describes as “attractive ‘labor mobility’ ” [159, p. 41]; while at risk of job losses, CISOs may not find it difficult to find another employer. Shareholder interests are themselves paradoxical, in that there is an expectation of an organisation taking the appropriate actions to manage risk and yet also the expectation that the organisation maximises returns. With the perceived incomprehensibility of cyber security, as opposed to, for example, financial risk, it may be difficult for shareholder interests to be clearly understood with regard to cyber-security risk and, therefore, appropriately aligned. These factors contribute to the sense of the CISO role being conflicted. CISOs are expected to act as agents of governance and yet are at risk of being punished for performing that role.[26]

Cyber security also played a role for these businesses in broader organisational governance, such as the application of discipline. Governance is strongly associated with discipline and control, in particular with boards of directors “monitoring and controlling top management” [149, p. 3]; indeed, this may be the primary task of the board [322]. Boards are considered to be a crucial method of internal governance for listed companies [322] and, as a form of governance, “constrain managers from pursuing risks that erode shareholder returns” [208].

Board-level governance

For most of these organisations, the board acted as a guardian against risk. It determined the effectiveness of controls and other mitigating actions taken, as well as the acceptability of any residual risk. It set boundaries for the organisation and made judgements that ensured the ongoing success, and continued viability, of those businesses. The board’s role in providing this risk governance was articulated as an obligation in the majority of annual reports. However, there was a suggestion that the manner in

[25] Such dissatisfaction may itself be motivated by those stakeholders being concerned about their own job security, if a CISO’s decision is impacting on their ability to take a risk that they see as career enhancing.

[26] Further paradoxical aspects of the CISO role are discussed in Section 5.5.

which this governance was performed was reasonably subtle. NED1 stated that "board members don't really *do* anything but they advise, ask questions, insist" (emphasis captured in original transcript). CISO11 alluded to this when describing how "boards are great but . . . all they're going to do is go 'oh okay, what are you doing about it [i.e., a cyber-security risk]?' ". A similar limitation was suggested by CISO13 who described how "all [the audit committee chairman] can do is really raise concerns and issues and make sure they're being followed through . . . but that's kind of the limit". This is contrary to NED1's description of boards having the power to "hire [and] fire people" and more delicately, CEO1 expressed that "the point of the non-executive director is very often the raised eyebrow". This suggests that although the role of the board in risk governance may be ostensibly formal, in practice it may be more understated than it appears.

As discussed in Chapter 2, previous research has established that there are temporal differences in corporate governance needs over an organisation's life cycle [149, 328, 515, 582]. While the present study has not attempted to measure organisational life stage, all of the businesses investigated can be argued as being relatively mature, at least from the perspective of having a multi-year tenure on the stock exchanges that they were listed on. Bonn and Pettigrew argue that a mature company will engage in "regular dialogue with stakeholders [to signal] . . . that the board is effective and vigilant" [149]. Such signalling is performed, in part, by the annual report, which "tells a story" [170, p. 198], and, certainly in this study, the stories told were ones of board-level vigilance, including with regard to cyber security. Mythen invokes Beck's concept of "organised irresponsibility" [123, p. 27][27] to highlight how "institutions have directed public attention towards image management and away from the details of preventative measures" [563]. Relaying the existence of a CISO in a public document such as an annual report may be as much about the former as the latter. Legal scholars Lawrence Trautman and Peter Ormerod describe how company directors have a "duty of care" with regard to cyber security [740, p. 1234], something that was alluded to by some of the non-CISO participants in this study. As well as being a motivator for semiotics regarding the fulfilment of this "duty of care", the lens of recreancy [340], as discussed above, is relevant. Part of the board's duty is in ensuring that the organisation is not recreant with regard to its own obligations regarding cyber security, which underpins the role of the board as a mechanism of control.

Davies and Zhivitskaya highlight the importance of boards in ensuring an organisation operates "within its risk appetite" [271, p. 36]. This construct suggests a 'banding' to risk, a continuum, that has boundaries within which the organisation is

[27] The normalisation of risky activities within an institution.

permitted to operate. This is similar to the way in which cyber security was positioned by participants more broadly,[28] suggesting perhaps a normative conception that risk is a spectrum, and that there is a sense of sanctioning actions relating to risk. These concepts also suggest that risk requires oversight, that decisions relating to risk require more than one party to review and validate those decisions.[29] This oversight was performed at multiple levels within these organisations, and a stratification associated with this was commonly codified, both in the interview and the annual report data, using the term 'three lines of defence'.

Three lines of defence. As introduced in Chapter 2, the 'three lines of defence' model appears to be pervasive in risk management. A number of participants, both CISOs and non-CISOs, made reference to this model when discussing cyber security, which was not limited to specific industries, although industry sector was identified by some as a factor in the level of awareness of the model. For example, CISO11 described how "in my background, I'm used to the three lines of defence model. That isn't something that is burned into the operating culture of of the industry that I work in". However, in the majority of annual reports, reference was made to the company operating a 'three lines of defence model' of risk management.

Zhivitskaya's findings suggested a rejection by the first line of the responsibilities assigned to them [796]. Such phenomena may be foundational in complacent behaviours and attitudes of employees with regard to risk, perceiving it as something that other teams are responsible for managing, and resulting in recreant behaviour. User complacency and apathy with regard to technology have been themes explored by a number of researchers, e.g. [493, 710, 711, 733], with some specifically identifying that employees believe that someone else is responsible for cyber security [79, 455]. This sense of cyber security being somebody else's problem may be countered by clearer explanation of the three lines of defence model. Equally, however, it may be exacerbated by it, as those in the first line gain a false sense of security from the existence of two additional lines of defence. There is also an implicit sense of culpability associated with the model, in that it suggests that the first line may be ineffective in managing or containing risk and, therefore, additional oversight is required.

The normative aspect of this model may be indexed by CISOs as a means to justify the existence of their role, and associated function. CISO10 summed up their role in that model as "[being] accountable for raising the profile of a risk existing, I'm not

[28] E.g., the "subtlety between 'do you want good practice or best practice' " (CISO7), the difference between "gold-plat[ing] dots [and] short-chang[ing]" (CFO2).

[29] This also suggests a moral aspect to risk management, in the sense of providing a mechanism to overrule self interest, building on Baier's definition of morality [104] as discussed in Chapter 4.

accountable for fixing it, that's a business decision based on corporate business risk appetite" and, similarly, CISO5 described their role as "providing assurance back to the business that we're doing what is required of us". However, it wasn't entirely clear for some CISOs which role they fulfilled, with CISO15 describing "having to position myself as the sort of one-and-a-half line of defence" and CISO13 referred to the line between the second and third lines of defence as being "a little bit blurred" in their organisation.

Whether the three lines of defence model provides any clarity for their stakeholders on what the purpose of a CISO is was not clear from this study. However, it does indicate benefits accruing to the CISO of the normative aspect of the model, which helps to justify their continued existence, as does the need for a continual check and balance due to the potential for control weaknesses elsewhere in the organisation. Building on the concept of instrumental versus intrinsic value discussed in Chapter 4, the three lines of defence model suggests an instrumental value to the CISO role, of being necessary as a response to weaknesses existing in the business. This distinction between instrumental and intrinsic value provides a useful analytic lens with which to view risk management in business, as I now explore.

5.5 Value and paradoxes in cyber-security risk management

It was notable that in the annual reports analysed for this study, references to risk management, including cyber-security risk management, were more prominent in the sections focused on governance than they were in those focused on strategy. Both interview and annual report data also indicated that cyber security was an obligation for these businesses, in many cases, due to regulatory or customer demand. This included the references that CEO1 made to the UK government "insisting [upon]" certain cyber-security standards and CISO4's description of being "under a [regulatory] regime", against which some CISOs felt they needed to have "a defendable position" (CISO15). Heath et al. refer to a trend that is "shifting more of the primary responsibilities for protection of human rights onto corporations" [399, p. 441] and, in relation to cyber security,[30] the UK government's perspective on the obligations of businesses in this domain is clear [747].[31]

The expression of risks in economic terms, as discussed in Section 5.4.2, indicates

[30] Which was positioned as an element of human rights and social obligation in a limited number of cases in the data.

[31] This may represent a "responsibilization" [494, p. 320], which has moral associations [494], providing a further link to the moral aspects of cyber security that were discussed in Chapter 4.

an instrumental value being placed on risk management, with quantification of risk itself indicating an instrumental logic [575]. It is not unreasonable for an organisation to view cyber-security risk management as being of instrumental value, in helping it to protect its reputation and meet externally driven obligations. Further, a premise founded on instrumental value does not necessarily undermine any moral aspects [454] and intrinsic value may be, at least fractionally, contingent on instrumental value [456]. However, if the person charged with overseeing cyber security sees their role as being intrinsically valuable, particularly if that view of intrinsic value is based on a (possibly mistaken [454]) moral basis, as discussed in Chapter 4, then a conflict between that individual and the organisation may occur. The CISO would then perceive a misalignment between their moral identity and that of the organisation, perhaps feeling like the organisation is paying lip service to cyber security for the purpose of a positive public image. This was indicated by the comment made by CISO13 in relation to cyber security being "something that they [the board] have to be concerned about and that they have to show that they're concerned about" and CISO15's description of cyber-security requirements being met "because you had to, not because you wanted to". While the CISOs did not explicitly suggest that their organisations were paying lip service to cyber security, there was clearly a conflicting sense of 'have to' versus 'ought to', which contributed to the detachment and anxiety they experienced, as described in Chapter 4, and summed up by CISO14's description of finding it "a really, really hard slog to get ... stakeholders to just engage with security and understand the value".

As suggested in Section 5.4.3, CISOs occupy somewhat of a paradoxical role, in that they are responsible for determining how an organisation can limit its exposure to cyber-security risks but in so doing, they may impair the organisation's success, by being "the people who put the no into innovation" (CISO7). However, a failure to limit such exposure would result in being "the guy [that gets fired]" (CISO12). Similarly, as described in Section 5.4.1, the provision of cyber-security education by a CISO may paradoxically result in non-knowing. In the following section, I describe further paradoxes arising from the analysis of the data.

5.5.1 Further paradoxes in cyber-security risk management

The expectations on the CISO to not just transform uncertainty into risk but to ensure that that risk is effectively managed[32] can result in a paradox of limiting an organisation's capacity to innovate while simultaneously enabling that business to succeed, by ensuring its continued viability. Although being "the ministry of no" (CISO8)

[32] To ensure the "protect[ion] ... [of] company assets ... crown jewels" (CFO2).

may impact on how they are perceived, the CISO performs a valuable[33] role for an organisation in ensuring that it is protected from existential threat. However, to a certain extent, they may also be holding it back from further growth, if indeed they are "slow[ing] things down" (CISO5). They are at once limiting factor and viability enabler, hindrance and facilitator. However, it is possible that, rather than this being a paradox, it is instead a question of balance. Returning to the notion of cyber security as a continuum, the role of the CISO is to enable an organisation to grow in a manner that is congruent with its "risk thermostat" [68, p. 15], and to act as "those good six piston calliper brakes" (CISO12).[34]

As discussed in Chapter 2, one component of the risk thermostat is "perceived danger" [68, p. 15]. The use of fear appeals by the CISOs in this study may result in their organisations placing an instrumental value on anything that helps them deal with the emotional uncertainty arising from the fearful nature of a threat, as identified by criminologist Martin Nøkleberg in his study of everyday security relating to transport [575], with associated consequences on how people experience security. The use of fear in cyber-security messaging and education may, therefore, serve to engender a response based on instrumental logic and thus prevent, or at least undermine, the perception of cyber security as having intrinsic value. In this regard, CISOs who deliberately utilise fear in their educative approach may, at least partially, be architects of their own discontent. Further, while on one hand fear appeals may motivate greater attention being paid to cyber-security risks, on the other they may result in poor decision making regarding them, and/or result in their audience disengaging from the subject.

Related to this, indications of employees failing to take certain actions in relation to cyber-security risks were mentioned by both CISOs and non-CISOs. For example, CISO3 referred to attempts to circumvent cyber-security controls, CISO1 was concerned about there being "cowboys out there [in the organisation] and that's where you get the risk", and CFO2 highlighted the possibility of "poor behaviour" in relation to cyber-security risk management. Employee behaviour was, for CEO1, "the one [factor] that normally lets you down", possibly due to "the idiocy of a single individual". CISO1 similarly described "users . . . [as] the biggest security risk", although they were in a minority of CISOs who referred to users in this way. These phenomena may motivate an organisation to employ, or maintain the employment of, a CISO, in order both to manage such risks in the absence of others within the business taking responsibility for them and to educate employees in how to deal with cyber-security risks and their feelings regarding them, which include being fearful of them. Somewhat paradoxically,

[33] Instrumentally valuable.

[34] Invoking the cliché of brakes, especially good brakes, enabling faster progress.

those CISOs may also manipulate or engender those feelings in order to encourage employee actions that reduce cyber-security risk. For example, using "virtual reality war games [where] you watch them shit themselves over the next half an hour" (CISO11), or providing information that "freaks them out" (CISO11).

Extending Ewald and Beck [123], the purpose of a CISO may be to act as a 'professional pessimist', to "imagine the worst possible" [321, p. 286] situation regarding risks relating to cyber security and, therefore, to prepare appropriate responses. However, this is also in the CISO's interests, as discussed in Chapter 4, and, as will be explored in Chapter 6, also supports existing structures of power. However, there were suggestions of "cyber fatigue" [260, p. 14] from some senior leaders in this study, such as the CEO who expressed a desire to avoid any sense of 'crying wolf' with regard to cyber threats.[35] Again, there is potential conflict here, in the sense that, according to Ewald and Beck, an organisation needs to consider catastrophic circumstances with regard to cyber security in order to fully understand its risk. If, however, the leaders of that organisation are fatigued by hearing about such scenarios, or consider them to be fanciful,[36] then not only will the risk not be thoroughly appreciated, and possibly disregarded, the person charged with relaying those messages is likely to experience both frustration and disengagement, as observed in this study. This indicates a further paradox with regard to the management of cyber-security risk in commercial businesses.

The implications of these paradoxes

As described in Section 5.4, businesses seek objective measurement of cyber-security risk, driven by a positivistic philosophy that permeates modern corporate culture. This leads to a disregarding, or at least a deprioritisation, of the social and emotional factors that constitute that risk, which may result in an increased likelihood of such risks occurring. Cyber-security risks are fearful and engender emotional responses that can include engulfment. Organisations employ CISOs in response to these feelings, however, those CISOs may further provoke emotional responses in a deliberate attempt to better express, and respond to, cyber-security risk.[37] According to Beck, in order for the organisation to fully understand the cyber-security risks it faces, it needs to consider a multiplicity of calamitous and fearful scenarios and yet may easily grow tired of hearing about such scenarios and reject what it considers to be scaremongering. Ironically, this rejection may lead to the CISO becoming disconnected from the organisation and, as a result of being devalued, either voluntarily or involuntarily leaving

[35] The need to "avoid ... shroud-waving ... because people then don't take it seriously" (CEO1).

[36] And possibly self-serving.

[37] Although this may be in vain, due to the difficulty in visualising such risks, as discussed in Chapter 2.

that business, resulting in the organisation being less able to manage its cyber-security risk. The cycle then begins again. However, in a further paradox, contributing to the uncertainty experienced with regard to cyber security may, in fact, support the CISO's continued employment, due to that uncertainty being unresolved. Therefore, CISOs as managers of cyber-security risk may generate either, or both, fear and indifference, which contributes to the sense of conflicted identity explored in the previous chapter.

5.6 Summary

In Chapter 4, I explored my findings through a lens of identity and ontological security. In this chapter, I applied a lens of risk. These concepts are linked by a thread of uncertainty. This study has shown that cyber-security threats generate uncertainty for businesses, which leads them to take actions in an attempt to reduce it. This uncertainty relates to fearful future events that could impact upon the continued viability of a business. In relation to cyber security, that uncertainty is seen to be growing.

Businesses see the management of cyber-security risk as a duty, an obligation, and cascade aspects of this duty throughout their organisations. This requires the CISO to identify and respond to recreant behaviour, resulting in them being an agent of governance. Cyber security represents a manufactured risk, not in the sense of being fabricated (although there is a risk that its uncertain nature and spatial and temporal fluidity facilitate fabrication), but in the sense of cyber-security incidents being an inevitable consequence of technological progress. As such risks are unavoidable, in a society that is obsessed by risk,[38] and driven by masculine logic,[39] there is a need for those risks to be controlled, measured, and overseen. Therefore, the CISO also represents a manifestation of this need for control within a business, and at least part of their purpose appears to be both to control cyber-security risks and to signify that those risks are being controlled. Due to the primacy afforded to supposedly objective measurements of cyber-security risk, important social and emotional risk factors may be neglected, with consequential increase in risk.

The present study shows that one approach commonly followed by organisations in preventing recreancy with regard to cyber security is to educate its employees, providing them with additional knowledge that would help them to understand and avoid cyber-security risks. However, this gap-filling approach may be ineffective and even counter-productive, with education regarding cyber-security risk simply resulting in greater non-knowing, and more uncertainty. Organisations may unwittingly engender

[38] Following Beck.

[39] Following Walklate, as discussed in Chapter 2.

this cyber-*Nichtwissen*, resulting in greater disconnection from those risks. This is one of a number of paradoxes with regard to cyber-security practice and the role of the CISO, with these contributing to the opacity of their purpose and potentially undermining their effectiveness. This includes the role they play in potentially limiting an organisation's growth while at the same time enabling them to survive. Consideration of, and reflection on, these paradoxical elements by both CISOs and their employers will be of value to all parties and enable a greater understanding of the role that CISOs fulfil, as I reflect on in more detail in Chapter 7.

Chapter 6

Cyber security and the Leviathan

This is the final findings chapter. This chapter employs Thomas Hobbes' Leviathan as an analytical lens.

6.1 Introduction

The chapter is structured into four main sections. I offer a brief introduction to Hobbes' work in Section 6.2 that provides a basic conceptual grounding to build on that provided in Chapter 2. I then explore his concept of the state of nature in Section 6.3. Next, I discuss a key aspect of Hobbes' social contract in Section 6.4 before expanding the application of Hobbes to cyber security at a state level in Section 6.5. Finally, I summarise my contributions in Section 6.6. As with the two preceding chapters, quotations from participants[1] and paraphrases from annual reports[2] are included where relevant to exemplify or support a theme or interpretation from the analysis. Where appropriate, I present key additional literature, to build on that introduced in Chapter 2, that supports the concepts discussed and the interpretations I make, bringing this into conversation with the findings.

6.1.1 Why Hobbes?

In this final discussion chapter, I apply a lens based on the work of political philosopher Thomas Hobbes to the findings from this research. Hobbes' *Leviathan*, in particular, has had a significant influence on Western political philosophy [94, 716] and it is primarily through this text that I develop my analysis. There are many theorists from the domains of political philosophy and IR whose work could have been applied as lenses

[1] Indicated by double quotation marks.

[2] Indicated by single quotation marks.

through which to interpret the data from this study.[3] Hobbes was employed due to multiple, and repeated, resonances within the data to his work. These were identified during the analysis and included themes of discipline, education and punishment, protection in exchange for obedience, permanent emergency, and state power. While Hobbes is not the only theorist of note to have discussed these themes, the resonances with his work arose through the process of inductive analysis, leading me to engage further with the literature, both that of Hobbes and prior research that has invoked his writings. This process of reflexive analysis, of bringing my data into conversation with these perspectives, led to valuable insights relating to cyber-security practice and the role of the CISO. For example, it motivated reflexive consideration of the political factors, both explicit and implicit, that affect the CISO's practice, as well as providing greater contextualisation of the wider society in which businesses, and CISOs, operate. Hence, this chapter focuses on the results of that analysis.

Some of the themes explored in this chapter overlap with those discussed in the previous two chapters. However, the application of Hobbes' work has allowed different analytical insights to be gleaned, adding nuance and greater depth to those discussions, by contextualising the CISO's practice in broader society. This analysis has enabled the same themes and data to be considered from a different perspective, and, in so doing, has resulted in the development of novel positions on the purpose of the CISO. In particular, there has been a consideration of different parties influencing, or being interested in, that purpose. Without the application of Hobbes as an analytic lens, such a consideration would not have occurred.

I am not the first to look at modern businesses through a Hobbesian lens, e.g. [205, 217] and others have invoked Hobbes in reference to cyber security, e.g. [429, 460, 716]. However, to my knowledge, this work is the first to apply a business-as-Leviathan lens to concepts of cyber security in business and how these relate to the wider state Leviathan.

In Figure 6.1, I highlight the relevant themes from the meta-analysis mentioned in Chapter 3 that are predominantly covered in this chapter. This diagram is intended to provide context and aid navigation through the thesis.

[3] And indeed, this is a suggestion for future research that is highlighted in Chapter 7.

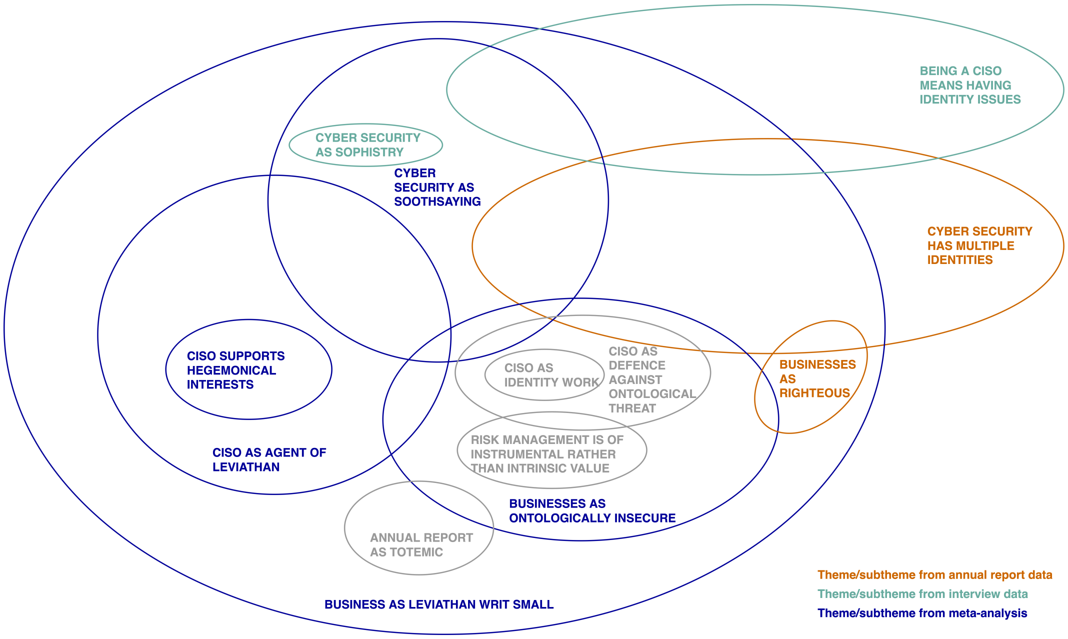

BEING A CISO MEANS HAVING IDENTITY ISSUES
CYBER SECURITY AS SOPHISTRY
CYBER SECURITY AS SOOTHSAYING
CYBER SECURITY HAS MULTIPLE IDENTITIES
CISO SUPPORTS HEGEMONICAL INTERESTS
CISO AS IDENTITY WORK
CISO AS DEFENCE AGAINST ONTOLOGICAL THREAT
BUSINESSES AS RIGHTEOUS
RISK MANAGEMENT IS OF INSTRUMENTAL RATHER THAN INTRINSIC VALUE
CISO AS AGENT OF LEVIATHAN
BUSINESSES AS ONTOLOGICALLY INSECURE
ANNUAL REPORT AS TOTEMIC
BUSINESS AS LEVIATHAN WRIT SMALL
Theme/subtheme from annual report data
Theme/subtheme from interview data
Theme/subtheme from meta-analysis

Figure 6.1: Meta-analytic themes covered in this chapter. Themes not covered in detail are greyed out.

This diagram demonstrates the multiplicity of themes related to Hobbesian concepts that were present in the data, and which were developed from numerous categories and codes. The identification of these themes inspired the use of Hobbes, particularly *Leviathan*, as an analytical lens and map onto the sections in this chapter as shown in Table 6.1. This motivated an in-depth exploration of Hobbes and associated literature, which resulted in the subsequent development of broader themes relating to Hobbes during the meta-analysis, and the application of his work as a lens through which to view the findings. Hence, this chapter discusses the findings through this lens, bringing into conversation the literature on this topic that was briefly discussed in Chapter 2 and supplementing this with additional literature where appropriate.

Table 6.1: Mapping of meta-themes to sections in this chapter

Section	**Meta-themes**
Section 6.3	CISO supports hegemonical interests
	CISO as defence against ontological threat
	Businesses as ontologically insecure
	Cyber security as soothsaying
	Cyber security as sophistry
Section 6.4	Being a CISO means having identity issues
	Cyber security has multiple identities
	Business as Leviathan writ small
	Businesses as ontologically insecure
Section 6.5	CISO as agent of Leviathan
	CISO supports hegemonical interests
	Business as Leviathan writ small

A summary of the themes that are represented in each of the core sections of this chapter.

Table 6.1 further demonstrates the reflexive nature of this work. This shows that the themes developed from the analysis are each reflected throughout the different sections of this chapter, where they are discussed in the context of Hobbes' theories and associated literature.

6.2 A brief introduction to Hobbes

Hobbes' thesis, expounded in *Leviathan* and other works that follow a consistent thread, e.g. [413, 415], is one of structured power and the establishment of an effective (bourgeois) society [521]. His philosophy is both political and moral, and influenced a number of other major philosophical works, e.g. [508, 645]. As others have pointed out, e.g. [217], there is a need for caution when applying historical concepts to modern situations without acknowledging the circumstances in which they were authored. However, given the influence Hobbesian thinking has had on modern society [94], it would be "a missed opportunity" [217, p. 103] to ignore the value that can be offered by this analytical lens.[4]

Leviathan was written during the English Civil War,[5] and this turmoil was a key concern of Hobbes, who believed that his political science could avoid any recurrence and achieve a lasting peace. It is premised on an argument that, without effective

[4] It should also be noted that extensive conversation regarding Hobbes continues in IR and sociology and it is not within the scope of this thesis to explore these debates. Hobbes offers a starting point into wider viewpoints from these disciplines and provides one perspective, rather than an authoritative view on modern societies.

[5] Although it was a development of earlier ideas [16].

governance, humankind would exist in a state of war, "of every man, against every man" [414, p. 185].[6] In this state, regardless of the existence of "actuall fighting" [414, p. 186], there is "continuall feare, and danger of violent death; And the life of man, solitary, poore, nasty, brutish, and short" [414, p. 186]. The avoidance of this 'state of nature', as it is referred to, e.g. [546], is a primary motivation in the establishment of the Leviathan,[7] which provides security against it in exchange for obedience. This is one of the key tenets of *Leviathan*; citizens enter into a contract with the state in which this exchange takes place [118].

The observance of this contract, according to Hobbes, was fundamental to achieving peace within a society, and was based on both "the absolute right of sovereigns to command . . . and the absolute duty of the people to obey" [128, p. 613]. This obedience is consensual [207, p. 80] although citizens may suffer diminution as a result [788]. This contract, and the extension of Hobbes' ideas, may equate to tyranny, even totalitarianism [94, 109] and the Leviathan's "ultimate end is accumulation of power" [94, p. 180]. The tyrannical aspect is something that Hobbes himself does not deny and is, in fact, "proud to admit" [94, p. 188]. He is dismissive towards accusations of tyranny, labelling these as simply the protestatory responses of malcontents [414, p. 240].

6.2.1 Mini-Leviathans

Throughout this chapter, I characterise the organisation as mini-Leviathan, extending an idea from political scientist Richard Chapman who refers to the family unit as "*Leviathan* writ small" [207, p. 77] (italics in original), something I return to later. Hobbes saw corporations as intrinsic parts of the Leviathan, even as "vital" [443, p. 66] to it. However, he also identified them as potential threats, as "wormes in the entrayles of a naturall man" [414, p. 375], and in order to address these threats, they needed to be adequately governed [443]. Both these aspects, of being both intrinsic and also potentially threatening, were indicated in the present study by one participant's description of their organisation as "the soft underbelly" for their customers who performed various functions for the broader societies in which they operated. The vast majority of organisations in this study also articulated their 'role in society' in their

[6] *Leviathan* is "covertly gendered" [200, p. 118], with "the important actors in life [being] men . . . or very rarely . . . masculinized women" [200, p. 118]. The primacy Hobbes provides to men is clear throughout the text, and he was "writing for a male audience . . . from a male point of view" [286, p. 635n10].

[7] Hobbes uses the term 'Leviathan' to refer to the "Artificiall Man" [414, p. 81] that represents the state. The Leviathan is composed of multiple constituent elements including "*Magistrates* . . . *Reward* and *Punishment* . . . The *Wealth* and *Riches* of all the particular members . . . *Cousellours* . . . *Equity* and *Lawes*" [414, p. 81]. He considered the ruling power over that body (the "*Soveraignty*") to be that body's "Artificall *Soul*" [414, p. 81](italics in original text throughout).

annual reports.

Threats to the state Leviathan posed by corporations may be more pronounced where those mini-Leviathans are multinational entities and, therefore, not subject to a single sovereign power [205, 217]. This can result in those corporations being able to direct and influence legislation and regulation differently in the different states they operate in [634], frustrating attempts to achieve consistent control. Hobbes was concerned that companies would become so strong that they affected the Leviathan's own power [443]. Political philosopher Hannah Arendt points out that Hobbes could see multinational corporations as the logical endpoint of the "acquisition of wealth conceived of as a never-ending process ... for the accumulating process must sooner or later force open all existing territorial limits" [94, p. 189]. This view of corporations as potential threats is similar to his view of children as potential threats to the mini-Leviathan of the family [207, 415] if they are not adequately controlled (through education and punishment).[8] In the remainder of this chapter, I discuss some specific Hobbesian concepts in more depth, using these to derive greater meaning from the findings from the present study. This is motivated by multiple resonances within the data to these concepts.

6.3 "Perpetuall feare"

While the Leviathan exists to avoid the state of nature, it benefits from the continued presence of this threat in the minds of its citizens. Without this threat, the Leviathan's power and dominion over its citizens is diminished; in order to exchange obedience for protection, there needs to be some peril, otherwise the equation is imbalanced. Security of citizens from threat is "[t]he *raison d'être* of the state" [94, p. 181] (italics in original). Sovereignty is both achieved and maintained through fear [506]. Hobbes describes how "that which enclineth men least to break the Laws, is Fear" [414, p. 343] and, further, that fear may in fact be "the onely thing ... that makes men keep them [i.e., laws]" [414, p. 343].[9] He believed that "feare of some coercive Power" [414, p. 196], owned by the sovereign, was necessary in order to make citizens keep their promises [595]. Political scholar Joshua Barkan, discussing philosopher Roberto Esposito [320], describes "the sovereign's power to expose life to death as opposing but also interlinked sides of a persistent immunitary [*sic*] dynamic" [109, p. 89]. In other words, it is beneficial for the sovereign for threat to life to exist, so that the sovereign can offer protection to the citizenry from such a threat; if this threat ceases to exist, or ceases

[8] Indeed, Hobbes uses a parent-child metaphor when referring to a form of corporation [443, p. 78].

[9] Hobbes describes "Feare and Liberty" as "consistent" [414, p. 262], that is, being afraid makes a person no less free.

to be *perceived* to exist, then the power of the sovereign in commanding obedience is diminished.

The perpetual nature of cyber-security threat was clear from the data in the present study. The businesses I researched considered that cyber security was fearful and that cyber threat was normalised. For example, NED1 described being "a little scared" in relation to cyber-security threats and CEO2 described "panic" as a likely response to a ransomware infection. The normalisation was evident from comments such as "the [cyber-security] threats will only increase" (CFO1) and CEO1's description of cyber-security threat as "a constant". Similarly, the analysis of the annual report data highlighted that cyber-security threats were fearful and were growing in 'sophistication' and 'complexity', as well as in frequency. The "scary and inevitable" (CISO8) aspects of cyber-security threats are also commonly reflected in wider discourse, e.g. [596]. Businesses needed to accept that they would be compromised. This implies a "perpetuall cyber warre" [716, p. 120]. The businesses I studied existed in "continuall feare" [414, p. 186], threatened by "death, poverty, or other calamity" [414, p. 169] arising from something, i.e, cyber security, that was not well understood, even mystical,[10] as "perpetuall feare, [is] always accompanying mankind in the ignorance of causes" [414, pp. 169-70]. Building on the conception of the CISO-as-soothsayer from Chapter 4, the role of the CISO may be valued as one "that can make the Holy Water" [414, p. 692] that provides protection from fearful things,[11] and, therefore, is motivated to maintain the fear and dread that underpins their value.[12] Providing a further link to concepts of belief discussed in Chapter 4, the state of nature may even be considered as a "secular hell" [128, p. 618].[13] I now develop the "perpetuall cyber warre" [716, p. 120] concept further.

[10] The impacts of cyber-security threats may be considered by these organisations as 'real' but the threats themselves, including their sources, may be considered more ephemeral, as discussed in Chapter 4.

[11] Hobbes refers to the existence, and primacy of, "the Soveraign Prophet" [414, p. 467]. In the mini-Leviathan of the corporation, the CISO may be performing this role.

[12] This offers potential for cyber sophistry, as discussed in Chapter 4. Hobbes did not seem opposed to sophistry, at least in the classical sense of artful rhetoric [370], considering that "All Actions, and Speeches, that proceed, *or seem to proceed* from much Experience, Science, Discretion, or Wit, are Honourable" [414, p. 155] (emphasis added). However, elsewhere, when discussing various forms of "Divination", he does offer caution that "[s]o easie are men to be drawn to believe any thing, from such men as have gotten credit with them; and can with gentlenesse, and dexterity, take hold of their fear, and ignorance" [414, pp. 175-7].

[13] Similar metaphors have been used by others with reference to cyber security, such as "cyber hell" [678, p. 480] and "cyber apocalypse" [716, p. 105].

6.3.1 Permanent cyber emergency

The concept of permanent emergency was introduced in Chapter 2 and, to recap, this refers to the maintenance of a state of ongoing crisis in which a population is considered to be, or described as being, continually under threat. This environment facilitates the establishment of various responses to those threats that restrict the freedoms of citizens, in the name of 'security' [179, 568], a concept which has many parallels with Hobbes' state of nature and which has been highlighted as underpinning power structures by others, e.g. [337].

Positioning cyber security as an existential threat, as a war with "apocalyptic" [716, p 121] consequences, may also allow for exceptionalism and deviance from existing laws, both national and supranational. Hobbes explicitly permitted defiance of law if motivated "by the terrour of present death" [414, p. 345], and also believed that "when peace is unattainable it is rationally allowed to wage war" [355, p. 245]. Such exceptionalism based on existential threat can be observed in modern societies, e.g. [38, 745, 746], including in relation to cyber-security threats [498, 766]. The fear, indeed, the "moral panic" [221, 498] generated by these threats propels citizens into "the waiting arms of whoever might be ruling" [207, p. 88].[14] Such fear may be a "necessity-justification" [207, p. 89] for enduring power, and, as Chapman suggests, it is straightforward to conceive of such "justification … [occurring] at the state level, as a function of real or manufactured inter-state crises" [207, p. 89], particularly with regard to threats that are hard to understand or somewhat ephemeral in nature, such as those related to cyber security. If cyber-security threats, or the "staging" of those threats [123, p. 10], result in fearful and bewildered citizens, those citizens are easier to moderate. Educating citizens on, or even communicating the existence of, cyber threats may couple "paranoia with pacification" [207, p. 90]. Additionally, as "war conceals history" [337, p. 158], there are additional benefits to those in power of maintaining a perception of cyber war.

References to national security, as observed in the data from the present study, also connect with this warfare motif. Examples of this indexation include one participant's description of being "acutely conscious of the sectors we play in, of meeting our responsibility to do our best to defend against [a cyber-security] attack",[15] cyber security being "an [easy] way to cause havoc in an enemy country" (CFO2), and one CEO describing being specifically obligated by government to take certain actions in relation to national security. Some participants described being regularly assessed by security

[14] The political benefits and motivations relating to the use of fear have been highlighted by many other scholars, including relation to cyber security, e.g. [498].

[15] Not attributed to limit the risk of identification.

services and other government departments.[16] Similarly, a number of these business articulated their role in, and obligations relating to, national security in their annual reports, with this being a 'critical market' in a number of instances. Both CISOs and non-CISOs made reference to threats from "rogue states" and "cyber war", as well as related expectations from government. This included participating in national security working groups as well as other interactions with national intelligence agencies in relation to cyber security. There were references to invitation-only and industry-specific information exchanges with representatives from state security services where specific threats were shared with attendees, as well as indications of more indirect governmental influence. The latter included senior leaders being invited by government departments to participate in "roundtable discussions". Such fora, in which government intelligence services share details of cyber threats with specific industries,[17] demonstrate the role that governments play in maintaining a state of permanent cyber emergency. They provide a mechanism through which governments can both maintain fear and amplify it. This could be achieved through exaggeration or even fabrication, particularly when considering the reliance of the state Leviathan on the persistence of this fear.[18] If the nation (or business) is 'under threat' then there is a collective sense of conflict and, therefore, a suggestion that everyone has to play their part.

Businesses that publicly articulate their cyber-security capability, through references to the existence of dedicated personnel and the actions they are taking to mitigate cyber risk, are demonstrating their strength and their readiness for war in a "calculated presentation" [337, p. 92].[19] Such pronouncements, particularly in annual reports, also serve to maintain the organisation's power by "memorializ[ing]" [337, p. 67] what the organisation has achieved, arguably also creating "an obligation" [337, p. 67] for future leaders of that organisation.

6.3.2 Survival

Hobbesian logic is based upon the avoidance of "death, pain, and disability" [355, p. 243] and that such "natural reason … makes use of instrumental reason and verbal reason to achieve its goals" [355, p. 248], that is, "the avoidance of an avoidable

[16] One participant described having been visited by representatives from the UK intelligence services immediately prior to the interview, which may have affected their responses.

[17] And, according to one participant, encourage the use of certain cyber-security frameworks.

[18] The use of falsehoods in the service of continued peace was something that Hobbes appeared to support [414, p. 703] [93, pp. 224, 290-1], although, as political theorist Teresa Bejan summarises, this reading is debated and other scholars have found his intentions "far less sinister" [128, p. 623n13]. However, Hobbes was clear that the authority of the sovereign was absolute, even in matters of "Prophecy" [414, pp. 466-469].

[19] This includes the use of CISOs as totems, as discussed in Chapter 4. Hobbes refers to a superstitious aspect to totems, in that they bring luck, particularly in situations of war [414, pp. 171-2].

death" [355, p. 249]. Hobbes believed that "the terrour of present death" was even a valid excuse for an individual to commit a crime "because no Law can oblige a man to abandon his own preservation" [414, p. 345], and described how "since every man hath a Right to preserve himself, he must also be allowed a Right *to use all the means, and do all the actions, without which He cannot Preserve himself*" [415, p. 5] (italics in original). However, such is the drive for self-preservation, that, without the governance of the Leviathan, this would lead to the 'war of all against all' [414], due to the "independence of the individuals in determining the best means to preserve their own life" [443, p. 74]. As well as self-preservation of individuals, Hobbes is "unequivocal that self-preservation is the primary goal of those forming a commonwealth" [540, p. 115]. Hobbes' concerns regarding survival, both of individuals and of the Leviathan itself,[20] are echoed in discussions in classical organisational literature regarding a business's concern with ensuring its own continued viability, e.g. [126, 549].

As explored in Chapter 4, survival was a concern for the businesses I studied. Cyber security was positioned as a threat to viability by many of these organisations, with fear of regulatory action, and associated fines and reputational damage, being a particular concern. This was evident from the analysis of the annual reports as well as the interview data, where a cyber-security incident could mean that "[in] the worst case ... your business is over" (CISO5). Such concerns with viability and survival, arguably the primary motivation for businesses [126], are analogous with Hobbesian "natural reason", seeking to avoid punishment that could lead to "pain, and disability" and, ultimately, "death" [355, p. 243]. The punishments they sought to avoid were enacted by the larger Leviathan of the state, for example, the "massive" regulatory fines referred to by CISO9 and the risk of imprisonment and "personal liability" of senior leaders highlighted by CISO15. These businesses cascaded this concept, instituting their own mechanisms of punishment for their employees, as I discuss further below. Internal experts were positioned by many of these organisations as 'guards' that protected them against the various harms that they faced. CISOs were seen as assuagement against threats to business viability, with CISO14 providing "[a] level of comfort" to their senior stakeholders and CISO6's existence being "a comfort factor". They helped these businesses to manage the uncertainty those threats presented, and ensure their continued survival. This allowed them to shape their future to a certain extent, aligning with Hobbes' encouragements towards continued attentiveness to threats [716], but also provided a resource that articulated and predicted those threats, based on both past, and imagined future, events.

Keeping this sense of a perceived ongoing menace with regard to cyber security in

[20] Through the avoidance of war.

mind, I now explore Hobbes' core social contractual exchange further.

6.4 Protection in exchange for (cyber) obedience

As with the Leviathan and its citizens, organisations in this study required obedience from their staff, in terms of policy compliance, as well as alignment with standards of behaviour. Cyber security was a particular area of discipline and of punishment. Obedience, whether through completion of mandatory training, compliance with cyber-security policies and standards, or through effective management of cyber-security risk, was mandatory and non-compliance would be punished. As described in Chapter 4, attempts to interfere or bypass cyber-security controls would result in "a disciplinary . . . that's known" (CISO3).

As well as disciplinary action, non-compliance resulted in impacts upon staff remuneration, particularly at a senior level. The potential for the organisation to remove a level of security from its staff, in terms of the security of continued employment and income, suggests the "immunitary dynamic" [109, p. 89] mentioned above. As with the Leviathan, these businesses were providing protection in exchange for obedience and if this obedience was not received, their protection could be removed. This included obedience to aspects of culture, with deviation from the latter resulting in punishment, as described in a number of annual reports.

Cyber security was also associated with state-directed punishment. For example, CFO2 referred to "sanctions from government" (CFO2) and CISO15 described needing to have "a defendable position" (CISO15). The threat of punishments relating to cyber security had a regulatory effect on these organisations, with considerable attention paid in the annual reports to addressing how compliance was monitored and enforced, including references to the organisational capabilities charged with these responsibilities. Organisations in this study wanted to 'do the right thing' in order to avoid punishment by the Leviathan and internally, as mini-Leviathans, instituted mechanisms of punishment for their employees, extending that same concept. The references that participants made to the 'usefulness' of cyber-security incidents affecting other organisations suggest a Hobbesian view of punishment as providing examples for others but also indicate a spectacular nature to cyber-security punishment. For example, CISO4 stated that "if there's an incident or a breach or a loss event that is topical . . . you want to use that . . . it will resonate with [board members]" and CEO2 portrayed major incidents (affecting other organisations) as "manna from heaven if you're trying to get people interested in cyber security". There were also explicit references to those incidents that resulted in regulatory action, such as the "massive" regulatory fines referred to by CISO9.

This spectacular nature to cyber-security punishment, as can also be seen in the way that regulators articulate their responses to data security incidents affecting businesses, e.g. [60, 61], is similar to that described by both Foucault [336] and legal scholar Anthony Paul Farley [323].[21] This aligns with Hobbes' views on the value that punishment provides, for the purpose of "correction, either of the offender, or of others by his example" [414, p. 389]. He considered that "the severest Punishments are to be inflicted for those Crimes, that are of most Danger to the Publique" [414, p. 389]. Punishment itself is a representation of power [336], something I return to later in this chapter. The (state) Leviathan is terrorised by cyber-security threats, whether real or imagined, which, in the most fearful type, arise from the Leviathan's known enemies. It expects its "lesser Common-wealths" [414, p. 375] to take action against these threats for the benefit of the larger commonwealth. Failure to obey results in punishment by the Leviathan, such punishments being public spectacles that provide examples to others.

As discussed in Chapter 4, the cyber-security departments in these organisations appeared to function as an official police force, despite CISOs wishing to avoid this characterisation, and performed surveillance of staff. They acted as agents of the mini-Leviathan, applying discipline and punishment. Beyond cyber security, these organisations applied punishments if staff did not comply with their dictates, including if they behaved contrary to their values. Punishment was imbued with morality by extending a concept of 'doing the right thing'.[22] These organisations educated and indoctrinated their staff, with fear being a component of these processes, something I now explore in more detail.

6.4.1 CISO as teacher and "counsellour"

Hobbes "sought to cool men off, to pacify them, to drive them into the waiting arms of whoever might be ruling with the frightening imagery of a state of nature" [207, p. 88]. One of the mechanisms through which he intended to achieve this was through education. Hobbes had a clear view on education as being authoritarian and as being a role, indeed, a duty, of the state [128]. What Hobbes wished to be taught, according to Bejan, was Leviathan's "'doctrine' ... This doctrine was no more than the existence of a 'mutual relation between protection and obedience', which required an 'inviolable observation'" [128, p. 613]. Hobbes believed that the sovereign's power should be "utterly authoritarian in principle ... and vigilantly oversee the intellectual life of his

[21] Farley also invokes Hobbes in his exploration of state punishment.

[22] Concepts of morality in connection with Hobbes are discussed further in Section 6.5 below.

subjects from the cradle to the universities, and from there to the grave" [128, p. 621].

Hobbes saw the family unit as playing a crucial role in initiating this obedience [207]. He saw parents as "representatives of the sovereign power" [128, p. 620], and that "[b]y direction of the sovereign, the connection between protection and obedience is to be made quite clear" [207, p. 82]. As Chapman summarises, "[i]n teaching a child the nature of obedience in the family, a parent is teaching the nature of obedience in the state" [207, p. 86] and, in addition, "[t]o teach one's children that their obedience is due when protection is given is to learn the same lesson for one's self" [207, p. 88]. The control over language that the Leviathan holds, as discussed in more detail below, underpins Hobbes' emphasis on education rather than force as the method by which the Leviathan maintained power [786], such control also helping sustain its identity [129]. However, Bejan [128, pp. 619, 623n17] argues that Hobbes intended to stress discipline rather than education or training, which are alternative translations of the *disciplina* used by Hobbes in *De Cive*.[23] Hobbes did appear to consider discipline and chastisement to be productive motivators for learning, with "negative reinforcement ... [being] an effective teacher" [207, p. 85].

As discussed in Chapter 4, the CISOs employed by the organisations in the present study were educators, which included "teaching ... obedience" [207, p. 86] and applying discipline. They ensured that the organisation's employees were "educated well" (CISO3) and that instances of non-compliance were brought "back on track" (CISO12). Staff were educated that both they, and the organisation itself, were subject to cybersecurity threats. In order for the organisation to mitigate those threats, protecting both itself and its staff, those staff must forgo certain liberties and agree to be regulated. As CISO4 described, "there's gotta be an amount of, you know, disruption that is necessary in order to do the right thing". The CISOs also utilised fear in their instruction, for example, using "war games [with senior leaders] ... and you watch them shit themselves" (CISO11), which itself aligns with Hobbes' template [207].

"Counsell". As well as being teachers, CISOs were advisors, "Counsellours" [414, p. 391], for these businesses. Hobbes distinguishes the value of "Counsell" from that of "Command" in that the latter "is directed to a mans [*sic*] own benefit" whereas the former is "to the benefit of another man" [414, p. 303]. He defines "the first condition of a good Counsellour ... [as being that] *his Ends, and Interest, be not inconsistent with the Ends and Interest of him he Counselleth*" [414, p. 307] (italics in original) and describes how

> "the Ability of Counselling proceedeth from Experience, and long study ...

[23] In which Hobbes states "Man is made fit for Society not by Nature, but by Education" [415, p. 8].

> *No man is presumed to be a good Counsellour, but in such Businesse, as he hath not onely been much versed in, but hath also much meditated on, and considered*" [414, p. 307] (italics in original).

Hobbes also identifies the need for interpretation in relation to "All Laws, written, and unwritten" [414, p. 322], which aligns with the interpretative aspects of the CISO role identified from the data, as discussed in Chapter 4.[24] He considered that "The wit required for Counsel ... is Judgement" [414, p. 308] and believed that "[t]he most able Counsellours, are they that have least hope of benefit by giving evill Counsell, and most knowledge of those things that conduce to the Peace, and Defence of the Common-wealth" [414, p. 391]. The CISOs in this study were certainly demonstrating the latter, helping to support this characterisation of them as "Cousellours". For example, CEO1 described having a need for the CISO to tell them "no you don't need to be worried about that, yes you do need to be worried about this" in relation to cyber security. The non-CISO stakeholders expected their CISOs to have the right level of experience and qualifications, aligning with Hobbes' expectations around "Experience, and long study". For example, CIO1 articulated the need for any individual who was responsible for cyber security to have "the credentials in place to do that first" and described how their staff have "incentives to gain qualifications quickly". The CISO-as-counsellour may reasonably be expected to have consistent "Ends and Interest" with the organisation, but may still derive "benefit by giving evill Counsell" [414, p. 391], as discussed in Chapter 4, particularly if that benefit is continued employment. However, there is a particular distinction between CISOs and Hobbes' counsellours in that they do not appear to share equivalence with regard to the risk of scapegoating. Hobbes' view was that "he that demandeth Counsell, is Author of it; and therefore cannot punish it" [414, p. 304]. This is contrasted with the CISOs in this study, who indicated concerns that they were, in fact, subject to punishment through job losses, such as CISO12's recognition that "it's implicit with our role, if something goes wrong ... you're the guy [that gets fired]".

6.5 Cyber security and the Leviathan(s)

It is not in the interests of a Hobbesian society to achieve "complete security" [94, p. 184]. Both the relative novelty of cyber-security threats and the continued emergence of

[24] However, Hobbes' views on what "make[s] a good Judge, or good Interpreter of the Lawes" are, perhaps, questionable, as, although on one hand preferring unemotional assessment, on the other he expects those that "have had most leisure" to make the best interpreters and for there to be no need to have learned from "other mens Writings" [414, p. 328].

new types of such threats, including the 'sophisticated' aspects thereof, can be viewed as "new props from the outside" [94, p. 184] that stoke the flames of the possibility of war, particularly when attributed to nation states, e.g. [238]. These threats also offer "new and ever-growing fields for the honorable and profitable employment" [416, p. 28] of citizens,[25] particularly the bourgeoisie, who are appeased by new job opportunities and further stimulate consumption and growth [94].

In a (post)modern world where threats to the state are less obvious or apparent, i.e., there is no obvious invader on the doorstep, particularly since the end of the Cold War,[26] the inclination of the citizen towards obedience may be weaker. The state may, therefore, feel the need to motivate obedience by making it clear that it is still offering protection, but not against obvious invaders. Rather, it is against opaque, mysterious, and highly sophisticated threats, from which the state is providing protection.[27] Not only do these threats need to be explained by specialists, due to their complexity, they also need to be 'sold' to citizens through education. It is even conceivable that such teachings could be contrary to "true Philosophy" [414, p. 703] but serve the benefit of the state, as well as securing the continued employment of the teacher [93]. This could motivate the embellishment of any threats communicated. It may be more advantageous for the state Leviathan to have such education delivered not through a state organ but rather through another component of society such as businesses. Rather than a conscious decision taken by the Leviathan this may be a fortuitous benefit, but one that it seeks to encourage through, e.g. communicating the 'responsibility' that businesses have in protecting wider society against cyber threats [747]. This was mentioned by CEO2, who described how "the UK government has been . . . quite vocal [on cyber security] in recent years".

6.5.1 The role of mini-Leviathans

Barkan argues that "corporate power and sovereign power are *ontologically linked*" [110, p. 4] (italics in original). The "entanglement" [382, p. 741] between corporate businesses and states provides a link between the concept of state Leviathans and the corporation as both agent-of-Leviathan[28] and as mini-Leviathan in its own right. Echoing

[25] Specifically, the employment of "sons" [416, p. 28].

[26] This section was written prior to the February 2022 invasion of Ukraine by Russia. However, the point still stands that the current level of nation state aggression globally is not equivalent to that experienced during the Cold War period.

[27] Hobbes, in a broader (politically-driven) polemic against (principally) Catholicism, describes how priests and other representatives of these belief systems benefit from "their Dæmonology", through which they "keep (or thinke they keep) the People more in awe of their Power" [414, p. 708]. Also cf. the CISO-as-soothsayer concept from Chapter 4.

[28] A possibly unintended consequence, which I argue in more detail below.

Chapman [207], Heath et al. refer to a corporation as "a society writ small", but also as "an actor within the larger society in which it operates" [399, p. 437]. Part of the role that a corporation plays as agent-of-Leviathan is in the generation of "social wealth" [217, p. 123] and partly through enacting regulatory control over the citizenry [110], even acting as a form of police [109, 338, 592].

The organisations in the present study taught their staff about the existence of cyber-security threats, communicated a defined set of rules, indoctrinated them into acceptable behaviours, monitored their compliance against these, and punished them when they transgressed. In order for both the organisation and their staff to be protected from these threats, staff were required to forgo certain liberties and agree to certain controls, such as being surveilled, as was described in both the interview data and the annual reports. Considering power relations as interactive, processual and two-way [129, p. 89], cyber-security practices within business can be seen as a mechanism through which employees participate in the maintenance of hegemonic power.[29] The present study suggests that CISOs repeat messages of insecurity and threat, and perform a policing role that normalises surveillance. This was also indicated by CEO1's comment that "[when staff] see the art of the possible and it's scary ... they say okay, I'm gonna whine less". Consequentially, the organisation's employees, who are also citizens of the states in which they live, inadvertently support hegemonic power in the role they play as the surveilled.

Cyber security and state power

The messages that CISOs support, and repeat, to the company's employees and their customers, relate to a broader security agenda [568]. There is a wider security industry that "must ... ensure that security is never really achieved" [568, p. 156]. This provides commercial benefits, as well as supporting an insecurity that is relied on by the state to achieve its aims [94, 568]. If states ultimately seek the perpetuation of (at least partial) insecurity, then it may be in their interests to define 'security' in an insecure manner, at the same time encouraging organisations and wider society to achieve a level of 'insecure security'. Recent attempts by governments to weaken or circumvent strong encryption, e.g. [53, 732], some successful, e.g. [723], can be argued as demonstrating this desire.[30] In addition, motivating organisations to operate a cyber-security function that accustoms employees to increased and intrusive surveillance and monitoring may

[29] Other hegemonical linkages identified in the data included the roles that these businesses played in national security and the presence of senior leaders on company boards that represented military or governmental actors, as well as references to both direct and indirect governmental influences on these organisations.

[30] Although increased surveillance may be possible without weakening encryption [351].

also contribute to this same ‘insecure security’, albeit potentially providing associated benefits to those employees, such as greater privacy.[31]

Cyber security can be used to terrorise citizens into compliance and to justify their surveillance. Cyber-security controls in businesses have an effect not just on the employee-as-employee but also the employee-as-citizen. Educating employees on what they need to be protected from, and what they need to obey in order to be protected, may, directly or indirectly, condition them towards broader obedience, including acceptance of controls that could be used beyond purposes of cyber security, providing benefits to the state over and above citizen protection.[32] The use, and acceptance, of surveillance in these organisations may function as a normative control [124], conditioning or preparing staff (citizens) to be surveilled in wider society and supporting a broader meta-narrative in relation to exchanging privacy for security. As described by CEO1, employees need “to tolerate some inconvenience ... because people become safer”. Such normalisation may be indicated by the seemingly unconcerned responses by many to the Edward Snowden exposé [117].[33] Mass surveillance by the state is no longer concealed and, according to CEO1, should be acquiesced to without question.[34] Although in some cases illegal [158], “[g]eneral surveillance of the population” [336, p. 280] may “not need to be written into the law” [150, p. 397] [336, p. 280]. The Leviathan-writ-small of the business plays a role on behalf of the state Leviathan in conditioning the employee-as-citizen towards obedience, and surrendering of liberties, in exchange for protection from threat. The opaque and relatively unseen nature of the threat, which requires specialists to deliver education about its existence, is beneficial to the state for ensuring continued obedience, and even in maintaining its own identity [401], and its own history [686].

In a Hobbesian society, there is a never-ending need for the state to expand its power; “only by constantly extending its authority and only through the process of power accumulation can it remain stable” [94, p. 184]. If such a society were to achieve “complete security”, then the state’s power would crumble [94, p. 184]. As Arendt describes, the “ever-present possibility of war guarantees the Commonwealth a prospect of permanence because it makes it possible for the state to increase its

[31] However, this greater privacy may still be conditional, i.e., they may be protected from external privacy threats and yet be exposed to internal ones.

[32] “The most potent weapon in the hands of the oppressor is the mind of the oppressed” [139, p. 137]. Also cf. lawyer Joseph Servan’s statement that “[a] stupid despot may constrain his slaves with iron chains; but a true politician binds them even more strongly by the chain of their own ideas” [670, p. 34] [336, pp. 102-3].

[33] Although public acceptance of mass surveillance seems to be dependent on many factors, and differs by country [204].

[34] “[Various governments] keep an eye out, which works in ways that neither you or I need to know how it works”.

power at the expense of other states" [94, pp. 184-5]. She further elaborates the need for a "never-ending accumulation of power [as being] necessary for the protection of a never-ending accumulation of capital" [94, p. 186] and how this has underpinned imperialism and indeed modern society.[35] Cyber security may, therefore, be implicated in the maintenance of state power, as has historically been observed with regard to "land, sea, air, and outer space" [162, p. 41]. Indeed, historical 'success' in achieving power through domination of those realms may be at the root of characterising cyberspace as an equivalent "domain of warfare" [162, p. 49]. Cyber security, or, more specifically, the sense of ongoing cyber threat, particularly from established enemies such as "China ... Iran" (CISO8), "somebody sitting in Siberia ... North Koreans", enables the maintenance of a "silent war" [337, p. 16], which, as Foucault describes, "reinscribe[s]" power structures, on "institutions, economic inequalities, language, and even the bodies of individuals" [337, p. 16].

Foucault and Hobbes. Although this chapter focuses on Hobbes, a brief tangent in relation to Foucault is warranted, particularly as he discusses power in depth, and *Leviathan* itself, in *Society Must Be Defended* [337]. Both Foucault and Hobbes offer differing, but not necessarily opposing, perspectives with which to explore the role that cyber security plays in structures of power.[36] Foucault's approach to studying power is "to abandon the model of Leviathan" [337, p. 34], and rather to focus on "the techniques and tactics of domination" [337, p. 34]. He describes power as "something that functions only when it is part of a chain" and is "exercised through networks" [337, p. 29]. The cyber-security industry, and cyber-security professionals such as CISOs, form part of this chain, and, following Foucault's perspective, the suggestion from this analysis is that cyber security functions as a "mechanism of power" [337, p. 30]. It is possible to take this further, and extend Foucault's arguments, that cyber security functions as a mechanism of power partly because it generates "economic profit" [337, p. 33] and partly because it offers "political utility" [337, p. 33]. Cyber security enables and supports power through "material operations [i.e., to economic ends], forms of subjugation [e.g. surveillance]" [337, p. 34] and, additionally, constitutes an "apparatus of knowledge" [337, p. 34] that is essential to the functioning of power [337, pp. 33-34].[37] Indeed, it constitutes a (relatively) new "branch of knowledge" that can not just

[35] Modern globalisation practices being equivalent with imperialistic ones [214]. Hobbes himself was actively involved in colonial enterprise [443].

[36] It is considered outside the scope of this thesis to explore further how Foucault's thinking can be applied to cyber security (and, indeed, others have previously applied Foucauldian lenses to this subject, e.g. [684]), however, this is a consideration for future research.

[37] Elsewhere, Foucault suggests that "power and knowledge directly imply one another ... there is no power relation without the correlative constitution of a field of knowledge" [336, p. 27].

augment but "multipl[y]" existing power in a cycle [336, p. 224] that, depending on perspective, is either vicious or virtuous.[38]

Foucault identifies the industrial economy as a motivating force behind the growth of what he refers to as "disciplinary power" [337, p. 36] (as opposed to sovereign power), particularly identifying "constant surveillance" [337, p. 36] as a requirement to ensure the effective "extract[ion] [of] time and labor" from "bodies" [337, p. 35]. Cyber security offers not just a mechanism for achieving this surveillance, and, therefore, supports a productive industrial society, but also a means by which that surveillance, if not "concealed" [337, p. 37], can be justified on the basis of there being an ongoing 'war', an "uninterrupted battle" [337, p. 47]. Within the context of a business, cyber-security practices function as what Foucault describes as a "local tactic of domination" [337, p. 46] that supports "global … structures of power" [337, p. 46]. The role of war is "to protect and preserve society", it is "the precondition for [society's] survival" [337, p. 217] according to Foucault. Therefore, contrary to a Leviathan intending to prevent a war of all against all, a Leviathan needs there to be a war, in order to maintain its power, and identity. Cyber security offers a mechanism by which this war can be created and maintained, and is particularly valuable in enabling that war to be "silent" [337, p. 16] and, through being specialist and arcane,[39] difficult to counterargue. Its intractable and ephemeral nature make it highly suited to both "dazzle" and "petrif[y]", to perform "a magical function" [337, p. 68]. Its military associations, as identified in Chapter 4, can help to justify expenditure, and, in its own right, cyber security produces economic benefits beyond the 'silent war'. I now briefly discuss how an increase in consumption benefits the Leviathan.

Consumption

Companies within a broader security industry accrue benefit from perpetuating a state of insecurity [483]. This may be exploited through a narrative of unforeseeable risks that builds uncertainty [483], fear stimulating consumption [116] in the same way as war [768]. The security and defence industries need there to be something to be defended against [568]. As well as cyber security being one of these industries, cyber-security capability is a factor in being 'allowed to play' in others, and can be a barrier to entry, as observed in the present study. Cyber security is thus enmeshed with a much broader aspect of modernity[40] in the sense of continued consumption, both as

[38] Following on from discussions of morality in Chapter 4, it is perhaps the intent of many that it is seen as the latter.

[39] "A dark art" (CISO4).

[40] And, indeed, history; Hobbes is clear that "Mony [money] [is] the Bloud [blood] of a Commonwealth" [414, p. 300].

an ("expensive"[41]) industry in its own right and as a facet of other industries. Some organisations in this study indicated, in their annual reports, the benefit they accrued from governmental spending on security-related products and services, further demonstrating the link between societal threat and certain business sectors. The Leviathan, which seeks continued and never-ending growth, can stimulate expansion by creating a need for spending that counteracts fear and anxiety [116].[42] Where that fear and anxiety is generated by unseen and ever-more-sophisticated sources, there is, in theory, no upper limit to the growth that could be achieved.

I propose a summarised view of the different interactions described throughout this section in Figure 6.2 below, which is influenced by Saldaña [653].[43]

[41] CEO1 and CISO6 both used this term explicitly, while the majority of CISOs described cyber security in similar terms.

[42] However, such spending can, arguably, "in some way 'improve' life in civil society" [768, p. 111].

[43] The interactions shown in this diagram also suggest opportunities for future research, which I summarise in Chapter 7.

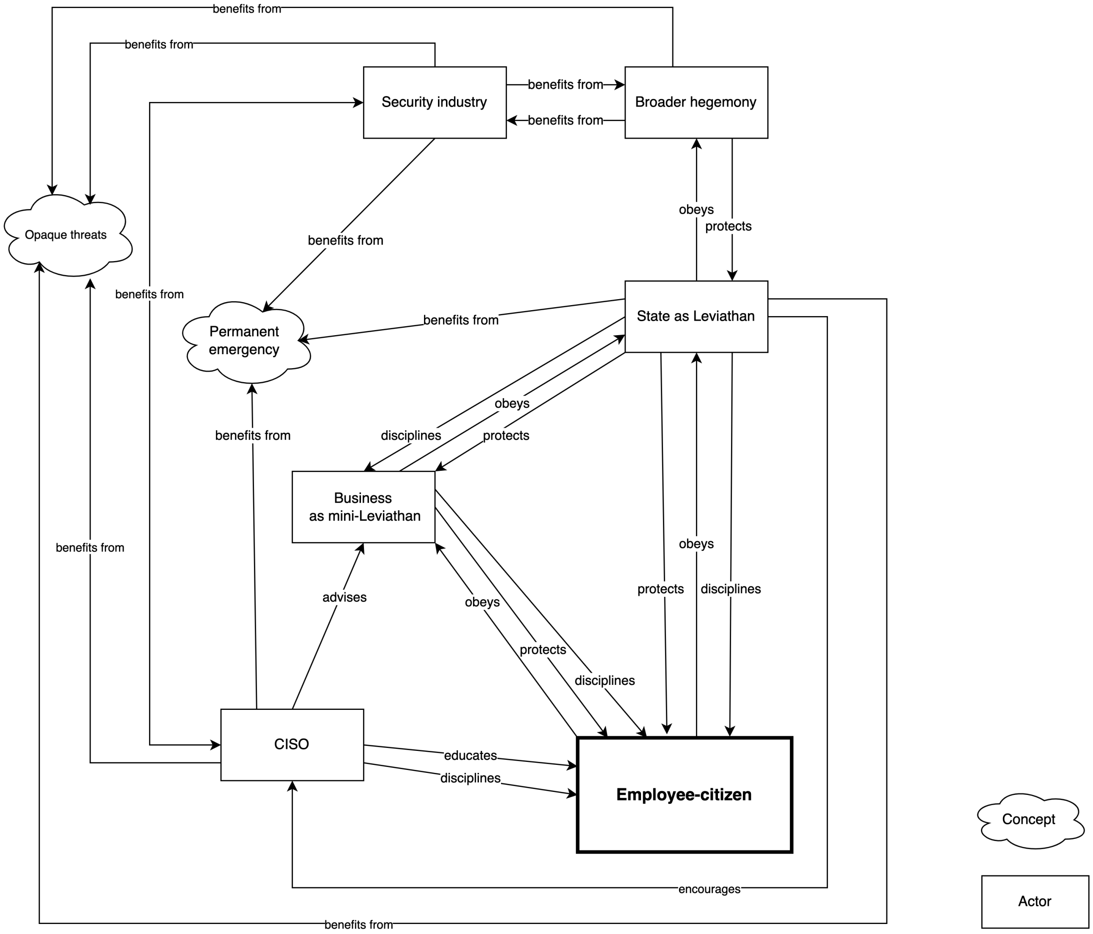


Figure 6.2: Interactions between phenomena identified from the data.

This diagram suggests that there is a broader cycle of benefit and control associated with cyber security, with multiple actors playing their part in maintaining that cycle. The CISO plays an important role in (directly or indirectly) maintaining this control, and also accrues benefit from the maintenance of a permanent emergency. They are encouraged in their role through messages from the state Leviathan that perpetuate the existence of that emergency and advise the mini-Leviathan of the business to maintain a social contract with their employees that exchanges obedience for protection, with the CISO performing a disciplinary role in this contract.

Cyber security offers a means for a Hobbesian state to grow or maintain its extraterritorial power, as well as its power over its own citizens. While other state Leviathans may contend the former, the latter may be opposed by those citizens, who, according to Hobbes, hold the right to rebel against the Leviathan if such rebellion is for self-defence [786]. As a precaution against such an eventuality, the Hobbesian state must "have recourse to arms to enforce civil order" [786, p. 221]. In *De Cive*, Hobbes describes how "[a]ll judgement therefore in a City belongs to him who hath the swords" [415, p. 48]; as mentioned earlier, the Leviathan is tyrannical. But the state must also remain trusted by its citizens, particularly in its determination of what is and is not a threat [786], and the most important control that the sovereign should have is over "language (which defines what is)" [786, pp. 219-220], something I now discuss in more detail.

6.5.2 Cyber-security discourse and politics

The collocation of certain words observed in the data, e.g. 'sophisticated' and 'threat', which are also seen in broader cyber-security discourse, e.g. [577], may carry "encoded ideologies" [129, p. 113] that serve to maintain power structures. References to 'nation state' alongside 'cyber threat' carry an association of war being waged. This was seen in the data, with, for example, CEO1 referring to being "attacked [by] somebody sitting in Siberia ... the Chinese ... North Koreans". Equally, references to terrorist threats, as also observed in the data,[44] can be argued as indexing ideological positions that demonise, and, therefore, exclude certain 'others', establishing the existence of "barbarian[s]" that are outside of (the West's) "civilization" [337, p. 195].[45] As "packaged, homogenized violence" [116, p. 160], such references not only maintain hegemonical power ('we' are threatened by 'them' therefore 'we' must take action) but also provide a means by which citizens are mollified, arguably even tranqullised [116].[46] Cyber security has its own discourse, which as well as establishing it as an expert system, establishes norms and provides it with power [337, p. 38].[47] This includes an "apocalyptic framing" [716, p. 121], something identified in historic discourses of power [337, p. 56], as well as a "mystification" [337, p. 269], both of which were identified in the data from the present study. Cyber-security impacts could be "catastroph[ic]" (CISO11), "debilitating" (CISO4) and "disastrous" (CISO9). Cyber security was "opaque and ... pervasive" (CISO15), and "most people won't understand it" (CISO4). Discourse that

[44] The annual reports featured references to cyber terrorists and non-cyber related terrorist threats were also mentioned in some cases.

[45] The implementation of the USA PATRIOT [*sic*] Act (which had considerable focus on cyber security [587]) in response to the September 11 2001 terrorist attacks resulted in significant discrimination against Muslims [605], and, in this context, it is notable that there are derogatory references to Islam in Leviathan, e.g. [414, p. 177], which go beyond his critiques of Catholicism. Each of these may be politically motivated, and certainly in the case of the latter given the historical context.

[46] As well as driving consumption [116].

[47] Foucault describes how, historically, "knowing the secret behind technological knowledge was a source of wealth" [337, p. 179]. As mentioned in Chapter 4, salary ranges in the cyber-security profession seem to indicate that this may still be the case.

positions cyber security as a perpetual war is what Foucault describes as a "historico-political" [337, p. 57] discourse that enables ("entitle[s]") those in power "to define the norm" [337, p. 60], including moral norms. These norms, and the power associated with them, can be indexed by those who seek to dominate [337, p. 45].

In a Hobbesian society, defining "what is" [786, pp. 219-220] includes defining what is right and what is wrong. Hobbes viewed morality as subjective [619, p. 42], and considered it to be the responsibility of the Leviathan to determine what qualified as "good and bad, true and false, right and wrong" [786, p. 230].[48] For Hobbes "truth is a function of logic and language" [786, p. 217] and "what is granted to that authority [i.e., the Leviathan] is the right to decide among irresolvably contested truths: to provide the authoritative criteria for what is" [786, p. 219]. This "control of normative doctrine" [506] assigned to the Leviathan means that as well as defining what is right and wrong, the state can define *who* is right and wrong, and of the latter, what threats they pose, resulting in, possibly deliberate, othering, as discussed in Chapters 4 and 5. If sovereignty is predicated on, or maintained using, fear, and if the sovereign has authority to determine what (and who) is to be feared, then it is in the sovereign's interest for there to exist "demons ... villains" [568, pp. 119, 223], "barbarian[s]" [337, p. 195]. Otherwise not only is the state's authority in question, as its citizens are providing obedience without receiving anything in exchange, as there is nothing to be protected from, but even its identity as a state may be threatened [401].

Hobbes does not refer to the benefits accruing to the state of maintaining the existence of specific threats, nor encourage their invention, however, in a criticism of religious authority, he does point out "who, that is in fear of Ghosts, will not bear great respect to those that can make the Holy Water, that drives them from him?" [414, p. 692]. By maintaining discourse that defines, or repeats, who and what are threats, and the relative urgency of those threats, the state can maintain broader narratives of fear, war, friend and enemy, good and bad, and right and wrong. Such narratives in connection with cyber security featured in the data but, in particular, the articulation of cyber threats in moral terms was consistent, as discussed in Chapter 4. A moral association may strengthen the power and importance of these threats for citizens but also result in unquestioning acceptance of those positions. Although morality may (arguably) be subjective [797],[49] it may be *experienced* objectively in everyday life [418] and, therefore, by assigning a moral dimension to cyber security, citizens may be discouraged from challenging the 'need' for intrusive controls associated with it.

[48] Hobbes' morality continues to be a topic of some interest, and debate, for many scholars, e.g. [505].

[49] It is outside the scope of this thesis to explore the ongoing and unresolved philosophical debate concerning this highly contentious position [293].

Specialist language

The use of specialist cyber-security language, which is inaccessible to non-specialists,[50] provides power to those that can understand it [337, p. 100], and this power is increased when there is an interpretation being provided.[51] An interpretation provides an opportunity, conscious or unconscious, to imbue its translation with other meanings, whether moral, political or emotional. CISO8 described a key part of their role as "a whole lot of translating threat landscape into reality", and language is a means by which reality is both experienced and constructed [129]. Those who have the power to interpret specialist or 'foreign'[52] language also have the power to construct reality for their audience. Cyber security may offer a channel through which sentiments and beliefs that are beneficial to the Leviathan can be established and maintained, such as those relating to 'enemy threats' or those relating to the problematical dualism of 'security versus privacy' [568]. These can then have (or maintain) subjugating effects, as Foucault describes [337, p. 45]. The 'enemy' aspects of this interact with militaristic elements, as I now briefly describe.

Militarism and masculinity. As discussed in Chapter 4, military tropes are plentiful in both academic and mass-media communication relating to cyber security, e.g. [147, 238, 463, 504] and many metaphors of war were observed throughout the data. As I noted in that chapter, these references may be motivated by a desire for those who work in cyber security, most of whom are male [594], to cast themselves as heroic, a masculine trait that is strongly Hobbesian [286]. Cyber-security professionals may possess a distinctive and exceptional "power" that helps form their heroic identity, namely "knowledge" and "right method" [286, p. 642] which represents "the requisite special weapon of the epic hero" [286, p. 642], and, similar to Hobbes' self-conception as heroic, cyber-security professionals may be "proposing a solution to a predicament that [is] more masculine than human in tenor" [286, p. 643]. As established, Hobbes has been hugely influential in the field of IR [200], a discipline that, like cyber security [594] and commercial business [232], is male-dominated [473],[53] and suffers from associated biases [308, 386, 526, 603]. This aspect provides useful insights into the motivations behind key concepts,

[50] Cyber-security professionals "speak in... hieroglyphics or we speak in ... language that nobody else speaks in" (CISO5).

[51] Cf. "no you don't need to be worried about that, yes you do need to be worried about this" (CEO1).

[52] As indeed cyber-security language was characterised in the data. This also has resonance with what Foucault describes as "linguistic sufferings" [337, p. 100], whereby those who can not understand a language are not able to counter or challenge concepts expressed in that language.

[53] As well as being male-dominated, modern corporations are heavily bureaucratised (as has been established by many others, e.g. [549]), with hierarchical structures being predominant that feature inherent masculinity through militaristic associations [200].

particularly as "Western political thought" [286, p. 633] is similarly gender biased.

6.6 Summary

This study has shown that cyber-security practices within commercial businesses exist within a wider context that must be recognised in order to fully understand the role of the CISO. Hobbes may be far from being the only political philosophy of note or relevance, however, this chapter has shown that his work provides a useful lens through which to view the role that cyber security plays in society within and without businesses, particularly given the importance of Hobbesian thinking to Western politics and the enmeshed nature of states and corporations. Cyber security offers a useful mechanism from which the Leviathan derives benefit. It supports the establishment of fear and discipline, therefore, cementing power through obedience and conformance. Additionally, although less obviously, it also drives accumulation of capital through consumption of products and services, and job creation.

Businesses play a crucial role for the Leviathan. They employ and educate citizens, inuring them to surveillance and punishing them when they transgress. They maintain narratives of morality. They generate and expand capital. In some cases, they operate critical infrastructure and perform other state functions on the Leviathan's behalf. Businesses are themselves mini-Leviathans, and are in fear of threats to their existence. CISOs within those businesses provide a means by which they seek to avoid a state of nature. They also, indirectly, provide that function to the state, supporting its attempts to dominate competing state Leviathans. Actions taken by businesses in relation to cyber security involve spending that provides fuel for the continued growth of the Leviathan's power, and that of the hegemony that the Leviathan supports. These are significant factors that are crucial to consider when researching cyber security within commercial businesses. By bringing these aspects into conversation with the data from this study, and highlighting their relevance to cyber-security practice, I enable a (potentially hitherto unexplored) reflexive engagement for practitioners as well as provoking further academic application of political philosophy to cyber security.

Chapter 7

Conclusion

In this concluding chapter, I highlight and discuss the contributions made by this thesis. In so doing, I address the research objectives and underpinning research questions established in Chapter 1.

In this thesis I have explored cyber security in businesses from multiple viewpoints, providing a number of contributions that advance knowledge in multiple domains. Previous scholarship relating to cyber-security practice in businesses has predominantly employed singular analytical lenses, and, in many (but not all) cases, has a technology-centric focus. I have brought multiple literatures and theoretical viewpoints into conversation and, through these, applied a range of different analytical lenses to an exploration of the CISO's purpose. These lenses have been applied to a relatively broad range of in-depth empirical data, in contrast to many prior studies of CISOs and cyber security in organisations, which have been limited in their scope in terms of sample size and participant roles. Through this research, I have both addressed a gap and opened up new avenues for research, as I discuss further in Section 7.3. As well as these directions for future research, by identifying novel perspectives on cyber-security practice, both in relation to businesses and also wider society, I have enabled reflexivity for practitioners and offered practical considerations.

7.1 Contributions

This work demonstrates the value of using different sociological theories to achieve a deeper understanding of cyber-security practice, particularly the role of the CISO. By applying and interweaving these theories, it has introduced new critical perspectives on cyber security, as well as providing a reciprocal contribution that enriches those theories by bringing cyber security into conversation with them. This is important, as cyber-security practice within organisations is often explored from a single perspective that omits the wider social context in which those organisations operate. Similarly, sociological explorations of organisations have not previously considered how domains such as cyber security, and security more broadly, may influence organisational phenomena. Given the impact of cyber-security practices on individuals, whether intended or unintended, the conversation between multiple disciplines that has been achieved in this thesis also provides a foundation for future research that explores cyber-security practice in broader settings than solely organisations.

In Chapters 4, 5 and 6 I presented deep and wide-ranging findings that relate to the purpose of the CISO and the practice of cyber security in commercial organisations, both from the perspective of the CISO and of their senior stakeholders.[1] These empirics indicated theoretical concepts with which to explore and interpret the data, in contrast to other studies of cyber-security practice that have been led by psychological theory, such as that performed by Ashenden and Sasse [97], or management theory, such as Reinfelder et al. [623]. The directions suggested by the data led me to employ different analytical lenses in the findings chapters that followed, resulting in the contributions discussed in the following sections. The breadth of participants, both CISO and non-CISO, that were engaged in this study represents an additional contribution, as this is more extensive than many previous studies and provides viewpoints from senior business leaders on the role of the CISO that have previously been unexplored.

The work also provides a methodological contribution, in that it is a practitioner-led study, in contrast to previous research which has been performed by non-practitioners, as discussed in Chapter 2. An additional methodological contribution results from this research being grounded in an interpretive socio-organisational paradigm and the application of a sociological perspective to cyber security within organisations, as called for by previous researchers. It also provides a further body of work that supports such an approach. This is in contrast to technology-centric approaches, which dominate in the cyber-security domain.

I conclude the thesis here by summarising the theoretical contributions that this thesis makes.

7.1.1 Contributions relating to theories of identity

The moral associations of cyber security identified in this study are also significant. Combined with the recondite and even metaphysical associations of cyber security, the indexation of morality illustrates that there is considerable power available to those

[1] With further methodological findings presented in Appendix A. The latter have not been explored in detail in this thesis as these aspects did not align to the research question.

involved with cyber security, whether practitioners or others who benefit from the existence of an inexhaustible well of opaque and malicious threats. This includes hegemonic, as well as commercial, interests.

In addition, the concepts applied in Chapter 4, that is, identity work, ontological security and morality, allow the exploration of the identity of CISOs themselves, which is conflicted and contradictory. CISOs are expected to perform multiple roles, and are at once precarious and necessary, scapegoat and totem. I proposed that one of their roles is akin to being a soothsayer, building on the moral and mystical associations of cyber security to suggest that the CISO is an interpreter and judge of fearful and arcane threats and uncertain signs, a protective and yet somewhat disquieting figure. The soothsayer metaphor enables a more thorough explanation of the purpose of the CISO and helps to articulate the complex and even paradoxical role that CISOs play. This is a contribution that not only illuminates a misunderstood and under-explored role but also contextualises cyber-security practice in businesses more broadly, highlighting its perceived opacity.

7.1.2 Contributions relating to risk management

Identity and ontological security are associated with uncertainty. In Chapter 5, I developed this thread of uncertainty further by applying normative concepts of risk management and governance to the interpretation of the data. I identified that the CISO represents an attempt by businesses to control uncertainty arising from cyber security, who are fearful of the impact that future cyber-security incidents may have on the continued viability of their business. The management of this uncertainty is considered by businesses to be an obligation, who cascade associated aspects of duty throughout their organisations. Identifying these aspects of duty led to the consideration of recreancy. Through the application of this concept, I suggest that one purpose of a CISO is to identify and respond to recreant behaviour within a business. This also indicates that the CISO role is a manifestation of the perceived, and normative, need for control within a business. The CISO's purpose appears to be one of both controlling cyber-security risks and, as per Chapter 4, to signify that those risks are being controlled.

Chapter 5 also highlighted the desire from businesses for objective measurement of cyber-security risk, driven by a normative positivistic philosophy. A key contribution here is that such a philosophy results in the disregarding and deprioritisation of the social and emotional factors that constitute cyber-security risk, which may result in an increased likelihood of such risks occurring. As with Chapter 6, the consequences of this extend beyond individual businesses and their CISOs.

I also applied Beck's concept of *Nichtwissen* to suggest that CISOs may unwittingly engender cyber-*Nichtwissen*, where the provision of knowledge to employees regarding cyber-security risks has an unintended counter-productive consequence of increasing their uncertainty and disconnection from those risks. This represents one of multiple paradoxes relating to the role of the CISO that have been identified through this research and which indicate the complex nature of their practice. In discussing these paradoxes, I have achieved a more comprehensive portrait of the CISO than has previously been achieved, as shown in Chapter 2. This is of value both to CISOs and their employers, as it enables a greater appreciation of intended purpose and unintended consequences from each perspective. Further, it is of value to the broader cyber-security industry and other associated actors in allowing greater reflection on the perceived purpose of the CISO in cyber-security risk management and uncertainty reduction. This is also of relevance across wider society.

7.1.3 Contributions relating to cyber security in wider contexts

Societal aspects of cyber security were explored in more detail in Chapter 6 which applied the work of Thomas Hobbes to the interpretation of the data in a discussion of cyber security in broader societal and state identity contexts. This identified that cyber-security practices within businesses present a number of benefits to the state and broader hegemony, including the normalisation of intrusive controls, as well as increased consumption. These aspects may not be intentional, however, there is a particularly important contribution made in enabling reflexivity for practitioners regarding the role that they play, highlighting perhaps unintended consequences. Cyber-security practice employs, and relies upon, fear and discipline, which, as with the Leviathan, cements power through obedience and conformance.

Cyber security represents survival-level threats that are feared by both states and businesses. For the latter, a CISO offers a means to avoid a state of nature, arising from a feared cyber war of all against all. For a state, CISOs provide a mechanism through which it can indirectly avoid such threats to its own survival, maintaining its power and ensuring continued growth. The use of Hobbes in Chapter 6 provides a valuable perspective on the context that the CISO operates within, and, in particular, offers great opportunity for reflexivity, as I describe further in the following section. By bringing concepts from IR into conversation with the data from this study, and highlighting their relevance to cyber-security practice, I have enabled a (to my knowledge, hitherto unexplored) reflexive engagement for practitioners as well as provoking further academic application of political philosophy to cyber-security practice.

The theoretical contributions that this thesis makes are motivators of further contributions relating to reflexivity, which I now discuss.

7.1.4 Reflections and reflexivity

A practical contribution of this research is the encouragement of greater reflexivity within the field of cyber security, for businesses, researchers, and for practitioners. In this section, I first describe my own reflections on this research as a practitioner and how they have subsequently affected my practice. I then discuss the contribution that the study makes in motivating reflexivity for others.

As a practicing CISO, the findings of this research are now a factor in my practice. This includes my staff development activities, which now include active discussion and engagement with the soothsayer construct described in Chapter 4. This identity, as soothsayer, is something that I have subsequently spent considerable time reflecting on, particularly in relation to the potentially negative associations of the term. For example, while I do not consider it to be denigratory, as described in in Chapter 4, others, including my professional stakeholders, could see it as such. In the positivistic environment of a modern business, as described in Chapter 5, a 'non-scientific' identity as a soothsayer may be seen as unimportant, even trivial. Although the activity of interpreting and forecasting risk may be considered valuable, the labelling of the activity as soothsaying may be suboptimal, despite its appositeness. This is something that I need to further reflect on, from a professional standpoint, including considering whether alternative phrasing would be beneficial. My staff development approach also now reflects on the paradoxes described in Chapter 5 and how these affect cyber-security practice, as well as on the use of fear in cyber-security discourse and how this may inadvertently undermine the outcomes that we wish to achieve.

The research has also motivated me to consider (and articulate) the importance of cyber-security practice in maintaining, and indeed establishing, organisational identity. This has enabled a clearer positioning of the value of the cyber-security function both to my stakeholders and to the cyber-security team itself. I have also reflected on whether the potential conflict between an intrinsic versus instrumentally valuable perspective on cyber-security practice within an organisation is a concern for my own professional practice. On one hand, I do not consider an instrumentally valuable perspective to be unreasonable, as a utilitarian aspect to all business functions, and indeed to all salaried roles, appears logical. Yet, on the other hand, I do regard cyber-security risk management as being fundamental to the successful operation of a modern business. At the risk of conjecture, my professional experience indicates that certain capabilities within a commercial business are considered to be more essential than cyber security. Therefore, reflecting on these perspectives, and opinions, and whether they affect my professional practice, has been a valuable result of this research.

A further important reflection has been in relation to the inherent masculinity associated with cyber-security practice. As well as being an area for my own future research to explore, as I explain in Section 7.3, this is an important perspective that I am highlighting with my staff, and stakeholders. I consider it to be incumbent on me as a cyber-security leader to highlight these factors and associated biases, and encourage other practitioners that I work with (and develop) to engage with and challenge the apparent masculine orthodoxy in cyber security. In particular, I am encouraging the use of different language and concepts where possible.

Finally, I have reflected on the role that I, as a CISO, inadvertently play in broader societal power structures, both political and commercial. Such reflections again now feature in staff development, whereby my employees are made aware of, and encouraged to engage with, the complex and enmeshed nature of our roles with the societies in which we participate. As I now discuss in more detail, such reflections are of value for others and are an important contribution of this research.

Motivation of reflexivity for others

Businesses themselves may benefit from reflecting on the role that they play in supporting the state Leviathan, and indeed in wider globalisation of Hobbesian models of control. Such reflexivity and improved recognition of broader contexts offers empowerment for individuals within those businesses, particularly CISOs. Part of the role of a CISO is being the agent of two Leviathans, the mini-Leviathan of the business that employs them and the larger Leviathan of the state. The latter role may not be as immediately obvious or recognisable and may be uncomfortable for many CISOs. However, recognising this allows for reflexive consideration and engagement with the implications, or at the very least an acknowledgement of what individual CISOs do or do not agree with. CISOs may acknowledge that there is value in implementing surveillance in order to protect the business-as-Leviathan but if that helps to normalise surveillance by the state Leviathan of the employee-citizen, there may be a potential internal conflict that they need to either resolve or come to terms with. I have considered whether this perspective could potentially lead to (perceived) negative outcomes for the cyber-security industry. For example, will there be less surveillance within organisations as a result of CISOs resisting the support that they indirectly provide to state surveillance? I consider this to be unlikely, however, it opens up further avenues of potential research, particularly to explore whether or not a CISO's primary focus is on their employer. After all, their employer is offering them the most immediate protection in terms of salary and continued employment and, similar to the Hobbesian family structure, is where their primary interest and indeed obedience may lie.[2] Therefore, the CISO may do what is in the interest of their employer and ensure that they protect them as best they can, including implementing controls that they would feel less comfortable with if they were in place in wider society. Their employer's interests may also be more closely aligned with their own, particularly in terms of ensuring continued viability, than with the state Leviathan's, and this symbiotic relationship may be an important factor in any decision-making regarding controls.

A further contribution arising from the reflexivity this research enables for others is in relation to the identities that CISOs occupy, and that are assigned to them. CISOs and their stakeholders can be motivated through this research to consider the implications of these identities and how they affect their relationships, and indeed their approaches to cyber security. As with my own reflections above, other CISOs can derive benefit from reflecting upon the messages they communicate to their stakeholders and whether the language that they use inadvertently subverts the achievement of their goals.

My overarching research objective was to understand the purpose of a CISO in commercial organisations. This purpose appears to be multiple, and fragmented. It exists to advise and educate, to interpret and caution, to protect and to signify protection. At the same time, it supports and maintains power through normalisation and conditioning of staff, through repetition and maintenance of narratives of fear and emergency, and through consumption. While these may not be deliberate, intentional aspects of purpose from the CISO's, or even the organisation's, perspectives, they are outcomes that can be seen as potentially purpose-driven from the view of hegemony. Hegemony is not an individual actor, with a singular identity. Rather, it is a representation of a multiplicity of interests that are aligned with maintenance and growth of power. I argue that the CISO is an element, albeit unwitting, in these power structures, an argument that may be uncomfortable for many CISOs, and other cyber-security practitioners. However, by identifying, acknowledging and reflecting on perspectives such as these, both practice and scholarship can advance.

7.2 Limitations

Due to difficulties with access, as described in Chapter 3, the level of involvement from senior leaders in this study was limited. There was also no representation from

[2] This is no different to other employees, and the workplace can be considered to be a site of conflicting interests for all within it. However, the CISO role may be unique in both its apparent precarity and the part it plays in determining and implementing controls that affect other staff, and indeed themselves.

other organisational stakeholders, including those that reported into the CISO and their peers. I did not achieve as broad a sample as I had originally hoped, and the occurrence of the Covid-19 pandemic partway through data collection affected both sampling and interviewing mode, as well as potentially affecting participant responses in different yet unclear ways.

While a range of different industries were investigated, there was an inadvertent weighting towards one sector in particular. A study that features greater diversity of industries may result in different findings. A further limitation is the lack of demographic diversity in the sample, which may have influenced the findings, although, as discussed in Chapter 3, this is representative of the business environment in the UK. In addition, this research explored cyber security in businesses that were based in the UK, and that had a major stock market listing. Different findings may result from a study of non-UK based businesses, those that are not listed companies, and those that are not commercial organisations, such as charities. The relative size of company may also be an important factor.

The solely Western, and Global Northern, perspectives of the participants and the businesses studied are likely to have influenced the findings, and, therefore, a similar study in different geographies may have different results, with the perceived purpose of the CISO being different. Equally, my choice of analytical lenses and how I have employed them will have been influenced by my geographic and cultural context, and my positionality. These were selected due to multiple resonances in the data identified during my analysis and were the means through which my contributions have been achieved. Other analytical lenses could have been deployed, and different avenues explored, and choices taken, when reviewing literature. Another researcher may, therefore, have reached different conclusions. However, I have made my decisions explicit throughout, so that the underpinning of my interpretation is clear.

These limitations do not detract from the contributions that this thesis has made, and the significance of its findings. They do not invalidate the work in any way, and simply reflect the conditions under which this research was conducted and constructed. They do, however, suggest other useful research directions to build on this work, which I explore in the following section.

7.3 Future work

In addition to addressing, albeit not definitively answering, the research questions that I originally defined, this thesis has generated further questions which suggest interesting future research directions.

First, to address the limitations identified above, similar studies could be performed on different types of businesses, with more diverse samples, and in different geographic locations. Such studies should also obtain perspectives from the CISO's other stakeholders.

This thesis has brought many diverse disciplines into conversation, and many of these, including IR, sociology and criminology, could be extended further to provide insights beyond those that I have achieved and derive greater insight into cyber-security practice. Other analytical lenses from these, or other, disciplines could also be employed, opening up further multi-disciplinary research opportunities for studies on the role and purpose of the CISO.

The Hobbesian perspective that I introduced in Chapter 6 may encourage the application of broader contexts from IR and political philosophy, using other theorists and perspectives to explore cyber security within businesses and wider society, with geographic and cultural relevancy being particularly important to consider. This could include more modern political philosophies, including those that are contrary to, or antagonistic towards, Hobbes. An integration of different political philosophies could be of particular value, where these viewpoints are brought into conversation with regard to cyber-security practice in business, and in wider society.[3] In particular, I consider there to be benefit to research avenues relating to the context of businesses within globalisation and geopolitics, including the establishment of cyber norms and other developing areas of study. The use of Hobbes as an analytical lens may be extended to other areas of business, particularly with regard to explorations of power and the context of business in wider society.

Future research could also consider the possibility of 'deviant' corporations and the concept of insider threats through a Hobbesian lens.[4] The latter, in particular, could also be expanded to consider the perspective of resistance.[5] Further, there may be an interesting parallel to explore with regard to biological threats, such as Covid-19, and cyber threats. Each of these can be considered as unseen, ephemeral threats that require specialist advisors and motivate restrictive controls that could be considered as offering additional benefits to a Hobbesian state.[6]

The masculinity inherent in cyber-security practice, as identified in this research, also provides a rich vein of future work. Indeed, this has been an area that I have explored in more detail during this study that is not included in this thesis for reasons

[3] Foucault's work, as partially employed in this thesis, could also be a useful lens to deploy more fully to aspects of cyber security, beyond the aspects of discipline and power I have considered, which could include aspects of discourse and knowledge construction.

[4] I thank one of the anonymous reviewers of [259] for these suggestions.

[5] This has potential parallels with prior work performed by Coles-Kemp et al. [224].

[6] Again, I thank one of the anonymous reviewers of [259] for inspiring this angle.

of space but which I intend to develop further in other venues.

Another research direction is to consider whether there are other organisational roles that experience conflicted identities and organisational othering. There may also be value in identifying whether the lens of soothsaying can be applied to other roles, and whether other business practices feature moralistic associations. For example, do those who work in fraud prevention conceive of themselves as 'doing right'? Value theory, and other aspects of moral philosophy, may be particularly useful lenses to apply in this regard. One specific question that could be explored here is 'doing right for whom?'. Another perspective to explore is whether a lens of ontological security can be applied elsewhere in businesses, and whether the experiences of the CISOs in this study with regard to a perceived challenge to their ontological security are experienced by those in more established or more well-understood roles.

Building on the totemic aspects of the CISO that were identified, other semiotic perspectives in relation to security and organisational identity may be worth exploring. Similarly, other semiotic aspects of the roles that businesses play in creating and maintaining state identities could also be interesting.

Finally, the lens of recreancy, as identified in Chapter 5, may provide a useful perspective for future studies of businesses, including areas of risk management unrelated to cyber security and other aspects of organisational governance. Aspects of punishment associated with recreancy could also be a worthwhile topic, including whether potential retribution such as clawbacks of bonuses have indeed been enacted in relation to cyber-security incidents, and what effects these have had.

Bibliography

[1] Bank of England — Prudential Regulation Authority — Policy — Prudential Regulation Authority Handbook & Rulebook. http://www.prarulebook.co.uk/. 30

[2] Bank of England Prudential Regulatory Authority PS13/16 Corporate governance: Board responsibilities. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2016/ps1316.pdf. 27, 71

[3] Code of Ethics — Complaint Procedures — Committee Members. https://www.isc2.org/Ethics. 175

[4] Companies Act 2006. https://www.legislation.gov.uk/ukpga/2006/46. 26, 90, 142

[5] Companies and Securities - London Stock Exchange. https://www.londonstockexchange.com/statistics/companies-and-issuers/companies-and-issuers.htm. 119

[6] The Companies (Miscellaneous Reporting) Regulations 2018. https://www.legislation.gov.uk/uksi/2018/860/contents/made. 27

[7] Cyber Governance Health Check 2018. https://www.gov.uk/government/publications/cyber-governance-health-check-2018. 30, 42

[8] Cybersecurity and IT Security Certifications and Training — (ISC)^2. https://www.isc2.org:443/. 111

[9] Cybersecurity Certification and Training — (ISC)^2. https://www.isc2.org:443/About. 180

[10] Cybersecurity Poised for Consolidation. https://www.morganstanley.com/ideas/cybersecurity-needs-new-paradigm. 176

[11] Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes. https://investor.equifax.com/news-events/press-releases/detail/237/equifax-releases-details-on-cybersecurity-incident. 58, 180, 182

[12] FCA Handbook - FCA Handbook. https://www.handbook.fca.org.uk/handbook. 30, 65, 66

[13] Financial Services and Markets Act 2000. https://www.legislation.gov.uk/ukpga/2000/8/contents. 27, 71

[14] FTSE 350 Cyber Governance Health Check 2018. 30

[15] Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019. 176

[16] Hobbes's Leviathan. https://www.bl.uk/collection-items/hobbess-leviathan. 216

[17] *ISO/IEC 27000 - Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary*. BSI. 21

[18] IT Governance - IT Certification - Serving IT Professionals — ISACA. https://www.isaca.org/About-ISACA/What-We-Offer-Whom-We-Serve/Pages/default.aspx. 53, 111, 160, 180

[19] Jail data abusers says Culture, Media and Sport Committee report - News from Parliament. https://old.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/news-parliament-2015/cyber-security-report-published-16-17/. 60

[20] Moralist, n. In *OED Online*. Oxford University Press. 175

[21] Progress of the 2016-2021 National Cyber Security Programme - National Audit Office (NAO) Report. https://www.nao.org.uk/report/progress-of-the-2016-2021-national-cyber-security-programme/. 42, 178

[22] Qualitative Data Analysis Software — NVivo. https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home. 112

[23] The reach of the UK Corporate Governance Code. https://www.out-law.com/page-8214. 66

[24] Recreant, adj. and n. In *OED Online*. Oxford University Press. 70

[25] Red Team Definition from Financial Times Lexicon. http://lexicon.ft.com/term?term=red-team. 55

[26] Risk, n. In *OED Online*. Oxford University Press. 62

[27] Schedule an Email Security Demo — Mimecast Ad. https://bigdatr.com/au/ad/ac2349467707. 176

[28] The Smart Energy Code - SEC. https://smartenergycodecompany.co.uk/the-smart-energy-code-2/. 27

[29] Style Matters: Ethnicity, race, and culture: Guidelines for research, audit, and publication — The BMJ. https://www.bmj.com/content/312/7038/1094.full. 98

[30] Talk Talk boss Dido Harding's utter ignorance is a lesson to us all. https://www.campaignlive.co.uk/article/talk-talk-boss-dido-hardings-utter-ignorance-lesson-us/1370062?utm_source=website&utm_medium=social. 110

[31] TalkTalk CISO given carte blanche over security investments. https://www.totaltele.com/492027/TalkTalk-CISO-given-carte-blanche-over-security-investments. 176

[32] Theft of Customer Data at British Airways. https://www.iairgroup.com/en/newsroom/press-releases/newsroom-listing/2018/06-09-2018-153747680. 57, 141

[33] Three random words or #thinkrandom - NCSC. https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0. 118

[34] Varonis. https://www.bluetext.com/varonis/. 176

[35] Viability, n.1. In *OED Online*. Oxford University Press. 65

[36] Virtuous, adj. and n. In *OED Online*. Oxford University Press. 175

[37] Powell: The U.S. Is 'Running Out Of Demons'. *The Seattle TImes*, Apr. 1991. 56, 179

[38] USA PATRIOT Act 2001, Oct. 2001. 220

[39] We have lift-off. *The Economist*, pages 91+, Feb. 2001. 65

[40] Controlled functions. https://www.fca.org.uk/firms/approved-persons/controlled-functions, Aug. 2015. 27

[41] TalkTalk cyber-attack: Website hit by 'significant' breach. *BBC News*, Oct. 2015. 47

[42] TalkTalk head of security: What we learned from the cyber attack. https://www.cbronline.com/business/talktalk-head-of-security-what-we-learned-from-the-cyber-attack-4886225/, May 2016. 29

[43] *ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT SYSTEMS REQUIREMENTS.* BSI, S.l., 2017. 31

[44] *ISO/IEC 27002 CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS.* BSI, S.l., 2017. 21

[45] Massive cyber-attack could cost Nurofen and Durex maker £100m. http://www.theguardian.com/business/2017/jul/06/cyber-attack-nurofen-durex-reckitt-benckiser-petya-ransomware, July 2017. 68

[46] Senior Managers and Certification Regime: Banking. https://www.fca.org.uk/firms/senior-managers-certification-regime/banking, July 2017. 27, 71

[47] British Airways boss apologises for 'malicious' data breach. *BBC News*, Sept. 2018. 47

[48] Industry Classification Benchmark (ICB). https://www.ftserussell.com/data/industry-classification-benchmark-icb, June 2018. 89, 119

[49] Major cyber-attack on UK a matter of 'when, not if' – security chief. *The Guardian*, Jan. 2018. 68

[50] Marriott Announces Starwood Guest Reservation Database Security Incident. https://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/, Nov. 2018. 57, 141

[51] This Billboard 'Powered' by Hackers Highlights the Danger of Cyber Crime. https://adage.com/creativity/work/honeypot-poster/53905, Feb. 2018. 176

[52] Data hacks and big fines drive cyber insurance growth. *Financial Times*, Nov. 2019. 68

[53] Google, Apple criticise GCHQ snooping tech. *BBC News*, May 2019. 228

[54] List of national capitals. *Wikipedia*, July 2019. 119

[55] Trump administration escalates cyber-attacks on Russia as warning to Putin. *The Independent*, June 2019. 42, 180

[56] Apple launches new privacy ad ahead of iPhone 12 launch. https://www.independent.co.uk/life-style/gadgets-and-tech/news/apple-iphone-12-release-date-privacy-ad-facebook-security-campaign-a9703246.html, Sept. 2020. 58

[57] Did a Chinese Hack Kill Canada's Greatest Tech Company? *Bloomberg.com*, July 2020. 72

[58] Financial Stability Report July 2021. Technical report, Bank of England, 2021. 30

[59] Unit 8200. *Wikipedia*, July 2021. 58

[60] Enforcement action. https://ico.org.uk/action-weve-taken/enforcement/, Jan. 2022. 224

[61] ICO fines British Airways £20m for data breach affecting more than 400,000 customers. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/, Jan. 2022. 224

[62] G. Abels and M. Behrens. Interviewing experts in political science: A reflection on gender and policy effects based on secondary analysis. In A. Bogner, B. Littig, and W. Menz, editors, *Interviewing Experts*, pages 138–156. Springer, 2009. 97

[63] J. D. Aberbach and B. A. Rockman. Conducting and Coding Elite Interviews. *PS: Political Science & Politics*, 35(4):673–676, Dec. 2002. 113

[64] R. Abratt and N. Kleyn. Corporate identity, corporate branding and corporate reputations: Reconciliation and integration. *European Journal of Marketing*, 46(7/8):1048–1063, July 2012. 45, 46, 139

[65] A. Abu-Musa. Information security governance in Saudi organizations: An empirical study. *Information Management & Computer Security*, 18(4):226–276, Oct. 2010. 19

[66] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, Dec. 1999. 22, 197

[67] D. Adams. *Life, the Universe and Everything*. Pan Books, 1982. 71, 199

[68] J. Adams. *Risk*. UCL Press, 1995. 67, 72, 73, 193, 209

[69] J. O. Adekunle. On Oral Tradition and History. Studies on Nigerian Borgu. *Anthropos*, 89(4/6):543–551, 1994. 180

[70] G. Adkins. Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism. *Journal of Strategic Security*, 6(Extra):1–9, Aug. 2013. 180

[71] P. A. Adler and P. Adler. Stability and Flexibility: Maintaining Relations Within Organized and Unorganized Groups. In W. Shaffir and R. A. Stebbins, editors, *Experiencing Fieldwork: An inside View of Qualitative Research*, pages 173–183. Sage Publications, Newbury Park, Calif., 1991. 93

[72] R. Adolphs. The Biology of Fear. *Current Biology*, 23(2):R79–R93, Jan. 2013. 39, 68, 136

[73] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 0(0):15, 2018. 77

[74] L. A. Aguilar. SEC.gov — Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus. https://www.sec.gov/news/speech/2014-spch061014laa. 30

[75] S. Ahuja, H. Heizmann, and S. Clegg. Emotions and identity work: Emotions as discursive resources in the constitution of junior professionals' identities. *Human Relations*, 72(5):988–1009, May 2019. 48, 49, 136, 175, 184

[76] S. Ainsworth and C. Hardy. Critical discourse analysis and identity: Why bother? *Critical Discourse Studies*, 1(2):225–259, Oct. 2004. 54

[77] A. Aissa, R. Abercrombie, F. Sheldon, and A. Mili. Defining and computing a value based cyber-security measure. *Information Systems & e-Business Management*, 10(4):433–453, Dec. 2012. 201

[78] S. Akbar, B. Kharabsheh, J. Poletti-Hughes, and S. Z. A. Shah. Board structure and corporate risk taking in the UK financial sector. *International Review of Financial Analysis*, 50:101–110, Mar. 2017. 25, 29

[79] E. Albrechtsen. A qualitative study of users' view on information security. *Computers & Security*, 26(4):276–289, June 2007. 71, 206

[80] B. A. Allan, K. L. Autin, and R. D. Duffy. Self-Determination and Meaningful Work: Exploring Socioeconomic Constraints. *Frontiers in Psychology*, 7, 2016. 99

[81] A. Alojairi. The Dynamics of IT Workaround Practices - A Theoretical Concept and an Empirical Assessment. *International Journal of Advanced Computer Science and Applications*, 8(7), 2017. 73

[82] S. Alvarez, A. Afuah, and C. Gibson. Editors' Comments: Should Management Theories Take Uncertainty Seriously? *Academy of Management Review*, 43(2):169–172, Apr. 2018. 63

[83] M. Alvesson. Beyond Neopositivists, Romantics, and Localists: A Reflexive Approach to Interviews in Organizational Research. *The Academy of Management Review*, 28(1):13–33, 2003. 113

[84] M. Alvesson and L. Empson. The construction of organizational identity: Comparative case studies of consulting firms. *Scandinavian Journal of Management*, 24(1):1–16, Mar. 2008. 45

[85] M. Alvesson and D. Kärreman. Taking the Linguistic Turn in Organizational Research: Challenges, Responses, Consequences. *The Journal of Applied Behavioral Science*, 36(2):136–158, June 2000. 35

[86] M. Alvesson and H. Willmott. Identity Regulation as Organizational Control: Producing the Appropriate Individual. *Journal of Management Studies*, 39(5):619–644, 2002. 59, 144

[87] J. Amernic and R. Craig. CEO speeches and safety culture: British Petroleum before the Deepwater Horizon disaster. *Critical Perspectives on Accounting*, 47:61–80, Sept. 2017. 30, 46

[88] A. Anderson. *Media, Culture and the Environment*. Routledge, 2013. 67

[89] M. Anteby. Identity Incentives as an Engaging Form of Control: Revisiting Leniencies in an Aeronautic Plant. *Organization Science*, 19(2):202–220, 2008. 60, 179

[90] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69:437–443, Apr. 2017. 23

[91] K. A. Appiah. *Cosmopolitanism Ethics in a World of Strangers.* Allen Lane, London, 2006. 49

[92] M. S. Archer. *The Reflexive Imperative in Late Modernity.* Cambridge University Press, 2012. 96, 97, 99, 100, 101

[93] H. Arendt. *Between Past and Future.* Penguin Publishing Group, 2006. 221, 227

[94] H. Arendt. *The Origins of Totalitarianism.* Penguin Books Limited, 2017 (1951). 179, 213, 216, 217, 218, 226, 227, 228, 229, 230

[95] D. Ashenden and D. Lawrence. Can we sell security like soap? a new approach to behaviour change. In *Proceedings of the 2013 New Security Paradigms Workshop*, NSPW '13, pages 87–94, New York, NY, USA, Sept. 2013. Association for Computing Machinery. 22

[96] D. Ashenden and D. Lawrence. Security Dialogues: Building Better Relationships between Security and Business. *IEEE Security & Privacy*, 14(3):82–87, May 2016. 19, 20, 186

[97] D. Ashenden and A. Sasse. CISOs and organisational culture: Their own worst enemy? *Computers & Security*, 39:396–405, Nov. 2013. 14, 15, 16, 19, 20, 94, 101, 102, 182, 186, 239

[98] B. E. Ashforth, S. H. Harrison, and K. G. Corley. Identification in Organizations: An Examination of Four Fundamental Questions. *Journal of Management*, 34(3):325–374, June 2008. 64

[99] P. J. Aspinall. Department of Health's requirement for mandatory collection of data on ethnic group of inpatients. *BMJ*, 311(7011):1006–1009, Oct. 1995. 98

[100] S. Aurigemma and T. Mattson. Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. *Computers & Security*, 73:219–234, Mar. 2018. 22

[101] J. L. Austin. *How to Do Things with Words.* Clarendon Press, 1975. 51

[102] J. L. Austin. *How to Do Things with Words.* Oxford : Oxford University Press, Oxford, 2nd ed., edited by j. o. urmson and marina sbisà. edition, 1976. 110

[103] M. Bada, A. M. Sasse, and J. R. C. Nurse. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *arXiv:1901.02672 [cs]*, Jan. 2019. 70

[104] K. Baier. *The Moral Point of View: A Rational Basis of Ethics*, volume 35. Cornell University Press, 1958. 167, 206

[105] D. A. Baldwin. The Concept of Security. *Review of International Studies*, 23(1):5–26, 1997. 33, 34

[106] P. Balozian and D. Leidner. Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory. *SIGMIS Database*, 48(3):11–43, Aug. 2017. 31

[107] D. Bambauer. Conundrum. *Minnesota Law Review*, 96(2):584–674, 2011. 34

[108] S. B. Banerjee. Decolonizing Management Theory: A Critical Perspective. *Journal of Management Studies*, 59(4), 2021. 66

[109] J. Barkan. Roberto Esposito's Political Biology and Corporate Forms of Life. *Law, Culture and the Humanities*, 8(1):84–101, Feb. 2012. 217, 218, 223, 228

[110] J. Barkan. *Corporate Sovereignty: Law and Government under Capitalism.* University of Minnesota Press, 2013. 227, 228

[111] J. B. Barlow, M. Warkentin, D. Ormond, and A. R. Dennis. Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, 39:145–159, Nov. 2013. 23

[112] J. Baron. The effect of normative beliefs on anticipated emotions. *Journal of Personality and Social Psychology*, 63(2):320–330, Aug. 1992. 70, 72

[113] J. Baron, J. C. Hershey, and H. Kunreuther. Determinants of Priority for Risk Reduction: The Role of Worry. *Risk Analysis*, 20(4):413–428, 2000. 66, 70, 136

[114] D. Barr-Pulliam, P. Nkansa, and K. Walker. From Compliance to Strategy: Using the Three Lines of Defense Model to Evaluate and Motivate Internal Audit Contributions to Accounting Research. Technical report, Working paper, University of Wisconsin–Madison, California State University, 2017. 28

[115] R. Baskerville, P. Spagnoletti, and J. Kim. Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, 51(1):138–151, Jan. 2014. 36, 37

[116] J. Baudrillard. *The Consumer Society : Myths and Structures.* London : Sage, London, 1998. 40, 44, 45, 52, 53, 62, 137, 179, 183, 231, 232, 234

[117] Z. Bauman, D. Bigo, P. Esteves, E. Guild, V. Jabri, D. Lyon, and R. B. J. Walker. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, 8(2):121–144, June 2014. 44, 229

[118] D. Baumgold. “Trust” in Hobbes's Political Thought. *Political Theory*, 41(6):838–855, Dec. 2013. 217

[119] J. Baxter and J. Eyles. Evaluating Qualitative Research in Social Geography: Establishing 'Rigour' in Interview Analysis. *Transactions of the Institute of British Geographers*, 22(4):505–525, Dec. 1997. 113

[120] M. S. Beasley, J. V. Carcello, D. R. Hermanson, and T. L. Neal. The Audit Committee Oversight Process. *Contemporary Accounting Research*, 26(1):65–122, 2009. 25, 26

[121] A. Beautement, I. Becker, S. Parkin, K. Krol, and M. A. Sasse. Productive Security: A scalable methodology for analysing employee security behaviours. In *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, page 19, 2016. 20, 186

[122] U. Beck. *Risk Society : Towards a New Modernity.* Sage, Los Angeles, [Calif.], 1992. 44, 62, 71, 194

[123] U. Beck. *World at Risk.* Polity Press, 2009. 22, 44, 62, 66, 67, 68, 71, 76, 78, 108, 190, 194, 198, 200, 202, 205, 210, 220

[124] N. Beech. On the Nature of Dialogic Identity Work. *Organization*, 15(1):51–74, Jan. 2008. 38, 48, 49, 50, 55, 59, 60, 144, 145, 166, 229

[125] N. Beech, C. Gilmore, P. Hibbert, and S. Ybema. Identity-in-the-work and musicians' struggles: The production of self-questioning identity work. *Work, Employment & Society*, 30(3):506–522, 2016. 47

[126] S. Beer. *The Heart of the Enterprise.* Wiley, 1979. 65, 222

[127] S. Beer. The Viable System Model: Its Provenance, Development, Methodology and Pathology. *The Journal of the Operational Research Society*, 35(1):7–25, 1984. 65

[128] T. M. Bejan. Teaching the Leviathan: Thomas Hobbes on education. *Oxford Review of Education*, 36(5):607–626, Oct. 2010. 197, 217, 219, 221, 224, 225

[129] B. Benwell and E. Stokoe. *Discourse and Identity*. Edinburgh: Edinburgh University Press, Edinburgh, 2006. 37, 49, 50, 54, 59, 144, 146, 161, 177, 178, 179, 225, 228, 234, 236

[130] F. Berenskoetter. Reclaiming the Vision Thing: Constructivists as Students of the Future. *International Studies Quarterly*, 55(3):647–668, 2011. 42

[131] N. Berg, S. Prakhya, and K. Ranganathan. A satisficing approach to eliciting risk preferences. *Journal of Business Research*, 82:127–140, Jan. 2018. 74

[132] P. L. Berger and T. Luckmann. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. Penguin Books, 1972 (1966). 82

[133] H. Berghoff. "Organised irresponsibility"? The Siemens corruption scandal of the 1990s and 2000s. *Business History*, 60(3):423–445, Apr. 2018. 73, 136

[134] E. Berne. *Transactional Analysis in Psychotherapy : A Systematic Individual and Social Psychiatry*. New York : Grove, New York, 1975. 20

[135] P. L. Bernstein. *Against the Gods: The Remarkable Story of Risk*. Wiley, 1998. 190

[136] M. D. Berzonsky. A Social-Cognitive Perspective on Identity Construction. In S. J. Schwartz, K. Luyckx, and V. L. Vignoles, editors, *Handbook of Identity Theory and Research*. Springer New York, New York, NY, UNITED STATES, 2011. 45, 46

[137] D. J. Betz and T. Stevens. Analogical reasoning and cyber security. *Security Dialogue*, 44(2):147–164, Apr. 2013. 36, 39

[138] D. Bigo. International flows, political order and social change: (in)security, by-product of the will of order over change. *Global Crime*, 18(3):303–321, July 2017. 41

[139] S. Biko. Black Consciousness & the Quest for a True Humanity. *Ufahamu: A Journal of African Studies*, 11(1), 1981. 229

[140] N. Blaikie. Confounding issues related to determining sample size in qualitative research. *International Journal of Social Research Methodology*, 21(5):635–641, Sept. 2018. 93

[141] N. E. Blankenstein, E. Schreuders, J. S. Peper, E. A. Crone, and A. C. K. van Duijvenvoorde. Individual differences in risk-taking tendencies modulate the neural processing of risky and ambiguous decision-making in adolescence. *NeuroImage*, 172:663–673, May 2018. 62

[142] C. R. Boddy. Sample size for qualitative research. *Qualitative Market Research: An International Journal*, 19(4):426–432, Jan. 2016. 93

[143] G. Boella, G. Governatori, A. Rotolo, and L. van der Torre. Lex Minus Dixit Quam Voluit, Lex MagisDixit Quam Voluit: A Formal Study on Legal Compliance and Interpretation. In P. Casanovas, U. Pagallo, G. Sartor, and G. Ajani, editors, *AI Approaches to the Complexity of Legal Systems. Complex Systems, the Semantic Web, Ontologies, Argumentation, and Dialogue*, Lecture Notes in Computer Science, pages 162–183, Berlin, Heidelberg, 2010. Springer. 84

[144] G. Boella, M. Janssen, J. Hulstijn, L. Humphreys, and L. van der Torre. Managing Legal Interpretation in Regulatory Compliance. In *Proceedings of the Fourteenth International Conference on Artificial Intelligence and Law*, ICAIL '13, pages 23–32, New York, NY, USA, 2013. ACM. 84

[145] A. Bogain. Security in the name of human rights: The discursive legitimation strategies of the war on terror in France. *Critical Studies on Terrorism*, 10(3):476–500, Sept. 2017. 37, 49, 51, 52, 56, 57, 178, 196

[146] L. E. Bohórquez Arévalo and A. Espinosa. Theoretical approaches to managing complexity in organizations: A comparative analysis. *Estudios Gerenciales*, 31(134):20–29, Jan. 2015. 66

[147] D. Bond. Britain preparing to launch new cyber warfare unit. *Financial Times*, Sept. 2018. 41, 180, 236

[148] D. Bond and D. Sevastopulo. US and UK accuse China of cyber espionage campaign. *Financial Times*, Dec. 2018. 43

[149] I. Bonn and A. Pettigrew. Towards a dynamic theory of boards: An organisational life cycle approach. *Journal of Management & Organization*, 15(1):2–16, 2009. 25, 26, 28, 29, 204, 205

[150] A. Bonneville de Marsangy. *Traité Des Diverses Institutions Complémentaires Du Régime Pénitentiaire*. 1847. 229

[151] K. Booth. Security and Emancipation. *Review of International Studies*, 17(4):313–326, 1991. 33, 77

[152] W. C. Booth. *The Rhetoric of RHETORIC: The Quest for Effective Communication*. Wiley, 2009. 186

[153] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler, and R. W. Boss. If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2):151–164, Apr. 2009. 23

[154] A. Boucher. Power in elite interviewing: Lessons from feminist studies for political science. *Women's Studies International Forum*, 62:99–106, May 2017. 97, 100

[155] L. D. Bougher. The Case for Metaphor in Political Reasoning and Cognition. *Political Psychology*, 33(1):145–163, 2012. 69

[156] P. Bourdieu. The Force of Law: Toward a Sociology of the Juridical Field Essay. *Hastings Law Journal*, 38(5):814–854, 1987. 168

[157] M. F. C. Bourdillon. Oracles and Politics in Ancient Israel. *Man*, 12(1):124–140, 1977. 180, 182

[158] O. Bowcott and O. B. L. affairs correspondent. GCHQ data collection regime violated human rights, court rules. *The Guardian*, Sept. 2018. 229

[159] E. H. Bowman. Risk Seeking by Troubled Firms. *Sloan Management Review*, 23(4):33–42, 1982. 29, 203, 204

[160] S. Boyson. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, 34(7):342–353, July 2014. 195

[161] S. Brammer, A. Millington, and S. Pavelin. Gender and Ethnic Diversity Among UK Corporate Boards. *Corporate Governance: An International Review*, 15(2):393–403, 2007. 96, 98

[162] J. Branch. What's in a Name? Metaphors and Cybersecurity. *International Organization*, 75(1):39–70, 2021/ed. 33, 36, 37, 230

[163] E. Brandstätter, G. Gigerenzer, and R. Hertwig. The priority heuristic: Making choices without trade-offs. *Psychological Review*, 113(2):409–432, Apr. 2006. 74

[164] V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, Jan. 2006. 15, 105, 112, 113

[165] V. Braun and V. Clarke. (Mis)conceptualising themes, thematic analysis, and other problems with Fugard and Potts' (2015) sample-size tool for thematic analysis. *International Journal of Social Research Methodology*, 19(6):739–743, Nov. 2016. 113, 114, 115

[166] V. Braun and V. Clarke. Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, 11(4):589–597, Aug. 2019. 113

[167] V. Braun, V. Clarke, N. Hayfield, and G. Terry. Thematic Analysis. In P. Liamputtong, editor, *Handbook of Research Methods in Health Social Sciences*, pages 843–860. Springer, Singapore, 2019. 113

[168] D. G. M. Breakwell. Risk: Social Psychological Perspectives. In J. D. Wright, editor, *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)*, pages 711–716. Elsevier, Oxford, Jan. 2015. 61, 62

[169] S. W. Brenner and L. L. Clarke. Civilians in Cyberwarfare: Conscripts. *Vanderbilt Journal of Transnational Law*, 43:1011–1076, 2010. 44

[170] G. Breton. From folk-tales to shareholder-tales: Semiotics analysis of the annual report. *Society and Business Review*, 4(3):187–201, Jan. 2009. 138, 205

[171] J. Brito and T. Watkins. Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy. *Harvard National Security Journal*, 3(1):39–84, 2011. 36

[172] J. Brocklesby and J. Mingers. The use of the concept autopoiesis in the theory of viable systems. *Systems Research & Behavioral Science*, 22(1):3–9, Jan. 2005. 65

[173] R. G. Brody, H. U. Chang, and E. S. Schoenberg. Malware at its worst: Death and destruction. *International Journal of Accounting & Information Management*, 26(4):527–540, Jan. 2018. 32

[174] R. S. Brower and M. Y. Abolafia. Bureaucratic Politics: The View from Below. *Journal of Public Administration Research and Theory: J-PART*, 7(2):305–331, 1997. 56, 175

[175] A. D. Brown. Narrative, Politics and Legitimacy in an IT Implementation. *Journal of Management Studies*, 35(1):35–58, 1998. 45, 52, 143

[176] A. D. Brown. Identities and Identity Work in Organizations. *International Journal of Management Reviews*, 17(1):20–40, Jan. 2015. 45

[177] A. D. Brown and C. Coupland. Identity Threats, Identity Work and Elite Professionals. *Organization Studies*, 36(10):1315–1336, Oct. 2015. 47, 48, 55, 56, 177, 183

[178] A. Bryman. *Social Research Methods*. Oxford, Oxford, fourth edition, 2012. 85, 113

[179] N. Bubandt. Vernacular Security: The Politics of Feeling Safe in Global, National and Local Worlds. *Security Dialogue*, 36(3):275–296, Sept. 2005. 33, 35, 38, 43, 220

[180] D. Buil-Gil, N. Lord, and E. Barrett. The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention. *Victims & Offenders*, 16(3):286–315, Apr. 2021. 22

[181] C. Burck. Comparing qualitative research methodologies for systemic research: The use of grounded theory, discourse analysis and narrative analysis. *Journal of Family Therapy*, 27(3):237–262, 2005. 85, 113

[182] M. Burdon and L. Coles-Kemp. The significance of securing as a critical component of information security: An Australian narrative. *Computers & Security*, 87:101601, Nov. 2019. 14, 77, 86

[183] B. Burgemeestre, J. Hulstijn, and Y.-H. Tan. Value-based argumentation for justifying compliance. *Artificial Intelligence and Law*, 19(2):149, Sept. 2011. 84

[184] W. J. Burns, E. Peters, and P. Slovic. Risk Perception and the Economic Crisis: A Longitudinal Study of the Trajectory of Perceived Risk. *Risk Analysis*, 32(4):659–677, 2012. 108

[185] T. Butcher. Longing to belong. *Qualitative Research in Organizations and Management: An International Journal*, 8(3):242–257, Jan. 2013. 110

[186] E. M. Butler. *The Myth of the Magus*. Cambridge University Press, canto edition, 1993. 179, 181

[187] J. Butler. *Gender Trouble : Tenth Anniversary Edition*. London : Routledge, 2nd ed. edition, 2002 (1990). 110, 177

[188] J. Butler. Performative Agency. *Journal of Cultural Economy*, 3(2):147–161, July 2010. 51

[189] B. Buzan. Peace, Power, and Security: Contending Concepts in the Study of International Relations. *Journal of Peace Research*, 21(2):109–125, 1984. 35

[190] B. Buzan. *People, States and Fear : An Agenda for International Security Studies in the Post-Cold War Era*. London : Harvester Wheatsheaf, London, 2nd ed. edition, 1991. 33, 34, 39, 183

[191] B. Buzan and O. Wæver. Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory. *Review of International Studies*, 35(2):253–276, 2009. 42

[192] B. Buzan, O. Waever, and J. de Wilde. *Security : A New Framework for Analysis*. London : Lynne Rienner, London, 1998. 41

[193] K. Caelli, L. Ray, and J. Mill. 'Clear as Mud': Toward Greater Clarity in Generic Qualitative Research. *International Journal of Qualitative Methods*, 2(2):1–13, June 2003. 111

[194] M. G. Cains, L. Flora, D. Taber, Z. King, and D. S. Henshel. Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk analysis*, 2021. 18, 34

[195] T. Caldwell. Plugging the cyber-security skills gap. *Computer Fraud & Security*, 2013(7):5–10, July 2013. 56

[196] C. Camerer and M. Weber. Recent developments in modeling preferences: Uncertainty and ambiguity. *Journal of Risk and Uncertainty*, 5(4):325–370, Oct. 1992. 62

[197] D. Campbell, P. Shrives, and H. Bombach-Saager. Voluntary Disclosure of Mission Statements in Corporate Annual Reports: Signaling What and To Whom? *Business & Society Review (00453609)*, 106(1):65, 2001. 138

[198] K. Campbell, L. A. Gordon, M. P. Loeb, and L. Zhou. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, 11(3):431, Sept. 2003. 13

[199] M. Carr. Public-private partnerships in national cyber-security strategies. *International Affairs*, 92(1):43–62, Jan. 2016. 42, 44

[200] T. Carver. Men and Masculinities in International Relations Research. *The Brown Journal of World Affairs*, 21(1):113–126, 2014. 217, 236

[201] H. Cavusoglu, H. Cavusoglu, J.-Y. Son, and I. Benbasat. Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, 52(4):385–400, June 2015. 21, 23

[202] H. Cavusoglu, B. Mishra, and S. Raghunathan. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9(1):69–104, 2004. 201

[203] B. B. Caza, H. Vough, and H. Puranik. Identity work in organizations and occupations: Definitions, theories, and pathways forward. *Journal of Organizational Behavior*, 39(7):889–910, 2018. 45, 46, 51, 59, 144

[204] C. Chambers. The psychology of mass government surveillance — Chris Chambers. *The Guardian*, Mar. 2015. 229

[205] A. D. Chandler and B. Mazlish, editors. *Leviathans: Multinational Corporations and the New Global History*. Cambridge University Press, 2005. 214, 218

[206] S. E. Chang and C. B. Ho. Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3):345–361, Mar. 2006. 19, 21

[207] R. A. Chapman. Leviathan Writ Small: Thomas Hobbes on the Family. *The American Political Science Review*, 69(1):76–90, 1975. 217, 218, 220, 224, 225, 228

[208] M. D. R. Chari, P. David, A. Duru, and Y. Zhao. Bowman's risk-return paradox: An agency theory perspective. *Journal of Business Research*, 95:357–375, Feb. 2019. 26, 28, 29, 74, 204

[209] K. Charmaz. *Constructing Grounded Theory*. SAGE Publications Ltd, London, second edition, 2014. 112

[210] K. Charmaz. Grounded Theory: Methodology and Theory Construction. In J. D. Wright, editor, *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)*, pages 402–407. Elsevier, Oxford, Jan. 2015. 113

[211] K. Charmaz. Shifting the grounds: Constructivist grounded theory methods. In J. M. Morse, P. N. Stern, J. Corbin, B. Bowers, K. Charmaz, and A. E. Clarke, editors, *Developing Grounded Theory: The Second Generation*, pages 127–154. Taylor & Francis, 2016. 111

[212] L. Cheng, Y. Li, W. Li, E. Holm, and Q. Zhai. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, 39:447–459, Nov. 2013. 23, 24

[213] L. Cheng, J. Pei, and M. Danesi. A sociosemiotic interpretation of cybersecurity in U.S. legislative discourse. *Social Semiotics*, 29(3):286–302, May 2019. 42, 84

[214] R. H. Chilcote. Globalization or Imperialism? *Latin American Perspectives*, 29(6):80–84, 2002. 230

[215] M. H. Christ, S. A. Emett, S. L. Summers, and D. A. Wood. The Effects of Preventive and Detective Controls on Employee Performance and Motivation*. *Contemporary Accounting Research*, 29(2):432–452, 2012. 24

[216] K. H. Chung, J. Elder, and J.-C. Kim. Corporate Governance and Liquidity. *The Journal of Financial and Quantitative Analysis*, 45(2):265–291, 2010. 26

[217] R. Claassen. Hobbes Meets the Modern Business Corporation. *Polity*, 53(1):101–131, Dec. 2020. 214, 216, 218, 228

[218] C. A. Clarke, A. D. Brown, and V. H. Hailey. Working identities? Antagonistic discursive resources and managerial identity. *Human Relations*, 62(3):323–352, Mar. 2009. 177

[219] S. R. Clegg, C. Rhodes, and M. Kornberger. Desperately Seeking Legitimacy: Organizational Identity and Emerging Industries. *Organization Studies*, 28(4):495–513, Apr. 2007. 45, 49, 52, 54, 176

[220] M. A. Cohen and D. Peterson. The Implicit Morality of the Market and Joseph Heath's Market Failures Approach to Business Ethics. *Journal of Business Ethics*, 159(1):75–88, Sept. 2019. 57, 168

[221] S. Cohen. Whose side were we on? The undeclared politics of moral panic theory. *Crime, media, culture*, 7(3):237–243, 2011. 220

[222] E. G. Coleman and A. Golub. Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, 8(3):255–277, Sept. 2008. 40

[223] L. Coles-Kemp. Inclusive Security: Digital Security Meets Web Science. *Foundations and Trends® in Web Science*, 7(2):88–241, Dec. 2020. 34, 35

[224] L. Coles-Kemp, D. Ashenden, and K. O'Hara. Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen. *Politics and Governance*, 6(2):41–48, June 2018. 16, 24, 25, 42, 44, 77, 78, 246

[225] L. Coles-Kemp and R. R. Hansen. Walking the Line: The Everyday Security Ties that Bind. In T. Tryfonas, editor, *International Conference on Human Aspects of Information Security, Privacy, and Trust*, volume 10292, pages 464–480, Cham, 2017. Springer International Publishing. 31, 35

[226] L. Coles-Kemp, R. B. Jensen, and R. Talhouk. In a New Land: Mobile Phones, Amplified Pressures and Reduced Capabilities. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, pages 1–13, Montreal QC, Canada, 2018. ACM Press. 34

[227] L. Coles-Kemp, A. Zugenmaier, and M. Lewis. Watching You Watching Me: The Art of Playing the Panopticon. *Stand Alone*, pages 147–162, 2014. 21, 24, 44, 73

[228] D. Collins. Mapping the Entrails: The Practice of Greek Hepatoscopy. *The American Journal of Philology*, 129(3):319–345, 2008. 180

[229] I. Colville and L. McAulay. A tragedy of understanding; accounting for ontological security. *Accounting, Auditing & Accountability Journal*, 9(5):7–22, Dec. 1996. 51

[230] T. D. Comeau and C. L. Kemp. Intersections of age and masculinities in the information technology industry. *Ageing & Society*, 27(2):215–232, Mar. 2007. 55

[231] W. A. Conklin and D. Shoemaker. Cyber-Resilience: Seven Steps for Institutional Survival. *EDPACS*, 55(2):14–22, Feb. 2017. 66

[232] R. W. Connell and J. Wood. Globalization and Business Masculinities. *Men and Masculinities*, 7(4):347–364, Apr. 2005. 236

[233] W. R. Connor. Early Greek Land Warfare as Symbolic Expression. *Past & Present*, (119):3–29, 1988. 180

[234] C. R. Conrad, S. E. Croco, B. T. Gomez, and W. H. Moore. Threat Perception and American Support for Torture. *Political Behavior*, 40(4):989–1009, Dec. 2018. 41

[235] J. A. Conti and M. O'Neil. Studying power: Qualitative methods and the global elite. *Qualitative Research*, 7(1):63–82, Feb. 2007. 91, 97, 103, 104

[236] D. Conway, R. Taib, M. Harris, K. Yu, S. Berkovsky, and F. Chen. A Qualitative Investigation of Bank Employee Experiences of Information Security and Phish-

ing. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 115–129, 2017. 20, 186

[237] F. Cooren. Communication Theory at the Center: Ventriloquism and the Communicative Constitution of Reality. *Journal of Communication*, 62(1):1–20, Feb. 2012. 110, 111

[238] G. Corera. NHS cyber-attack 'came from N Korea'. https://www.bbc.com/news/technology-40297493, June 2017. 40, 42, 43, 178, 180, 227, 236

[239] G. Corfield. At the Supreme Court, Morrisons pops data breach liability win into its trolley – but it's not a get-out-of-compo free card for businesses. https://www.theregister.co.uk/2020/04/01/ morrisons_wins_data_breach_vicarious_liability_supreme_court/, 2020. 32

[240] K. G. Corley. A Commentary on "What Grounded Theory Is...": Engaging a Phenomenon from the Perspective of Those Living it. *Organizational Research Methods*, 18(4):600–605, Oct. 2015. 86

[241] P. Cormack. *Sociology and Mass Culture: Durkheim, Mills, and Baudrillard*. University of Toronto Press, 2004. 181

[242] F. R. Council. TalkTalk – customer communication in a crisis. https://www.frc.org.uk/directors/the-culture-project/case-study-talktalk-%E2%80%93-customer-communication-in-a. 29

[243] F. R. Council. UK Corporate Governance Code. https://www.frc.org.uk/getattachment/88bd8c45-50ea-4841-95b0-d2f4f48069a2/2018-UK-Corporate-Governance-Code-FINAL.pdf, 2018. 25, 26, 65, 139

[244] J. Cox. Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, 28(5):1849–1858, Sept. 2012. 23

[245] A. Crawford and S. Hutchinson. Mapping the Contours of 'Everyday Security': Time, Space and Emotion. *The British Journal of Criminology*, 56(6):1184–1202, Nov. 2016. 38, 39, 41, 78, 176

[246] A. Cresswell and S. Hassan. Organizational Impacts of Cyber Security Provisions: A Sociotechnical Framework. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, pages 98–98, Jan. 2007. 35

[247] S. Croft. Constructing Ontological Insecurity: The Insecuritization of Britain's Muslims. *Contemporary Security Policy*, 33(2):219–235, Aug. 2012. 37

[248] S. Croft and N. Vaughan-Williams. Fit for purpose? Fitting ontological security studies 'into' the discipline of International Relations: Towards a vernacular turn. *Cooperation and Conflict*, 52(1):12–30, Mar. 2017. 33

[249] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville. Future directions for behavioral information security research. *Computers & Security*, 32:90–101, Feb. 2013. 23

[250] M. L. Crossley. Narrative Psychology, Trauma and the Study of Self/Identity. *Theory & Psychology*, 10(4):527–546, Aug. 2000. 139

[251] M. Crouch and H. McKenzie. The logic of small samples in interview-based qualitative research. *Social Science Information*, 45(4):483–499, Dec. 2006. 93

[252] I. Culpitt. *Social Policy and Risk*. Sage, 1999. 58, 75

[253] A. L. Cunliffe. Managers as Practical Authors: Reconstructing our Understanding of Management Practice. *Journal of Management Studies*, 38(3):351–371, 2001. 36, 46, 48, 49, 50, 56, 58, 124, 166, 176

[254] A. L. Cunliffe. Crafting Qualitative Research: Morgan and Smircich 30 Years On. *Organizational Research Methods*, 14(4):647–673, Oct. 2011. 15, 110

[255] CyCognito. Leadership — The CyCognito Team. https://www.cycognito.com/leadership. 58

[256] B. Czarniawska. *Narratives in Social Science Research*. Sage, 2004. 36, 37, 45, 47, 49, 50, 91, 106, 112, 171, 180

[257] B. Czarniawska. How to Misuse Institutions and Get Away with It: Some Reflections on Institutional Theory(ies). In R. Greenwood, C. Oliver, K. Sahlin, and R. Suddaby, editors, *The SAGE Handbook of Organizational Institutionalism*. Sage Publications Ltd, United Kingdom, 2008. 83

[258] J. Da Silva. Producing 'good enough' automated transcripts securely: Extending Bokhove and Downey (2018) to address security concerns. *Methodological Innovations*, 14(1):2059799120987766, Jan. 2021. 87, 106

[259] J. Da Silva. Cyber security and the Leviathan. *Computers & Security*, 116:102674, May 2022. 246

[260] J. Da Silva and R. B. Jensen. 'Cyber security is a dark art': The CISO as soothsayer. *ACM Conference On Computer-Supported Cooperative Work And Social Computing (CSCW)*, Feb. 2022. 77, 210

[261] A. Da Veiga and J. H. P. Eloff. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2):196–207, Mar. 2010. 22

[262] A. Da Veiga and N. Martins. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49:162–176, Mar. 2015. 22

[263] A. Da Veiga and N. Martins. Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, 70:72–94, Sept. 2017. 22, 72

[264] H. S. Daemmrich and I. Daemmrich. *Themes & Motifs in Western Literature: A Handbook*. Francke, 1987. 172, 179

[265] R. Daft, J. Murphy, and H. Willmot. *Organization Theory and Design*. 2010. 64

[266] J. D'Arcy and T. Herath. A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 20(6):643–658, Nov. 2011. 23

[267] J. D'Arcy, A. Hovav, and D. Galletta. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20(1):79–98, Mar. 2009. 24, 40

[268] J. M. Darley. Research on Morality: Possible Approaches, Actual Approaches. *Psychological Science*, 4(6):353–357, 1993. 40

[269] S. Das, A. Mukhopadhyay, and M. Anand. Stock Market Response to Information Security Breach: A Study Using Firm and Attack Characteristics. *Journal of Information Privacy and Security*, 8(4):27–55, Oct. 2012. 13

[270] B. Davies and R. Harré. Positioning: The discursive production of selves. *Journal for the theory of social behaviour*, 20(1):43–63, 1990. 50

[271] H. Davies and M. Zhivitskaya. Three Lines of Defence: A Robust Organising Framework, or Just Lines in the Sand? *Global Policy*, 9(S1):34–42, 2018. 28, 205

[272] J. Dawson and R. Thomson. The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology*, 9, 2018. 16, 20, 71

[273] J. Day. Strangers on the train: The relationship of the IT department with the rest of the business. *Information Technology & People*, 20(1):6–31, Mar. 2007. 54, 64, 150

[274] W. de Lint and S. Virta. Security in ambiguity: Towards a radical security politics. *Theoretical Criminology*, 8(4):465–489, Nov. 2004. 44, 76

[275] H. Deakin and K. Wakefield. Skype interviewing: Reflections of two PhD researchers. *Qualitative Research*, 14(5):603–616, Oct. 2014. 107

[276] R. S. Debreceny. Research on IT Governance, Risk, and Value: Challenges and Opportunities. *Journal of Information Systems*, 27(1):129–135, 2013. 31

[277] S. Deetz. *Transforming Communication, Transforming Business: Building Responsive and Responsible Workplaces*. Hampton Press, 1995. 59

[278] R. J. Deibert and R. Rohozinski. Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, 4(1):15–32, Mar. 2010. 16

[279] G. Deleuze and F. Guattari. *A Thousand Plateaus: Capitalism and Schizophrenia*. Athlone Press, 1988. 35

[280] Department for Business, Energy & Industrial Strategy. Corporate governance reform-government response. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/640470/corporate-governance-reform-government-response.pdf, 2017. 27

[281] D. Dequech. Bounded Rationality, Institutions, and Uncertainty. *Journal of Economic Issues (Association for Evolutionary Economics)*, 35(4):911, Dec. 2001. 62

[282] J. Der Derian. *Critical Practices in International Theory : Selected Essays*. London : Routledge, London, 2009. 33, 35, 39, 41, 42

[283] R. Descartes and M. Moriarty. *Meditations on First Philosophy: With Selections from the Objections and Replies*. OUP Oxford, 2008. 77

[284] M. L. DeVault. Talking and Listening from Women's Standpoint: Feminist Strategies for Interviewing and Analysis. *Social Problems*, 37(1):96–116, 1990. 97, 105

[285] G. Dhillon and J. Backhouse. Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, 11(2):127–153, Apr. 2001. 15, 21

[286] C. Di Stefano. Masculinity as ideology in political theory: Hobbesian man considered. *Women's Studies International Forum*, 6(6):633–644, Jan. 1983. 217, 236, 237

[287] C. Dierksmeier. The Freedom–Responsibility Nexus in Management Philosophy and Business Ethics. *Journal of Business Ethics*, 101(2):263–283, June 2011. 201

[288] T. Dinev and Q. Hu. The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, 8(7):386–408, July 2007. 22

[289] Y. Diogenes. *Cybersecurity, Attack and Defense Strategies : Infrastructure Security with Red Team and Blue Team Tactics*. Infrastructure Security with Red Team and Blue Team Tactics. Birmingham, UK : Packt Publishing, 2018. 180

[290] C. Dobinson. TalkTalk Business COO Duncan Gooding on security strategy since 2015 data breach. https://www.cio.co.uk/it-security/talktalk-business-coo-on-security-since-cyberattack-3654833/. 29

[291] M. Dodel and G. Mesch. Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society*, 21(5):712–728, May 2018. 99

[292] M. Dodel and G. Mesch. An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. *Computers & Security*, 86:75–91, Sept. 2019. 99

[293] D. Dorsey. Objective Morality, Subjective Morality and the Explanatory Question. *Journal of Ethics & Social Philosophy*, 6(3):[i]–24, 2011. 40, 235

[294] M. Douglas. *How Institutions Think*. London : Routledge & Kegan Paul, London, 1987. 49, 51, 52, 59, 72, 73, 143, 144

[295] T. Douglas. *Scapegoats: Transferring Blame*. Routledge, 2002. 59

[296] L. Drabble, K. F. Trocki, B. Salcedo, P. C. Walker, and R. A. Korcha. Conducting qualitative interviews by telephone: Lessons learned from a study of alcohol use among sexual minority and heterosexual women. *Qualitative social work : QSW : research and practice*, 15(1):118–133, Jan. 2016. 107

[297] R. Drake. Cybersecurity is Everyone's Job. https://www.nist.gov/news-events/news/2018/10/cybersecurity-everyones-job, Oct. 2018. 71

[298] A. Dreiling. On the impact of the 'linguistic turn' on research in information systems. *ECIS 2006 Proceedings*, Jan. 2006. 35

[299] J. Driver. Moral Expertise: Judgement, Practice, and Analysis. *Social Philosophy and Policy*, 30(1-2):280–296, Jan. 2013. 57, 168

[300] J. N. Druckman and R. McDermott. Emotion and the Framing of Risky Choice. *Political Behavior*, 30(3):297–321, 2008. 69

[301] P. Du Gay and S. Vikkelsø. *For Formal Organization: The Past in the Present and Future of Organization Theory.* Oxford University Press, 2016. 27, 65, 66, 78, 86

[302] M. Dunn Cavelty. Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics*, 4(1):19–36, Apr. 2008. 39

[303] M. Dunn Cavelty. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, 15(1):105–122, Mar. 2013. 35, 36, 45

[304] G. Duttge and S. W. Lee. *The Law in the Information and Risk Society.* Gttingen : Universittsverlag Gttingen, 2011. 39

[305] J. E. Dutton and J. M. Dukerich. Keeping an Eye on the Mirror: Image and Identity in Organizational Adaptation. *The Academy of Management Journal*, 34(3):517–554, 1991. 90

[306] A. C. Edmondson and S. E. McManus. Methodological Fit in Management Field Research. *The Academy of Management Review*, 32(4):1155–1179, 2007. 101

[307] K. E. Eichensehr. Public-Private Cybersecurity. *Texas Law Review*, 95(3):467–538, Feb. 2017. 42, 44

[308] M. Eichler. Militarized Masculinities in International Relations Gender in International Relations. *Brown Journal of World Affairs*, 21:81–94, 2014. 56, 236

[309] K. M. Eisenhardt and M. E. Graebner. Theory Building from Cases: Opportunities and Challenges. *The Academy of Management Journal*, 50(1):25–32, 2007. 93

[310] N. Ellemers, R. Spears, and B. Doosje. Self and Social Identity. *Annual Review of Psychology*, 53(1):161–186, Feb. 2002. 47, 48

[311] K. D. Elsbach and C. B. Bhattacharya. Defining Who You Are by What You're Not: Organizational Disidentification and the National Rifle Association. *Organization Science*, 12(4):393–413, 2001. 54

[312] J. Elster. *Strong Feelings: Emotion, Addiction, and Human Behavior*. The Jean Nicod Lectures Series. MIT Press, 2000. 39, 68, 134, 183

[313] J. Elster. *Closing the Books: Transitional Justice in Historical Perspective*. Cambridge University Press, Cambridge, 2004. 38

[314] J. Elster and G. Lowenstein. Utility from memory and anticipation. In *Choice over Time*, pages 213–234. Russell Sage Foundation, 1992. 72

[315] K. J. Emich. Who's bringing the donuts: The role of affective patterns in group decision making. *Organizational Behavior and Human Decision Processes*, 124(2):122–132, July 2014. 70

[316] L. Empson. Elite interviewing in professional organizations. *Journal of Professions and Organization*, 5(1):58–69, Mar. 2018. 85, 91, 92, 100, 101, 103, 104

[317] E. H. Erikson. *Identity and the Life Cycle*. Norton, 1980. 171

[318] E. H. E. H. Erikson. *Identity, Youth and Crisis*. London : Faber & Faber, London, 1968. 46

[319] S. Ernest Chang and C.-S. Lin. Exploring organizational culture for information security management. *Industrial Management & Data Systems*, 107(3):438–458, Apr. 2007. 22, 72

[320] R. Esposito. *Bíos: Biopolitics and Philosophy*. University of Minnesota Press, 2008. 218

[321] F. Ewald. The Return of Descartes's Malicious Demon: An Outline of a Philosophy of Precaution. In T. Baker and J. Simon, editors, *Embracing Risk: The Changing Culture of Insurance and Responsibility*, pages 273–302. University of Chicago Press, Feb. 2002. 77, 210

[322] E. F. Fama and M. C. Jensen. Separation of Ownership and Control. *The Journal of Law & Economics*, 26(2):301–325, 1983. 25, 28, 204

[323] A. P. Farley. Amusing monsters. *Cardozo L. Rev.*, 23:1493, 2001. 43, 224

[324] M. B. Farooq and C. de Villiers. Telephonic qualitative research interviews: When to consider them and how to do them. *Meditari Accountancy Research*, 25(2):291–316, Jan. 2017. 107, 109

[325] F. Feldman. Hyperventilating about Intrinsic Value. *The Journal of Ethics*, 2(4):339–354, Dec. 1998. 139

[326] J. Fendt and W. Sachs. Grounded Theory Method in Management Research: Users' Perspectives. *Organizational Research Methods*, 11(3):430–455, July 2008. 82, 120

[327] R. Fichter. Do the Right Thing! Developing Ethical Behavior in Financial Institutions. *Journal of Business Ethics*, 151(1):69–84, Aug. 2018. 30

[328] I. Filatotchev, S. Toms, and M. Wright. The firm's strategic dynamics and corporate governance life-cycle. *International Journal of Managerial Finance*, 2(4):256–279, Oct. 2006. 26, 205

[329] A. Finden. Hygiene, Morality and the Pre-Criminal: Genealogies of Suspicion from Twentieth Century British-Occupied Egypt. *Australian Feminist Law Journal*, 0(0):1–19, June 2021. 30, 40, 140, 178

[330] S. Fineman. Constructing the Green Manager. *British Journal of Management*, 8(1):31, Mar. 1997. 139, 169

[331] M. L. Finucane, A. Alhakami, P. Slovic, and S. M. Johnson. The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making*, 13(1):1–17, 2000. 69

[332] C. Firestone and B. J. Scholl. Cognition does not affect perception: Evaluating the evidence for "top-down" effects. *Behavioral and Brain Sciences*, 39, 2016/ed. 68

[333] A. J. Fletcher. Applying critical realism in qualitative research: Methodology meets method. *International Journal of Social Research Methodology*, 20(2):181–194, Mar. 2017. 83

[334] D. Florêncio, C. Herley, and A. Shostack. FUD: A plea for intolerance. *Communications of the ACM*, 57(6):31–33, June 2014. 182, 183, 184, 186

[335] J. Foster and I. Parker. *Carrying out Investigations in Psychology: Methods and Statistics*. Wiley, 1995. 15

[336] M. Foucault. *Discipline and Punish*. Penguin Books, 1991 (1977). 167, 177, 178, 224, 229, 230, 231

[337] M. Foucault. *Society Must Be Defended*. Penguin Books, 2004. 43, 44, 220, 221, 230, 231, 234, 235, 236

[338] M. Foucault. *Security, Territory, Population*. Palgrave Macmillan, 2009. 228

[339] J. J. Francis, M. Johnston, C. Robertson, L. Glidewell, V. Entwistle, M. P. Eccles, and J. M. Grimshaw. What is an adequate sample size? Operationalising data saturation for theory-based interview studies. *Psychology & Health*, 25(10):1229–1245, Dec. 2010. 94

[340] W. R. Freudenburg. Risk and Recreancy: Weber, the Division of Labor, and the Rationality of Risk Perceptions. *Social Forces*, 71(4):909–932, 1993. 70, 71, 205

[341] N. H. Frijda. *The Emotions*. Cambridge University Press, 1986. 38, 39

[342] D. Frincke. Balancing Cooperation and Risk in Intrusion Detection. *ACM Trans. Inf. Syst. Secur.*, 3(1):1–29, Feb. 2000. 24

[343] L. A. Fujii. Shades of truth and lies: Interpreting testimonies of war and violence. *Journal of Peace Research*, 47(2):231–241, Mar. 2010. 90

[344] F. Furedi. *Culture of Fear Revisited : Risk-Taking and the Morality of Low Expectation*. London : Continuum, London, 4th ed. edition, 2006. 40, 44, 178

[345] S. Furnell. The cybersecurity workforce and skills. *Computers & Security*, 100:102080, Jan. 2021. 175

[346] A. Furnham, S. C. Richards, and D. L. Paulhus. The Dark Triad of Personality: A 10 Year Review. *Social and Personality Psychology Compass*, 7(3):199–216, 2013. 73

[347] P. I. Fusch and L. R. Ness. Are We There Yet? Data Saturation in Qualitative Research - ProQuest. *The Qualitative Report*, 20(9):1408–1416, 2015. 94, 95

[348] Y. Gabriel. *Storytelling in Organizations : Facts, Fictions, and Fantasies*. Oxford : Oxford University Press, Oxford, 2000. 171

[349] Y. Gabriel. *Myths, Stories, and Organizations: Premodern Narratives for Our Times*. Oxford University Press, 2004. 171

[350] W. B. Gallie. Essentially Contested Concepts. *Proceedings of the Aristotelian Society*, 56:167–198, 1955. 33

[351] U. Gasser, N. Gertner, J. L. Goldsmith, S. Landau, J. S. Nye, D. O'Brien, M. G. Olsen, D. Renan, J. Sanchez, B. Schneider, L. Schwartzol, and J. L. Zittrain. Don't Panic: Making Progress on the "Going Dark" Debate. *Berkman Center Research Publication*, 2016. 228

[352] U. E. Gattiker and H. Kelley. Morality and Computers: Attitudes and Differences in Moral Judgments. *Information Systems Research*, 10(3):233–254, 1999. 40

[353] K. J. Gergen. *The Saturated Self*. Basic Books, 1991. 50, 56, 176

[354] M. Gergen. Social ghosts, our imaginal dialogues with others. In *Annual Meeting of the American Psychology Association, New York*, 1987. 50, 56, 176

[355] B. Gert. Hobbes on Reason. *Pacific Philosophical Quarterly*, 82(3-4):243–257, 2001. 220, 221, 222

[356] S. Ghoshal. Bad Management Theories Are Destroying Good Management Practices. *Academy of Management Learning & Education*, 4(1):75–91, 2005. 66

[357] A. Giddens. *The Constitution of Society : Outline of the Theory of Structuration*. Berkeley : University of California Press, Berkeley, 1984. 146

[358] A. Giddens. *The Consequences of Modernity*. Stanford University Press, 1990. 38, 44, 46, 62, 65, 77, 133, 134, 135

[359] A. Giddens. *Modernity and Self-Identity : Self and Society in the Late Modern Age*. Cambridge : Polity, Cambridge, 1991. 34, 46, 48, 49, 58, 136, 160, 161, 198

[360] A. Giddens. Risk and Responsibility. *Modern Law Review*, 62(1):1–10, Jan. 1999. 61, 67

[361] M. Gilding. Motives of the Rich and Powerful in Doing Interviews with Social Scientists. *International Sociology*, 25(6):755–777, Nov. 2010. 104

[362] D. A. Gioia, K. G. Corley, and A. L. Hamilton. Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, 16(1):15–31, 2012. 111, 120

[363] E. Goffman. *The Presentation of Self in Everyday Life*. London : Penguin, London, 1990 (1959). 54, 59, 102, 103, 118, 160, 161, 169

[364] E. Goffman. On Face-Work: An Analysis of Ritual Elements in Social Interaction. *Reflections*, 4(3):7–13, 2003. 103

[365] E. Goffman. *Asylums : Essays on the Social Situation of Mental Patients and Other Inmates*. London : Routledge, 2017 (1961). 45

[366] V. Gonzalez. Contentious Storytelling Online: Articulating Activism through Negotiation of Metanarratives. *Sociological Perspectives*, 63(4):589–607, Aug. 2020. 37

[367] J. R. Goodall, W. G. Lutters, and A. Komlodi. I know my network: Collaboration and expertise in intrusion detection. In *Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work*, CSCW '04, pages 342–345, New York, NY, USA, Nov. 2004. Association for Computing Machinery. 21, 24, 186

[368] N. Goodman. *Languages of Art : An Approach to a Theory of Symbols*. Indianapolis : Hackett, Indianapolis, 2nd ed. edition, 1976. 32

[369] L. A. Gordon, M. P. Loeb, and L. Zhou. Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security*, 07(02):49–59, 2016. 66

[370] D. C. Gore. Sophists and Sophistry in the Wealth of Nations. *Philosophy & Rhetoric*, 44(1):1–26, 2011. 139, 186, 219

[371] A. Gramsci. *Prison Notebooks*. New York, New York, 1991. 59, 178

[372] J. Green, M. Franquiz, and C. Dixon. The Myth of the Objective Transcript: Transcribing as a Situated Act. *TESOL Quarterly*, 31(1):172–176, 1997. 105

[373] J. Green and N. Thorogood. *Qualitative Methods for Health Research*. SAGE Publications, 2009. 95

[374] A. Greene. Separating Normalcy from Emergency: The Jurisprudence of Article 15 of the European Convention on Human Rights Legitimacy and the Future of the European Court of Human Rights. *German Law Journal*, 12:1764–1785, 2011. 43

[375] C. J. Greenhouse. Hegemony and Hidden Transcripts: The Discursive Arts of Neoliberal Legitimation. *American Anthropologist*, 107(3):356–368, 2005. 42, 178, 179

[376] R. Greenwood, C. Oliver, K. Sahlin, and R. Suddaby, editors. *The SAGE Handbook of Organizational Institutionalism*. United Kingdom: Sage Publications Ltd, 2008. 83

[377] O. Gross. The Normless and Exceptionless Exception: Carl Schmitt's Theory of Emergency Powers and the Norm-Exception Dichotomy. *Cardozo Law Review*, 21:1825–1868, 2000. 41

[378] G. Guest, A. Bunce, and L. Johnson. How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods*, 18(1):59–82, Feb. 2006. 94

[379] J. Gunn. The rhetoric of exorcism: George W. Bush and the return of political demonology. *Western Journal of Communication*, 68(1):1–23, Mar. 2004. 179

[380] C. Guven and I. Hoxha. Rain or shine: Happiness and risk-taking. *The Quarterly Review of Economics and Finance*, 57:1–10, Aug. 2015. 70

[381] P. Hall, C. Heath, and L. Coles-Kemp. Critical visualization: A case for rethinking how we visualize risk and security. *Journal of Cybersecurity*, 1(1):93–108, Sept. 2015. 14, 84

[382] S. Hall. Entanglements Between Finance, Corporate Power and State Sovereignty. *Geopolitics*, 19(3):740–745, July 2014. 227

[383] M. Hammersley and P. Atkinson. *Ethnography Principles in Practice (Second Edition)*. Routledge, 1995. 83, 85, 91, 92, 93, 102, 103, 107, 113, 120

[384] J. Han, Y. J. Kim, and H. Kim. An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, 66:52–65, May 2017. 22, 23

[385] J. M. Haney and W. G. Lutters. ”It's Scary…It's Confusing…It's Dull”: How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 411–425, 2018. 21, 39, 69, 168, 169, 173, 175

[386] L. Hansen. The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School. *Millennium*, 29(2):285–306, June 2000. 56, 236

[387] L. Hansen and H. Nissenbaum. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53(4):1155–1175, 2009. 18, 35

[388] S. A. Hardy and G. Carlo. Moral identity. In S. J. Schwartz, K. Luyckx, and V. L. Vignoles, editors, *Handbook of Identity Theory and Research*. Springer New York, New York, NY, United States, 2011. 57, 139, 168, 175

[389] J. Harris and S. Holm. Is there a moral obligation not to infect others? *BMJ*, 311(7014):1215–1217, Nov. 1995. 71

[390] O. Hart. Thinking about the Firm: A Review of Daniel Spulber's The Theory of the Firm. *Journal of Economic Literature*, 49(1):101–113, Mar. 2011. 29

[391] C. C. Hartmann and J. Carmenate. Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research. *Current Issues in Auditing*, 15(2):A9–A23, Apr. 2021. 31

[392] W. S. Harvey. Strategies for conducting elite interviews. *Qualitative Research*, 11(4):431–441, Aug. 2011. 105, 110

[393] M. J. Hatch. *Organization Theory*. 1997. 62, 63, 64

[394] T. Havakhor, T. Zhang, and B. Hammer. Cybersecurity Talents and the Value of IT Security Investments. SSRN Scholarly Paper ID 3324696, Social Science Research Network, Rochester, NY, Jan. 2019. 176

[395] M. L. A. Hayward and D. C. Hambrick. Explaining the Premiums Paid for Large Acquisitions: Evidence of CEO Hubris. *Administrative Science Quarterly*, 42(1):103–127, 1997. 135

[396] J. Heath. An Adversarial Ethic for Business: Or When Sun-Tzu Met the Stakeholder. *Journal of Business Ethics*, 72(4):359–374, 2007. 139, 175, 176, 178

[397] J. Heath. Business Ethics and Moral Motivation: A Criminological Perspective. *Journal of Business Ethics*, 83(4):595–614, 2008. 57, 167, 168

[398] J. Heath. *Morality, Competition, and the Firm: The Market Failures Approach to Business Ethics*. Oxford University Press, USA, 2014. 57

[399] J. Heath, J. Moriarty, and W. Norman. Business Ethics and (or as) Political Philosophy. *Business Ethics Quarterly*, 20(3):427–452, 2010. 139, 207, 228

[400] K. Hedström, E. Kolkowska, F. Karlsson, and J. P. Allen. Value conflicts for information security management. *The Journal of Strategic Information Systems*, 20(4):373–384, Dec. 2011. 20, 23, 24

[401] A. Heraclides. 'What will become of us without barbarians?' The enduring Greek–Turkish rivalry as an identity-based conflict. *Southeast European and Black Sea Studies*, 12(1):115–134, Mar. 2012. 54, 56, 57, 174, 229, 235

[402] T. Herath and H. R. Rao. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2):154–165, May 2009. 22, 23, 24

[403] C. Herley. So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, NSPW '09, pages 133–144, New York, NY, USA, 2009. ACM. 22

[404] C. Herley and P. Van Oorschot. SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 99–120, May 2017. 184, 185, 186

[405] J. C. Hermanowicz. The Great Interview: 25 Strategies for Studying People in Bed. *Qualitative Sociology*, 25(4):479–499, Dec. 2002. 86, 87, 103, 107, 118, 324

[406] J. C. Hermanowicz. Argument and Outline for the Sociology of Scientific (and Other) Careers. *Social Studies of Science*, 37(4):625–646, Aug. 2007. 103, 325

[407] T. Herr. Cyber insurance and private governance: The enforcement power of markets. *Regulation & Governance*, 15(1):98–114, 2021. 31

[408] M. Hildebrandt. Balance or Trade-off? Online Security Technologies and Fundamental Rights. *Philosophy & Technology*, 26(4):357–379, Dec. 2013. 77

[409] S. Hitlin. Values, Personal Identity, and the Moral Self. In S. J. Schwartz, K. Luyckx, and V. L. Vignoles, editors, *Handbook of Identity Theory and Research*. Springer New York, New York, NY, UNITED STATES, 2011. 175

[410] M. A. Hitt, J.-L. Arregle, and R. M. Holmes. Strategic Management Theory in a Post-Pandemic and Non-Ergodic World. *Journal of Management Studies*, page 10.1111/joms.12646, Oct. 2020. 66

[411] HM Government. National Cyber Security Strategy 2016 to 2021. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021, 2016. 27, 42, 53, 144

[412] HM Government. National Cyber Strategy 2022, 2022. 27, 42, 53, 144

[413] T. Hobbes. *The English Works of Thomas Hobbes of Malmesbury; Now First Collected and Edited by Sir Willaim Molesworth, Bart.*, volume 6. John Bohn, London, 1839. 216

[414] T. Hobbes. *Leviathan*. Penguin Books, London, 1985 (1651). 33, 43, 77, 173, 197, 217, 218, 219, 220, 221, 222, 224, 225, 226, 227, 231, 234, 235

[415] T. Hobbes. *De Cive*. Dodo Press, 2009 (1642). 216, 218, 222, 225, 234

[416] J. A. Hobson. *Capitalism and Imperialism in South Africa*. The Tucker Publishing Co., New York, 1900. 227

[417] R. Hoda, J. Babb, and J. Nørbjerg. Toward Learning Teams. *IEEE Software*, 30(4):95–98, July 2013. 112

[418] W. Hofmann, D. C. Wisneski, M. J. Brandt, and L. J. Skitka. Morality in everyday life. *Science*, 345(6202):1340–1343, 2014. 235

[419] J. Holstein and J. Gubrium. *The Active Interview*. SAGE Publications, Inc., Thousand Oaks, California, 1995. 85, 102, 105

[420] A. Holt. Using the telephone for narrative interviewing: A research note. *Qualitative Research*, 10(1):113–121, Feb. 2010. 109

[421] V. Hooper and J. McKissack. The emerging role of the CISO. *Business Horizons*, 59(6):585–591, Nov. 2016. 14, 16, 20, 186

[422] D. Howard. Civic Virtue and Cybersecurity. In F. Demont-Biaggi, editor, *The Nature of Peace and the Morality of Armed Conflict*, pages 181–201. Springer International Publishing, Cham, 2017. 40, 71

[423] D. Howard. Technomoral Civic Virtues: A Critical Appreciation of Shannon Vallor's Technology and the Virtues. *Philosophy & Technology*, 31(2):293–304, June 2018. 31, 40

[424] Q. Hu, T. Dinev, P. Hart, and D. Cooke. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, 43(4):615–660, 2012. 20

[425] Q. Hu, P. Hart, and D. Cooke. The role of external and internal influences on information systems security – a neo-institutional perspective. *The Journal of Strategic Information Systems*, 16(2):153–172, June 2007. 64

[426] D. W. Hubbard and R. Seiersen. *How to Measure Anything in Cybersecurity Risk*. United States: John Wiley & Sons Inc, 2016. 76

[427] G. Huber and A. D. Brown. Identity Work, Humour and Disciplinary Power. *Organization Studies*, 38(8):1107–1126, Aug. 2017. 49

[428] Hugh Grove and Maclyn Clouse. Corporate governance for trillion dollar opportunities. *Corporate Board: Role*, 13(3):19–27, 2017. 66

[429] R. Hughes. A treaty for cyberspace. *International Affairs (Royal Institute of International Affairs 1944-)*, 86(2):523–541, 2010. 214

[430] J. Huysmans. Security! What Do You Mean?: From Concept to Thick Signifier. *European Journal of International Relations*, 4(2):226–255, June 1998. 33, 34, 40

[431] J. Huysmans. *The Politics of Insecurity : Fear, Migration, and Asylum in the EU*. Routledge, Milton Park, Abingdon, Oxon, 2006. 38

[432] J. Huysmans. What's in an act? On security speech acts and little security nothings. *Security Dialogue*, 42(4-5):371–383, Aug. 2011. 35, 36, 41

[433] M. M. Hyland and P. A. Marcellino. Examining gender on corporate boards: A regional study. *Corporate Governance: The international journal of business in society*, Dec. 2002. 96

[434] H. Ibarra and J. L. Petriglieri. Identity work and play. *Journal of Organizational Change Management*, 23(1):10–25, Jan. 2010. 47

[435] D. Ihde. *Technology and the Lifeworld: From Garden to Earth*. Indiana University Press, 1990. 83

[436] D. Ihde and E. Selinger, editors. *Chasing Technoscience : Matrix for Materiality*. Indiana Series in the Philosophy of Technology. Indiana University Press, Bloomington, IN, 2003. 14

[437] D. I. Ince. Strong password. In D. Ince, editor, *A Dictionary of the Internet*. Oxford University Press, Sept. 2013. 118

[438] P. Institute. 2022 Cost of Insider Threats Global Report. Technical report, Ponemon Institute, 2022. 32

[439] M. S. Islam, N. Farah, and T. F. Stafford. Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal*, 33(4):377–409, Apr. 2018. 90

[440] Y. Isoda. Use Japanese Castles to Better Communicate Defense-in-Depth Strategies. https://www.gartner.com/doc/2864017/use-japanese-castles-better-communicate, Oct. 2014. 37

[441] L. A. Janssen, E. M. Luciano, and M. G. Testa. The Influence of Organizational Culture on IT Governance: Perception of a Group of IT Managers from Latin American Companies. In *2013 46th Hawaii International Conference on System Sciences*, pages 4485–4494, Jan. 2013. 101

[442] G. C. Jayakrishnan, G. R. Sirigireddy, S. Vaddepalli, V. Banahatti, S. P. Lodha, and S. S. Pandit. Passworld: A Serious Game to Promote Password Awareness and Diversity in an Enterprise. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 1–18, 2020. 20

[443] M. H. Jessen. The State of the Company: Corporations, Colonies and Companies in Leviathan. *Journal of Intellectual History and Political Thought*, 1(1):56–85, 2012. 217, 218, 222, 230

[444] B. Jessop. Interpretive Sociology and the Dialectic of Structure and Agency. *Theory, Culture & Society*, 13(1):119–128, Feb. 1996. 146

[445] Z. Ji, D. Pons, and J. Pearse. Why Do Workers Take Safety Risks?—A Conceptual Model for the Motivation Underpinning Perverse Agency. *Safety*, 4(2):24, June 2018. 73

[446] P. Jiraporn, P. Chatjuthamard, S. Tong, and Y. S. Kim. Does corporate governance influence corporate risk-taking? Evidence from the Institutional Shareholders Services (ISS). *Finance Research Letters*, 13:105–112, May 2015. 25, 203

[447] H. Joffe. *Risk and 'The Other'*. Cambridge University Press, Cambridge, 1999. 37, 58, 59, 68, 72, 75, 76, 108, 190, 196

[448] D. R. Johnson, C. P. Scheitle, and E. H. Ecklund. Beyond the In-Person Interview? How Interview Quality Varies Across In-person, Telephone, and Skype Interviews:. *Social Science Computer Review*, pages 1–17, Dec. 2019. 107, 109

[449] A. C. Johnston and M. Warkentin. Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34(3):549–566, 2010. 39, 70

[450] L. Johnston and C. Shearing. *Governing Security: Explorations in Policing and Justice*. Routledge, 2003. 28, 203

[451] J. Jolly. Huge rise in hacking attacks on home workers during lockdown. *The Guardian*, May 2020. 39, 68

[452] R. Joyce, T. Pope, and B. Roantree. The characteristics and incomes of the top 1%. https://www.ifs.org.uk/publications/14303, Aug. 2019. 100

[453] K. Julisch. Understanding and overcoming cyber security anti-patterns. *Computer Networks*, 57(10):2206–2211, July 2013. 21, 24

[454] J. Justus, M. Colyvan, H. Regan, and L. Maguire. Buying into conservation: Intrinsic versus instrumental value. *Trends in Ecology & Evolution*, 24(4):187–191, Apr. 2009. 208

[455] M. E. Kabay, B. Robertson, M. Akella, and D. T. Lang. Using Social Psychology to Implement Security Policies. In *Computer Security Handbook*, pages 50.1–50.25. John Wiley & Sons, Ltd, 2015. 71, 206

[456] S. Kagan. Rethinking Intrinsic Value. *The Journal of Ethics*, 2(4):277–297, Dec. 1998. 208

[457] K. Kaiser. Protecting Respondent Confidentiality in Qualitative Research. *Qualitative Health Research*, 19(11):1632–1641, Nov. 2009. 119, 120

[458] N. K. Kakabadse, C. Figueira, K. Nicolopoulou, J. H. Yang, A. P. Kakabadse, and M. F. Özbilgin. Gender Diversity and Board Performance: Women's Experiences and Perspectives. *Human Resource Management*, 54(2):265–281, 2015. 96

[459] J. Kallinikos. *Governing Through Technology : Information Artefacts and Social Practice*. Basingstoke, GB: Palgrave Macmillan, 2011. 31, 32

[460] R. T. Kaminski. Escaping the cyber state of nature: Cyber deterrence and international institutions. In C. Czosseck and K. Podins, editors, *Conference on Cyber Conflict Proceedings 2010*, pages 79–94, Tallinn, 2010. CCD COE Publications. 44, 214

[461] A. Kangas, J. Kujala, A. Heikkinen, A. Lönnqvist, H. Laihonen, and J. Bethwaite. *Leading Change in a Complex World : Transdisciplinary Perspectives*. Tampere University Press, 2019. 44

[462] A. Kankanhalli, H.-H. Teo, B. C. Y. Tan, and K.-K. Wei. An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2):139–154, Apr. 2003. 23

[463] V. Kanniainen. Cyber Technology and the Arms Race. *German Economic Review*, 20(4):e523–e544, 2019. 41, 180, 236

[464] E. Karanja. The role of the chief information security officer in the management of IT security. *Information and Computer Security*, 25(3):300–329, July 2017. 20, 31, 186

[465] D. Kärreman and M. Alvesson. Cages in Tandem: Management Control, Social Identity, and Identification in a Knowledge-Intensive Firm. *Organization*, 11(1):149–175, Jan. 2004. 146

[466] D. Katz and R. L. Kahn. *The Social Psychology of Organizations: By Daniel Katz and Robert L. Kahn*. Wiley, 1966. 64

[467] M. Keil, G. Depledge, and A. Rai. Escalation: The Role of Problem Recognition and Cognitive Bias. *Decision Sciences*, 38(3):391–421, Aug. 2007. 135

[468] S. Kemp and L. Dwyer. An examination of organisational culture — the Regent Hotel, Sydney. *International Journal of Hospitality Management*, 20(1):77–93, Mar. 2001. 51

[469] R. Kerr. Discourse and leadership: Using the paradigm of the permanent state of emergency. *Critical Discourse Studies*, 5(3):201–216, Aug. 2008. 41

[470] A. Kharlamov and G. Pogrebna. Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity†. *Regulation & Governance*, 15(3):709–724, 2021. 31

[471] C. Kiesling, G. T. Sorell, M. J. Montgomery, and R. K. Colwell. Identity and spirituality: A psychosocial exploration of the sense of spiritual self. *Developmental Psychology*, 42(6):1269–1277, Nov. 2006. 171

[472] S. F. Kiesling. Hegemonic identity-making in narrative. In A. De Fina, D. Schiffrin, and M. Bamberg, editors, *Discourse and Identity*, Studies in Interactional Sociolinguistics, pages 261–287. Cambridge University Press, Cambridge, 2006. 37, 42

[473] C. Kinnvall. Feeling ontologically (in)secure: States, traumas and the governing of gendered space. *Cooperation and Conflict*, 52(1):90–108, Mar. 2017. 236

[474] I. Kirlappos, A. Beautement, and M. A. Sasse. "Comply or die" is dead: Long live security-aware principal agents. In *Financial Cryptography and Data Security*, 2013. 20, 24, 25, 186

[475] I. Kirlappos, S. Parkin, and M. A. Sasse. Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security. http://dx.doi.org/10.14722/usec.2014.23007, Feb. 2014. 24

[476] I. Kirlappos, S. Parkin, and M. A. Sasse. "Shadow security" as a tool for the learning organization. *ACM SIGCAS Computers and Society*, 45(1):29–37, Feb. 2015. 73

[477] H. K. Klein. Seeking the new and the critical in critical realism: Déjà vu? *Information and Organization*, 14(2):123–144, Apr. 2004. 83, 85

[478] F. H. Knight. *Risk, Uncertainty and Profit.* Cosimo, Incorporated, 2006 (1921). 63, 191

[479] L. Kocksch, M. Korn, A. Poller, and S. Wagenknecht. Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):92:1–92:20, Nov. 2018. 21, 22, 40, 176, 182, 186

[480] E. Kolkowska and G. Dhillon. Organizational power and information security rule compliance. *Computers & Security*, 33:3–11, Mar. 2013. 24

[481] R. Koppel, S. W. Smith, J. Blythe, and V. H. Kothari. Workarounds to computer access in healthcare organizations: You want my password or a dead patient? In *ITCH*, pages 215–220, 2015. 73

[482] D. Korff, B. Wagner, J. Powles, R. Avila, and U. Buermeyer. Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes. SSRN Scholarly Paper ID 2894490, Social Science Research Network, Rochester, NY, Jan. 2017. 42

[483] E. Krahmann. The market for ontological security. *European Security*, 27(3):356–373, July 2018. 231

[484] G. E. Kreiner. Tabula Geminus: A "Both/And" Approach to Coding and Theorizing. In *Handbook of Qualitative Organisational Research. Innovative Pathways and Methods*, pages 350–361. Routledge, 2016. 112, 113

[485] H. Kuchler. Hackers find suppliers are an easy way to target companies. *Financial Times*, Oct. 2014. 195

[486] H. Kuchler. FireEye bulks up for 'cyber arms race'. *Financial Times*, Jan. 2016. 41, 58, 166

[487] J. Kwon, J. R. Ulmer, and Tawei Wang. The Association between Top Management Involvement and Compensation and Information Security Breaches. *Journal of Information Systems*, 27(1):219–236, 2013. 31

[488] M. M. D. Lambert. *Medieval Heresy : Popular Movements from the Gregorian Reform to the Reformation*. Oxford : Blackwell, Oxford, 2nd ed. edition, 1992. 173

[489] N. Lankton, J. B. Price, and M. Karim. Cybersecurity Breaches and the Role of Information Technology Governance in Audit Committee Charters. *Journal of Information Systems*, 35(1):101–119, 2021. 31

[490] J. Lanz. The Chief Information Security Officer: The New CFO of Information Security. *CPA Journal*, 87(6):52–57, June 2017. 16

[491] J. C. Lapadat and A. C. Lindsay. Transcription in Research and Practice: From Standardization of Technique to Interpretive Positionings. *Qualitative Inquiry*, 5(1):64–86, Mar. 1999. 105

[492] M. Lapke and G. Dhillon. A Semantic Analysis of Security Policy Formulation and Implementation: A Case Study. *AMCIS 2006 Proceedings*, Dec. 2006. 24

[493] L. Lapointe and S. Rivard. A Multilevel Model of Resistance to Information Technology Implementation. *MIS Quarterly*, 29(3):461–491, 2005. 206

[494] O. L. Larsson. The connections between crisis and war preparedness in Sweden. *Security Dialogue*, 52(4):306–324, Aug. 2021. 207

[495] C. Lasch. *The Culture of Narcissism : American Life in an Age of Diminishing Expectations*. New York : Norton, New York, 1978. 161

[496] C. Lasch. *The Minimal Self: Psychic Survival in Troubled Times*. W. W. Norton, 1985. 161

[497] B. Latour. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford University Press, Incorporated, Oxford, UNITED KINGDOM, 2005. 35

[498] A. Lavorgna. Cyber-organised crime. A case of moral panic? *Trends in Organized Crime*, 22(4):357–374, Dec. 2019. 220

[499] P. R. Lawrence and J. W. Lorsch. *Organization and Environment*. Irwin, 1967. 65

[500] I. Lee. Becoming a writing teacher: Using "identity" as an analytic lens to understand EFL writing teachers' development. *Journal of Second Language Writing*, 22(3):330–345, Sept. 2013. 111

[501] C. Leuprecht, D. B. Skillicorn, and V. E. Tait. Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly*, 33(2):250–257, Apr. 2016. 36, 37

[502] D. I. Levy. Active Cyber Defence - The Second Year, 2019. 60

[503] N. Liang and S. Lin. Erroneous Learning from the West? A Narrative Analysis of Chinese MBA Cases Published in 1992, 1999 and 2003. *MIR: Management International Review*, 48(5):603–638, 2008. 66

[504] J. Limnéll. The cyber arms race is accelerating – what are the consequences? *Journal of Cyber Policy*, 1(1):50–60, Jan. 2016. 41, 44, 66, 180, 236

[505] S. A. Lloyd. *Morality in the Philosophy of Thomas Hobbes: Cases in the Law of Nature*. Cambridge University Press, Cambridge, 2009. 235

[506] S. A. Lloyd and S. Sreedhar. Hobbes's Moral and Political Philosophy. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, fall 2020 edition, 2020. 218, 235

[507] I. Loader, B. Goold, and A. Thumala. Grudge Spending: The Interplay between Markets and Culture in the Purchase of Security. *The Sociological Review*, 63(4):858–875, Nov. 2015. 39, 176

[508] J. Locke. *An Essay Concerning Human Understanding*. Penguin Classics. Penguin Books, London [Eng.], [1690] 1997. 39, 62, 216

[509] K. Locke. Rewriting the Discovery of Grounded Theory after 25 Years? *Journal of Management Inquiry*, 5(3):239–245, Sept. 1996. 85

[510] L. L. Lopes. Between Hope and Fear: The Psychology of Risk. In L. Berkowitz, editor, *Advances in Experimental Social Psychology*, volume 20, pages 255–295. Academic Press, Jan. 1987. 67

[511] R. Luburic, M. Perovic, and R. Sekulovic. QUALITY MANAGEMENT IN TERMS OF STRENGTHENING THE "THREE LINES OF DEFENCE" IN RISK MANAGEMENT - PROCESS APPROACH. *International Journal for Quality Research*, 9(2):243–250, June 2015. 28

[512] N. Luhmann. *Risk : A Sociological Theory*. Berlin : de Gruyter, Berlin, 1993. 62

[513] J. Lumby. Performativity and identity: Mechanisms of exclusion. *Journal of Education Policy*, 24(3):353–369, May 2009. 51

[514] D. Lupton and J. Tulloch. 'Life would be pretty dull without risk': Voluntary risk-taking and its pleasures. *Health, Risk & Society*, 4(2):113–124, July 2002. 58, 61

[515] M. D. Lynall, B. R. Golden, and A. J. Hillman. Board Composition from Adolescence to Maturity: A Multitheoretic View. *The Academy of Management Review*, 28(3):416–431, 2003. 205

[516] S. Lyons. Defending Our Stakeholders: Corporate Defence Management Explored. SSRN Scholarly Paper ID 2202135, Social Science Research Network, Rochester, NY, July 2012. 28

[517] J.-F. Lyotard. *The Postmodern Condition : A Report on Knowledge*. Manchester : Manchester University Press, Manchester, 2001. 37

[518] E. MacAskill and P. Johnson. MI5 head: 'increasingly aggressive' Russia a growing threat to UK. *The Guardian*, Nov. 2016. 77

[519] D. A. MacDonald. Spiritual Identity: Individual Perspectives. In S. J. Schwartz, K. Luyckx, and V. L. Vignoles, editors, *Handbook of Identity Theory and Research*. Springer New York, New York, NY, UNITED STATES, 2011. 171

[520] K. Mackenzie. Staff may open doors to criminals. *Financial Times*, May 2006. 71

[521] C. B. Macpherson. Introduction. In *Leviathan*. Penguin Books, London, 1985. 216

[522] J. Magnusson, C. Juiz, B. Gomez, and B. Bermejo. Governing Technology Debt: Beyond Technical Debt. In *2018 IEEE/ACM International Conference on Technical Debt (TechDebt)*, pages 76–84, May 2018. 31

[523] S. Maitlis, T. J. Vogus, and T. B. Lawrence. Sensemaking and emotion in organizations. *Organizational Psychology Review*, 3(3):222–247, Aug. 2013. 58, 68, 69, 74

[524] K. Makortoff. Travelex falls into administration, with loss of 1,300 jobs. *The Guardian*, Aug. 2020. 72

[525] Y. Maleh, A. Sahid, and M. Belaissaoui. A Maturity Framework for Cybersecurity Governance in Organizations. *EDPACS*, 63(6):1–22, June 2021. 31

[526] D. Maliniak, R. Powers, and B. F. Walter. The Gender Citation Gap in International Relations. *International Organization*, 67(4):889–922, 2013. 236

[527] A. S. R. Manstead. The psychology of social class: How socioeconomic status impacts thought, feelings, and behaviour. *British Journal of Social Psychology*, 57(2):267–291, 2018. 99

[528] M. V. Mäntylä, B. Adams, F. Khomh, E. Engström, and K. Petersen. On rapid releases and software testing: A case study and a semi-systematic literature review. *Empirical Software Engineering*, 20(5):1384–1425, Oct. 2015. 112

[529] J. G. March and H. A. Simon. *Organizations*. Wiley, 1993 (1958). 64

[530] A. Marchais-Roubelat and F. Roubelat. The Delphi method as a ritual: Inquiring the Delphic Oracle. *Technological Forecasting and Social Change*, 78(9):1491–1499, Nov. 2011. 180, 182

[531] A. Markham. Fabrication as Ethical Practice. *Information, Communication & Society*, 15(3):334–353, Apr. 2012. 120

[532] K. Martin and R. E. Freeman. Some Problems with Employee Monitoring. *Journal of Business Ethics*, 43(4):353–361, Apr. 2003. 40

[533] L. M. Martin, I. Warren-Smith, J. M. Scott, and S. Roper. Boards of directors and gender diversity in UK companies. *Gender in Management: An International Journal*, May 2008. 96

[534] M. Mason. Sample Size and Saturation in PhD Studies Using Qualitative Interviews. *Forum: Qualitative Social Research*, 11(3), Aug. 2010. 94

[535] P. Masons. The Senior Managers Regime. 27

[536] H. R. Maturana. The organization of the living: A theory of the living organization. *International Journal of Man-Machine Studies*, 7(3):313–332, May 1975. 65

[537] M. L. Maznevski and K. M. Chudoba. Bridging Space over Time: Global Virtual Team Dynamics and Effectiveness. *Organization Science*, 11(5):473–492, 2000. 101

[538] J. McAuley, L. D. Souza, V. Sharma, I. Robinson, C. J. Main, and A. O. Frank. Self defined ethnicity is unhelpful. *BMJ*, 313(7054):425–426, Aug. 1996. 98

[539] J. McAvoy and T. Butler. A critical realist method for applied business research. *Journal of Critical Realism*, 17(2):160–175, Mar. 2018. 83

[540] C. S. McClure. War, Madness, and Death: The Paradox of Honor in Hobbes's Leviathan. *The Journal of Politics*, 76(1):114–125, 2013. 222

[541] M. McDonald. Securitization and the Construction of Security. *European Journal of International Relations*, 14(4):563–587, Dec. 2008. 41

[542] C. J. McLachlan and R. J. Garcia. Philosophy in practice? Doctoral struggles with ontology and subjectivity in qualitative interviewing. *Management Learning*, 46(2):195–210, Apr. 2015. 82, 83

[543] P. McLaren. Field Relations and the Discourse of the Other: Collaboration in Our Own Ruin. In W. Shaffir and R. A. Stebbins, editors, *Experiencing Fieldwork: An inside View of Qualitative Research*, pages 149–163. Sage Publications, Newbury Park, Calif., 1991. 103

[544] C. McRae. Teaching Like a Bass Player: Performative Pedagogy and Practice. *Transformations: The Journal of Inclusive Scholarship and Pedagogy*, 20(1):78–86, 2009. 151

[545] B. McSweeney. *Security, Identity and Interests : A Sociology of International Relations*, volume 69. Cambridge : Cambridge University Press, Cambridge, 1999. 22, 33, 34, 43, 55, 97

[546] C. E. Merriam. Hobbes's Doctrine of the State of Nature. *Proceedings of the American Political Science Association*, 3:151–157, 1906. 43, 217

[547] O. Michalec, S. Milyaeva, and A. Rashid. Reconfiguring governance: How cyber security regulations are reconfiguring water governance. *Regulation & Governance*, 16(4), 2022. 30

[548] R. Miles and C. Snow. *Organizational Strategy, Structure, and Process*. 1978. 62, 64

[549] H. Mintzberg. *The Structuring of Organizations*. Prentice-Hall, 1979. 25, 62, 63, 64, 78, 222, 236

[550] J. Mirkovic, P. Reiher, C. Papadopoulos, A. Hussain, M. Shepard, M. Berg, and R. Jung. Testing a Collaborative DDoS Defense In a Red Team/Blue Team Exercise. *IEEE Transactions on Computers*, 57(8):1098–1112, Aug. 2008. 55

[551] J. Mitzen. Ontological Security in World Politics: State Identity and the Security Dilemma. *European Journal of International Relations*, 12(3):341–370, Sept. 2006. 34, 43, 64, 133

[552] J. Monaghan. Terror carceralism: Surveillance, security governance and de/civilization. *Punishment & Society*, 15(1):3–22, Jan. 2013. 187

[553] T. Moore, S. Dynes, and F. R. Chang. Identifying How Firms Manage Cybersecurity Investment. Working Paper, Southern Methodist University, Dallas, Texas, 2015. 28

[554] A. Morse, W. Wang, and S. Wu. Executive Lawyers: Gatekeepers or Strategic Officers? *The Journal of Law and Economics*, 59(4):847–888, Nov. 2016. 51

[555] J. M. Morse. Subjects, Respondents, Informants, and Participants? *Qualitative Health Research*, 1(4):403–406, Nov. 1991. 90

[556] J. M. Morse. "Data Were Saturated . . . ". *Qualitative Health Research*, 25(5):587–588, 2015. 93

[557] A. Moser and I. Korstjens. Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice*, 24(1):9–18, Jan. 2018. 92, 94

[558] G. B. Moskowitz and P. Li. Egalitarian goals trigger stereotype inhibition: A proactive form of stereotype control. *Journal of Experimental Social Psychology*, 47(1):103–116, Jan. 2011. 74, 93, 101

[559] M. Müller and C. Schurr. Assemblage thinking and actor-network theory: Conjunctions, disjunctions, cross-fertilisations. *Transactions of the Institute of British Geographers*, 41(3):217–229, 2016. 35

[560] A.-B. Munteanu and D. Fotache. Enablers of Information Security Culture. *Procedia Economics and Finance*, 20:414–422, Jan. 2015. 134

[561] C. Murphy, A. C. Klotz, and G. E. Kreiner. Blue skies and black boxes: The promise (and practice) of grounded theory in human resource management research. *Human Resource Management Review*, 27(2):291–305, June 2017. 84, 111, 120

[562] S. Murray. Human skills are essential in battle against cyber crime. Nov. 2016. 175

[563] G. Mythen. *Ulrich Beck: A Critical Introduction to the Risk Society.* United Kingdom: Pluto Press, 2004. 58, 61, 62, 67, 68, 69, 72, 75, 76, 191, 202, 205

[564] T. Nagel. War and Massacre. *Philosophy & Public Affairs*, 1(2):123–144, 1972. 57

[565] C. V. Nakassis. Brand, Citationality, Performativity. *American Anthropologist*, 114(4):624–638, 2012. 51

[566] A. Nasir, R. A. Arshah, M. R. A. Hamid, and S. Fahmy. An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications*, 44:12–22, Feb. 2019. 22

[567] M. Neocleous. The Problem with Normality: Taking Exception to "Permanent Emergency". *Alternatives*, 31(2):191–213, Apr. 2006. 41, 43

[568] M. Neocleous. *Critique of Security.* Edinburgh : Edinburgh University Press, Edinburgh, 2008. 33, 34, 35, 37, 39, 41, 43, 44, 53, 75, 77, 137, 178, 179, 181, 183, 187, 195, 220, 228, 231, 235, 236

[569] M. Nicho. A process model for implementing information systems security governance. *Information and Computer Security*, 26(1):10–38, Mar. 2018. 24

[570] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke. SCADA security in the light of Cyber-Warfare. *Computers & Security*, 31(4):418–436, June 2012. 34, 175

[571] J. Nicholson, L. Coventry, and P. Briggs. Introducing the Cybersurvival Task: Assessing and Addressing Staff Beliefs about Effective Cyber Protection. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 443–457, 2018. 186

[572] D. Nissenbaum. Author Warns U.S. Military to Focus on China. *Wall Street Journal*, June 2015. 180, 183

[573] H. Nissenbaum. Where Computer Security Meets National Security. *Ethics and Information Technology*, 7(2):61–73, June 2005. 40, 44

[574] S. Nixon and B. Crewe. Pleasure at Work? Gender, Consumption and Work-based Identities in the Creative Industries. *Consumption Markets & Culture*, 7(2):129–147, June 2004. 175

[575] M. Nøkleberg. Expecting the exceptional in the everyday: Policing global transportation hubs. *Security Dialogue*, pages 1–18, June 2021. 208, 209

[576] C. Nolan, G. Lawyer, and R. M. Dodd. Cybersecurity: Today's most pressing governance issue. *Journal of Cyber Policy*, 4(3):425–441, Sept. 2019. 30

[577] L. Noonan. Bank of England-backed cyber security war game opens to more companies. *Financial Times*, Oct. 2021. 234

[578] S. N. Nordstrom. Not So Innocent Anymore: Making Recording Devices Matter in Qualitative Interviews. *Qualitative Inquiry*, 21(4):388–401, Apr. 2015. 105

[579] G. Novick. Is There a Bias Against Telephone Interviews In Qualitative Research? *Research in nursing & health*, 31(4):391–398, Aug. 2008. 107, 109

[580] E. N.V. Euronext Frequently Asked Questions 2019. https://www.euronext.com/sites/default/files/2019-11/52118_Euronext-FAQ-2019_v08.pdf, 2019. 90

[581] J. Nyman. Pragmatism, practice and the value of security. In *Ethical Security Studies: A New Research Agenda*. Taylor & Francis, 2016. 40

[582] T. O'Connor and J. Byrne. Governance and the corporate life-cycle. *International Journal of Managerial Finance*, 11(1):23–43, Jan. 2015. 29, 205

[583] G. Öğütçü, Ö. M. Testik, and O. Chouseinoglou. Analysis of personal information security behavior and awareness. *Computers & Security*, 56:83–93, Feb. 2016. 22

[584] P. O'Malley. Experiments in risk and criminal justice. *Theoretical Criminology*, 12(4):451–469, Nov. 2008. 62, 76, 201, 202

[585] C. O'Reilly. Corporations, Culture, and Commitment: Motivation and Social Control in Organizations. *California Management Review*, 50(2):85–101, Feb. 2008. 72

[586] M. O'Reilly and N. Parker. 'Unsatisfactory Saturation': A critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research*, 13(2):190–197, Apr. 2013. 94

[587] S. A. Osher. Privacy, Computers and the Patriot Act: The Fourth Amendment Isn't Dead, But No One Will Insure It Essay. *Florida Law Review*, 54(3):521–542, 2002. 234

[588] S. A. Ostrander. "SURELY YOU'RE NOT IN THIS JUST TO BE HELPFUL": Access, Rapport, and Interviews in Three Studies of Elites. *Journal of Contemporary Ethnography*, 22(1):7, 1993. 103, 104

[589] D. Page. Desirable organisational masculinities: Competition and entrepreneurialism in schools of construction in further education colleges. *British Journal of Sociology of Education*, 35(6):895–913, Nov. 2014. 72

[590] S. Pahnila, M. Siponen, and A. Mahmood. Employees' Behavior towards IS Security Policy Compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, pages 156b–156b, Jan. 2007. 23

[591] A. Pal, T. Herath, R. De', and H. R. Rao. Is the Convenience Worth the Risk? An Investigation of Mobile Payment Usage. *Information Systems Frontiers*, 23(4):941–961, Aug. 2021. 77

[592] P. Pasquino. *Theatrum Politicum: The Genealogy of Capital - Police and the State of Prosperity*. Chicago : University of Chicago Press, Chicago, 1991. 228

[593] D. L. Paulhus and K. M. Williams. The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality*, 36(6):556–563, Dec. 2002. 73

[594] D. Peacock and A. Irons. Gender Inequality in Cybersecurity: Exploring the Gender Gap in Opportunities and Progression. *International Journal of Gender, Science and Technology*, 9(1):25–44, May 2017. 55, 56, 96, 176, 236

[595] M. Peacock. Obligation and Advantage in Hobbes' "Leviathan". *Canadian Journal of Philosophy*, 40(3):433–458, 2010. 218

[596] K. Pearlson, B. Thorson, S. Madnick, and M. Coden. Cyberattacks Are Inevitable. Is Your Company Prepared? *Harvard Business Review*, Mar. 2021. 219

[597] M. Peel, M. Murgia, and H. Foy. EU scrambles to stop Russian interference ahead of May elections. *Financial Times*, Feb. 2019. 43, 178

[598] R. B. Peterson. Empirical Research in International Management: A Critique and Future Agenda. In *Handbook of Qualitative Research Methods for International Business*, pages 25–55. Edward Elgar, 2004. 101

[599] J. L. Petriglieri. Under threat: Responses to and the consequences of threats to individuals' identities. *The Academy of Management Review*, 36(4):641–662, 2011. 47

[600] A. Pettigrew and T. McNulty. Control and creativity in the boardroom. In D. C. Hambrick, D. Nadler, and M. L. Tushman, editors, *How CEOs, Top Teams and Boards Steer Transformation*, pages 226–255. Harvard Business School Press, Boston, MA, 1998. 29

[601] D. Pettman. *Look at the Bunny: Totem, Taboo, Technology*. John Hunt Publishing, 2013. 49, 51, 136, 179, 181, 182

[602] S. L. Pfleeger, M. A. Sasse, and A. Furnham. From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management*, 11(4), Jan. 2014. 22, 197

[603] K. Phull, G. Ciflikli, and G. Meibauer. Gender and bias in the International Relations curriculum: Insights from reading lists. *European Journal of International Relations*, page 1354066118791690, Aug. 2018. 236

[604] M. Pirson. A Humanistic Perspective for Management Theory: Protecting Dignity and Promoting Well-Being. *Journal of Business Ethics*, 159(1):39–57, Sept. 2019. 66

[605] C. Pitt. U.S. PATRIOT ACT AND RACIAL PROFILING: ARE THERE CONSEQUENCES OF DISCRIMINATION? *Michigan Sociological Review*, 25:53–69, 2011. 234

[606] J. Platt. On Interviewing One's Peers. *The British Journal of Sociology*, 32(1):75–91, 1981. 85, 89

[607] A. Poller, L. Kocksch, S. Türpe, F. A. Epp, and K. Kinder-Kurlanda. Can Security Become a Routine? A Study of Organizational Change in an Agile Software Development Group. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '17, pages 2489–2503, New York, NY, USA, Feb. 2017. Association for Computing Machinery. 20, 21, 186

[608] J. F. Porac, H. Thomas, F. Wilson, D. Paton, and A. Kanfer. Rivalry and the Industry Model of Scottish Knitwear Producers. *Administrative Science Quarterly*, 40(2):203–227, 1995. 54

[609] C. Posey, T. L. Roberts, P. B. Lowry, and R. T. Hightower. Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, 51(5):551–567, July 2014. 20, 24

[610] J. Potter. Discourse analysis and constructionist approaches: Theoretical background. In J. Richardson, editor, *Handbook of Qualitative Research Methods for Psychology and the Social Sciences*, pages 125–140. BPS Books (The British Psychological Society), Leicester, 1996. 84

[611] A. Prasad, P. Green, and J. Heales. On IT governance structures and their effectiveness in collaborative organizational structures. *International Journal of Accounting Information Systems*, 13(3):199–220, Sept. 2012. 101

[612] PricewaterhouseCoopers. Travelex Holdings Limited and certain subsidiaries - in administration. https://www.pwc.co.uk/services/business-restructuring/administrations/travelex.html. 72

[613] J. G. Proudfoot, R. J. Boyle, and J. A. Clements. Mitigating Threats to Collaboration and CMC: Identifying Antecedents of Online Deviance. In *2013 46th Hawaii International Conference on System Sciences*, pages 325–334, Jan. 2013. 40

[614] J. A. Raelin. The End of Managerial Control? *Group & Organization Management*, 36(2):135–160, Apr. 2011. 66

[615] S. Rai and P. Chukwuma. Ciso – Career Is Surely Over? *EDPACS*, 59(6):1–4, June 2019. 16

[616] A. Ram. Petya attack raises fears of escalation of global cyber arms race. *Financial Times*, July 2017. 39, 41

[617] R. Ramirez and N. Choucri. Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review. *IEEE Access*, 4:2216–2243, 2016. 13

[618] P. Ranasinghe. Discourse, practice and the production of the polysemy of security. *Theoretical Criminology*, 17(1):89–107, 2012. 36, 38, 61

[619] D. D. Raphael. *Hobbes: Morals and Politics*. George Allen & Unwin Ltd, 1977. 235

[620] D. D. Raphael. *Moral Philosophy*. Oxford University Press, 1994. 39, 178

[621] J. Reed, Y. Zhong, L. Terwoerds, and J. Brocaglia. The 2017 Global Information Security Workforce Study- Women in Cybersecurity.pdf, 2017. 96, 176

[622] R. Reid and J. Van Niekerk. From information security to cyber security cultures. In *2014 Information Security for South Africa*, pages 1–7, Aug. 2014. 22

[623] L. Reinfelder, R. Landwirth, and Z. Benenson. Security Managers Are Not The Enemy Either. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 1–7, New York, NY, USA, May 2019. Association for Computing Machinery. 15, 20, 21, 24, 185, 186, 239

[624] B. Reinheimer, L. Aldag, P. Mayer, M. Mossano, R. Duezguen, B. Lofthouse, T. von Landesberger, and M. Volkamer. An investigation of phishing awareness and education over time: When and how to best remind users. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 259–284, 2020. 20, 22, 186

[625] K. Renaud. Blaming Noncompliance Is Too Convenient: What Really Causes Information Breaches? *IEEE Security Privacy*, 10(3):57–63, May 2012. 24

[626] K. Renaud and M. Dupuis. Cyber security fear appeals: Unexpectedly complicated. In *Proceedings of the New Security Paradigms Workshop*, NSPW '19, pages

42–56, New York, NY, USA, Sept. 2019. Association for Computing Machinery. 70

[627] H.-S. Rhee, C. Kim, and Y. U. Ryu. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(8):816–826, Nov. 2009. 40

[628] H.-S. Rhee, Y. Ryu, and C.-T. Kim. I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security. *ICIS 2005 Proceedings*, page 15, 2005. 66, 76, 135

[629] C. Rhodes and A. D. Brown. Narrative, organizations and research. *International Journal of Management Reviews*, 7(3):167–188, 2005. 49

[630] A. Riaz. How to Identify Moral Experts. *The Journal of Ethics*, June 2020. 57

[631] G. Rice. Reflections on interviewing elites. *Area*, 42(1):70–75, Mar. 2010. 85

[632] J. Richards. Cyber Crime: An Evolutionary Arms Race. *ITNOW*, 58(3):38–39, Sept. 2016. 41

[633] M. J. Rizzo and M. Dold. Knightian uncertainty: Through a Jamesian window. *Cambridge Journal of Economics*, 45(5):967–988, Sept. 2021. 63

[634] B. Roach. A Primer on Multinational Corporations. In A. D. Chandler and B. Mazlish, editors, *Leviathans: Multinational Corporations and the New Global History*, pages 19–44. Cambridge University Press, 2005. 218

[635] P. Robbins. 'Global Visions and Globalizing Corporations: An Analysis of Images and Texts from Fortune Global 500 Companies'. *Sociological Research Online*, 9(2):66–85, May 2004. 138

[636] J. Roberts. *The Modern Firm : Organizational Design for Performance and Growth*. Oxford University Press, Oxford, 2004. 26, 31

[637] S. Roberts, A. Secor, and M. Zook. Critical Infrastructure: Mapping the Leaky Plumbing of US Hegemony. *Antipode*, 44(1):5–9, 2012. 66

[638] R. N. Robinson and T. Baum. Work(ing) artefacts: Tools of the trade, totems or trophies? *Human Relations*, 73(2):165–189, Feb. 2020. 49, 51

[639] W. Rocha Flores, E. Antonsen, and M. Ekstedt. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43:90–110, June 2014. 21

[640] F. Rochberg. *The Heavenly Writing: Divination, Horoscopy, and Astronomy in Mesopotamian Culture*. Cambridge University Press, 2004. 180

[641] P. Roe. The 'Value' of Positive Security. *Review of International Studies*, 34(4):777–794, 2008. 34

[642] P. Rogaway. Practice-Oriented Provable Security and the Social Construction of Cryptography. *IEEE Security & Privacy*, 14(6):10–17, Nov. 2016. 35

[643] P. Rohmeyer and J. L. Bayuk. How Do I Manage This? In *Financial Cybersecurity Risk Management*, pages 125–156. Springer, 2019. 28

[644] Y. Rottenstreich and C. K. Hsee. Money, Kisses, and Electric Shocks: On the Affective Psychology of Risk. *Psychological Science*, 12(3):185–190, May 2001. 69, 72, 76

[645] J.-J. Rousseau. *The Social Contract*. Penguin Books, 1968 (1762). 216

[646] M. Roussy and M. Rodrigue. Internal Audit: Is the 'Third Line of Defense' Effective as a Form of Governance? An Exploratory Study of the Impression Management Techniques Chief Audit Executives Use in Their Annual Accountability to the Audit Committee. *Journal of Business Ethics*, 151(3):853–869, Sept. 2018. 28

[647] N. Rovnick. Cyber attack hits sales at Reckitt Benckiser — Financial Times. 68

[648] N. Rowe. Researcher as storyteller and performer: Parallels with playback theatre. In *Reflexivity*. Wiley-Blackwell, Apr. 2008. 110

[649] L. Rowlands and J. Handy. An addictive environment: New Zealand film production workers' subjective experiences of project-based labour. *Human Relations*, 65(5):657–680, May 2012. 175, 184

[650] Royal Society (Great Britain). *Risk: Analysis, Perception and Management*. Royal Society, 1992. 66

[651] R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. Cano. A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). In *2017 International Conference on Information Systems and Computer Science (INCISCOS)*, pages 253–259, Nov. 2017. 28

[652] N. S. Safa, R. Von Solms, and S. Furnell. Information security policy compliance model in organizations. *Computers & Security*, 56:70–82, Feb. 2016. 19, 21, 23

[653] J. Saldaña. *The Coding Manual for Qualitative Researchers*. SAGE Publications Ltd, 3rd edition, 2016. 10, 111, 113, 158, 232, 314, 321, 322, 323, 333

[654] M. P. Sallos, A. Garcia-Perez, D. Bedford, and B. Orlando. Strategy and organisational cybersecurity: A knowledge-problem perspective. *Journal of Intellectual Capital*, 20(4):581–597, Jan. 2019. 84

[655] M. B. Salter. *Barbarians and Civilization in International Relations*. Pluto Press, 2002. 57

[656] D. Sarathchandra, K. Haltinner, and N. Lichtenberg. College Students' Cybersecurity Risk Perceptions, Awareness, and Practices. In *2016 Cybersecurity Symposium (CYBERSEC)*, pages 68–73, Apr. 2016. 69, 70

[657] M. A. Sasse, S. Brostoff, and D. Weirich. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, 19(3):122–131, 2001. 22

[658] B. Saunders, J. Kitzinger, and C. Kitzinger. Anonymising interview data: Challenges and compromise in practice. *Qualitative Research*, 15(5):616–632, Oct. 2015. 119

[659] B. Saunders, J. Kitzinger, and C. Kitzinger. Participant Anonymity in the Internet Age: From Theory to Practice. *Qualitative Research in Psychology*, 12(2):125–137, Apr. 2015. 120

[660] B. Saunders, J. Sim, T. Kingstone, S. Baker, J. Waterfield, B. Bartlam, H. Burroughs, and C. Jinks. Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, 52(4):1893–1907, July 2018. 94

[661] A. Sayer. Making Our Way Through the World: Human Reflexivity and Social Mobility. By Margaret S. Archer. *Journal of Critical Realism*, 8(1):113–123, May 2009. 99

[662] D. Schatz and R. Bashroush. The impact of repeated data breach events on organisations' market value. *Information and Computer Security*, 24(1):73–92, Feb. 2016. 13

[663] S. Schinagl, A. Shahim, and S. Khapova. Paradoxical tensions in the implementation of digital security governance: Toward an ambidextrous approach to governing digital security. *Computers & Security*, 122:102903, Nov. 2022. 19, 20, 23

[664] B. Schneier. *Beyond Fear : Thinking Sensibly about Security in an Uncertain World*. New York : Copernicus Books, New York, 2003. 102, 109

[665] B. Schneier. The Psychology of Security. In *First International Conference on Cryptology in Africa Casablanca, Morocco, June 11-14, 2008 Proceedings*, page 30. Springer-Verlag Berlin Heidelberg, 2008. 102, 109

[666] M. Schwaninger and C. Scheef. A Test of the Viable System Model: Theoretical Claim vs. Empirical Evidence. *Cybernetics and Systems*, 47(7):544–569, Oct. 2016. 65

[667] C. R. Scott. Anonymity in Applied Communication Research: Tensions Between IRBs, Researchers, and Human Subjects. *Journal of Applied Communication Research*, 33(3):242–257, Aug. 2005. 119

[668] J. C. Scott. *Domination and the Arts of Resistance: Hidden Transcripts*. New Haven: Yale University Press, New Haven, 1990. 42, 178

[669] C. Seale. *The Quality of Qualitative Research*. Introducing Qualitative Research. SAGE Publications Ltd, 2000 (1999). 82, 90, 94, 112, 113, 118, 120, 338

[670] J. M. A. Servan. *Discours Sur l'administration de La Justice Criminelle*. 1768. 229

[671] S. Shapin and S. Schaffer. *Leviathan and the Air-Pump: Hobbes, Boyle, and the Experimental Life*. Princeton University Press, 2011. 14

[672] S. Sharwood. Trump fires cybersecurity boss Chris Krebs for doing his job: Securing the election and telling the truth about it. https://www.theregister.com/2020/11/18/trump_fires_krebs/. 180, 182

[673] J. Shires. Enacting Expertise: Ritual and Risk in Cybersecurity. *Politics and Governance*, 6(2):31–40, June 2018. 16, 35

[674] J. Shires. Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy*, 41(1):82–107, Jan. 2020. 40

[675] J. L. Short and M. W. Toffel. Making Self-Regulation More Than Merely Symbolic: The Critical Role of the Legal Environment. *Administrative Science Quarterly*, 55(3):361–396, 2010. 30

[676] J. Shotter and K. Gergen. Series blurb. In T. R. Sarbin and J. I. Kitsuse, editors, *Constructing the Social*. Sage Publications, 1994. 83

[677] P. Shrivastava. Ecocentric Management for a Risk Society. *The Academy of Management Review*, 20(1):118–137, 1995. 63

[678] H. Shrobe, D. L. Shrier, and A. Pentland. Conclusion. In *New Solutions for Cybersecurity*, pages 477–482. MIT Press, 2018. 219

[679] J. Shropshire, M. Warkentin, and S. Sharma. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49:177–191, Mar. 2015. 23

[680] R. Shumba, K. Ferguson-Boucher, E. Sweedyk, C. Taylor, G. Franklin, C. Turner, C. Sande, G. Acholonu, R. Bace, and L. Hall. Cybersecurity, Women and Minorities: Findings and Recommendations from a Preliminary Investigation. In *Proceedings of the ITiCSE Working Group Reports Conference on Innovation and Technology in Computer Science Education-working Group Reports*, ITiCSE -WGR '13, pages 1–14, New York, NY, USA, 2013. ACM. 98

[681] H. Siadati, S. Palka, A. Siegel, and D. McCoy. Measuring the Effectiveness of Embedded Phishing Exercises. In *10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17)*, 2017. 186

[682] M. Sillic. Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the Shadow IT context. *Computers & Security*, 80:108–119, Jan. 2019. 22

[683] J. Sim, B. Saunders, J. Waterfield, and T. Kingstone. Can sample size in qualitative research be determined a priori? *International Journal of Social Research Methodology*, 21(5):619–634, Sept. 2018. 93

[684] S. Simon and M. de Goede. Cybersecurity, Bureaucratic Vitalism and European Emergency. *Theory, Culture & Society*, 32(2):79–106, Mar. 2015. 230

[685] D. Sims. Living a Story and Storying a Life: A Narrative Understanding of Distributed Self. In A. Pullen and S. Linstead, editors, *Organization and Identity*, pages 86–104. Routledge, 2005. 47, 157, 159, 183, 184

[686] D. Sims. You Bastard: A Narrative Exploration of the Experience of Indignation within Organizations. *Organization Studies*, 26(11):1625–1640, Nov. 2005. 56, 175, 229

[687] A. N. Singh, A. Picot, J. Kranz, M. P. Gupta, and A. Ojha. Information Security Management (ISM) Practices: Lessons from Select Cases from India and

Germany. *Global Journal of Flexible Systems Management*, 14(4):225–239, Dec. 2013. 15, 19, 101

[688] M. Singh. Trump fires director of US cybersecurity agency that refuted voter fraud claims. *The Guardian*, Nov. 2020. 180, 182

[689] M. Siponen, M. Adam Mahmood, and S. Pahnila. Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2):217–224, Mar. 2014. 22

[690] M. Siponen and R. Willison. Information security management standards: Problems and solutions. *Information & Management*, 46(5):267–270, June 2009. 20

[691] M. T. Siponen. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1):31–41, Mar. 2000. 22, 23, 25

[692] G. P. Siroli. Considerations on the Cyber Domain as the New Worldwide Battlefield. *The International Spectator*, 53(2):111–123, Apr. 2018. 41, 44

[693] K. Sköldberg. Tales of Change: Public Administration Reform and Narrative Mode. *Organization Science*, 5(2):219–238, 1994. 37, 47

[694] B. D. Slife. Taking Practice Seriously: Toward a Relational Ontology. *Journal of theoretical and philosophical psychology*, 24(2):157–178, 2004. 53, 54

[695] P. Slovic. The Psychology of risk. *Saúde e Sociedade*, 19(4):731–747, Dec. 2010. 62, 68, 69, 76, 108

[696] P. Slovic, M. L. Finucane, E. Peters, and D. G. MacGregor. Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality. *Risk Analysis*, 24(2):311–322, 2004. 69, 74

[697] P. Slovic, D. Griffin, and A. Tversky. Compatibility effects in judgment and choice. In *Insights in Decision Making: A Tribute to Hillel J. Einhorn*, pages 5–27. 1990. 74

[698] A. Smith. Do you believe in ethics? Latour and Ihde in the trenches of the science wars (or: Watch out, Latour, Ihde's got a gun). *Chasing technoscience: Matrix for materiality*, pages 182–194, 2003. 32

[699] B. Smith. Narrative analysis. In E. Lyons and A. Coyle, editors, *Analysing Qualitative Data in Psychology*, pages 202–221. Sage, London, second edition, 2016. 84, 86

[700] C. Smith and T. Elger. Critical Realism and Interviewing Subjects. In P. Edwards, J. O'Mahoney, and S. Vincent, editors, *Studying Organizations Using Critical Realism: A Practical Guide*, pages 109–131. Oxford University Press, Oxford, Jan. 2014. 83, 85

[701] G. M. Smith. Into Cerberus' Lair: Bringing the Idea of Security to Light. *The British Journal of Politics and International Relations*, 7(4):485–507, Nov. 2005. 42, 324, 326

[702] N. C. Smith, S. S. Simpson, and C.-Y. Huang. Why Managers Fail to Do the Right Thing: An Empirical Study of Unethical and Illegal Conduct. *Business Ethics Quarterly*, 17(4):633–667, 2007. 23

[703] P. Smith. *Discerning the Subject.* Minneapolis : University of Minnesota Press, Minneapolis, 1988. 50

[704] S. Snook and R. Khurana. Studying Elites in Institutions. In K. D. Elsbach and R. M. Kramer, editors, *Handbook of Qualitative Organisational Research: Innovative Pathways and Methods*, pages 54–65. Routledge, 2016. 101

[705] D. A. Snow and L. Anderson. Identity Work Among the Homeless: The Verbal Construction and Avowal of Personal Identities. *American Journal of Sociology*, 92(6):1336–1371, 1987. 45, 140, 141

[706] J.-Y. Son. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, 48(7):296–302, Oct. 2011. 21, 23

[707] M. Spence. Job Market Signaling. *The Quarterly Journal of Economics*, 87(3):355–374, 1973. 138

[708] G. C. Spivak. *The Post-Colonial Critic: Interviews, Strategies, Dialogues.* Taylor & Francis, 2014. 161

[709] G. staff and agencies. US hospital systems facing 'imminent' threat of cyber attacks, FBI warns. http://www.theguardian.com/society/2020/oct/28/us-healthcare-system-cyber-attacks-fbi, Oct. 2020. 68

[710] T. Stafford. Consumer apathy and the emerging revenue model of the internet: The economic case for spyware. *Journal of Electronic Commerce in Organizations*, 3(4):1–4, 2005. 71, 206

[711] T. F. Stafford and R. Poston. Online Security Threats and Computer User Intentions. *Computer*, 43(1):58–64, Jan. 2010. 206

[712] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton. Analysis of end user security behaviors. *Computers & Security*, 24(2):124–133, Mar. 2005. 40

[713] J. Starobinski and D. O. Via. The Struggle with Legion: A Literary Analysis of Mark 5: 1-20. *New Literary History*, 4(2):331–356, 1973. 179

[714] B. J. Steele. Ontological Security and the Power of Self-Identity: British Neutrality and the American Civil War. *Review of International Studies*, 31(3):519–540, 2005. 34

[715] S. Steele and C. Wargo. An Introduction to Insider Threat Management. *Information Systems Security*, 16(1):23–33, Mar. 2007. 24

[716] T. Stevens. *Cyber Security and the Politics of Time*. Cambridge University Press, 2016. 14, 16, 35, 39, 43, 213, 214, 219, 220, 222, 234

[717] S. Stewart. *Media Training 101: A Guide to Meeting the Press*. Wiley, 2003. 110

[718] D. W. Straub. Effective IS Security: An Empirical Study. *Information Systems Research*, 1(3):255–276, 1990. 24

[719] M. C. Suchman. Managing Legitimacy: Strategic and Institutional Approaches. *The Academy of Management Review*, 20(3):571–610, 1995. 51, 52, 143

[720] E. Sugiura, L. Lewis, and A. Slodkowski. Toyota to shut down Japanese plants after supplier hit by cyber attack. *Financial Times*, Feb. 2022. 68

[721] M. Taddeo and L. Floridi. Regulate artificial intelligence to avert cyber arms race. *Nature*, 556(7701):296, Apr. 2018. 41

[722] P. A. Talbot. Corporate Generals: The Military Metaphor of Strategy. *Irish Journal of Management*, 24(2):1–10, Oct. 2003. 55

[723] J. Taylor. Australia's anti-encryption laws being used to bypass journalist protections, expert says. *The Guardian*, July 2019. 228

[724] S. E. Taylor and J. D. Brown. Illusion and well-being: A social psychological perspective on mental health. *Psychological Bulletin*, 103(2):193–210, Mar. 1988. 135

[725] P. ten Have. Methodological issues in Conversation Analysis. *BMS: Bulletin of Sociological Methodology / Bulletin de Méthodologie Sociologique*, (27):23–51, 1990. 105

[726] M. A. Terlizzi, F. d. S. Meirelles, and M. A. Viegas Cortez da Cunha. Behavior of Brazilian Banks Employees on Facebook and the Cybersecurity Governance. *Journal of Applied Security Research*, 12(2):224–252, Apr. 2017. 31

[727] S. Thalmann, D. Bachlechner, L. Demetz, and R. Maier. Challenges in Cross-Organizational Security Management. In *2012 45th Hawaii International Conference on System Sciences*, pages 5480–5489, Jan. 2012. 21

[728] D. Thomas. TalkTalk chief signals change after cyber attack. *Financial Times*, Mar. 2016. 29, 46

[729] R. Thomas. Is the Viable System Model of Organization inimical to the concept of human freedom? *Journal of Organisational Transformation & Social Change*, 3(1):69–83, 2006. 65

[730] R. Thomas and A. Linstead. Losing the Plot? Middle Managers and Identity. *Organization*, 9(1):71–93, Feb. 2002. 53

[731] S. M. Thompson. Insider risk management – who's the boss? https://www.csoonline.com/article/3487297/insider-risk-management-whos-the-boss.html, Dec. 2019. 175, 176

[732] I. Thomson. Low Barr: Don't give me that crap about security, just put the backdoors in the encryption, roars US Attorney General. https://www.theregister.co.uk/2019/07/23/us_encryption_backdoor/, 2019. 228

[733] K. Thomson and J. van Niekerk. Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security*, 20(1):39–46, Mar. 2012. 21, 71, 206

[734] T. Thornborrow and A. D. Brown. 'Being Regimented': Aspiration, Discipline and Identity Work in the British Parachute Regiment. *Organization Studies*, 30(4):355–376, Apr. 2009. 55, 56

[735] J. Tidy. How hackers are preying on coronavirus fears. *BBC News*, Mar. 2020. 39, 108

[736] E. Tikk-Ringas. International Cyber Norms Dialogue as an Exercise of Normative Power. *Georgetown Journal of International Affairs*, 17(3):47–59, 2016. 42

[737] T. Todorov. *The Poetics of Prose*. Ithaca, N.Y. : Cornell University Press, Ithaca, N.Y., 1977. 47

[738] W. A. Tol, B. A. Kohrt, M. J. D. Jordans, S. B. Thapa, J. Pettigrew, N. Upadhaya, and J. T. V. M. de Jong. Political violence and mental health: A multi-disciplinary review of the literature on Nepal. *Social Science & Medicine*, 70(1):35–44, Jan. 2010. 112

[739] M. Tolich. Internal Confidentiality: When Confidentiality Assurances Fail Relational Informants. *Qualitative Sociology*, 27(1):101–106, Mar. 2004. 119

[740] L. J. Trautman and P. C. Ormerod. Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach. *American University Law Review*, 66:1231–1292, 2016. 205

[741] Z. Tu and Y. Yuan. Critical Success Factors Analysis on Effective Information Security Management: A Literature Review. *Information Systems Security*, page 13, 2014. 24

[742] M. L. Tushman. A Political Approach to Organizations: A Review and Rationale. *The Academy of Management Review*, 2(2):206–216, 1977. 64, 65

[743] A. Tversky and D. Kahneman. Judgment under Uncertainty: Heuristics and Biases. *Science*, 185(4157):1124–1131, Sept. 1974. 76, 135

[744] A. Tversky and D. Kahneman. Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty*, 5(4):297–323, Oct. 1992. 74

[745] UK Government. Regulation of Investigatory Powers Act 2000, 2000. 42, 220

[746] UK Government. Terrorism Act 2006, 2006. 220

[747] UK Government. National Cyber Security Strategy 2016-2021, 2016. 138, 207, 227

[748] N. M. Underberg. Soothsayer (Diviner, Oracle, Etc.): Motif D1712. In *Archetypes and Motifs in Folklore and Literature: A Handbook*, pages 147–153. Routledge, 2017. 179, 180, 182

[749] J. Underwood and C. Rhodes. A qualitative investigation of hospital visitors' experiences using the analytic lens of liminality: Informing nursing practice and policy. *Nursing Inquiry*, 25(3):e12239, 2018. 111

[750] B. Valeriano and R. C. Maness. International Relations Theory and Cyber Security. *The Oxford Handbook of International Political Theory*, page 259, 2018. 42

[751] R. Van der Kleij, G. Kleinhuis, and H. Young. Computer Security Incident Response Team Effectiveness: A Needs Assessment. *Frontiers in Psychology*, 8, Dec. 2017. 101

[752] J. van Erp. New governance of corporate cybersecurity: A case study of the petrochemical industry in the Port of Rotterdam. *Crime, Law and Social Change*, 68(1):75–93, Sept. 2017. 30

[753] T. Van Leeuwen and R. Wodak. Legitimizing Immigration Control: A Discourse-Historical Analysis. *Discourse Studies*, 1(1):83–118, Feb. 1999. 52

[754] J. F. Van Niekerk and R. Von Solms. Information security culture: A management perspective. *Computers & Security*, 29(4):476–486, June 2010. 22, 66

[755] C. Vásquez and R. D. Benavente. Revisiting Autopoiesis. *Management Communication Quarterly*, Vol. 30(2):269–274, 2016. 65

[756] J. Veen and S. Boeke. No Backdoors: Investigating the Dutch Standpoint on Encryption. *Policy & Internet*, 12(4):503–524, 2020. 43

[757] A. Vishwanath, L. S. Neo, P. Goh, S. Lee, M. Khader, G. Ong, and J. Chin. Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, 128:113160, Jan. 2020. 40

[758] C. von Clausewitz. *On War*. N. Trübner & Company, London, 1873. 44

[759] R. von Solms and J. van Niekerk. From information security to cyber security. *Computers & Security*, 38:97–102, Oct. 2013. 13

[760] R. Von Solms and C. Vermeulen. The information security management toolbox – taking the pain out of security management. *Information Management & Computer Security*, 10(3):119–125, Aug. 2002. 31

[761] D. Voreacos, K. Chiglinsky, and R. Griffin. Merck Cyberattack's $1.3 Billion Question: Was It an Act of War? *Bloomberg.com*, Dec. 2019. 40

[762] C. Vroom and R. von Solms. Towards information security behavioural compliance. *Computers & Security*, 23(3):191–198, May 2004. 25

[763] O. Waever. Securitization and desecuritization. In R. D. Lipschutz, editor, *On Security*, pages 46–86. Columbia University Press, New York, 1995. 35

[764] O. Waever, B. Buzan, M. Kelstrup, and P. Lemaitre. *Identity, Migration, and the New Security Agenda in Europe*. Pinter Publishers Ltd, London, 1993. 34

[765] G. Walford. Research ethical guidelines and anonymity. *International Journal of Research & Method in Education*, 28(1):83–93, Apr. 2005. 119

[766] C. Walker. Cyber-Terrorism: Legal Principle and the Law in the United Kingdom. *Penn State Law Review*, 110:625–665, 2006. 220

[767] O. Walker. Why cyber risks are getting even more important for big banks. *Financial Times*, May 2021. 201

[768] R. B. J. Walker. *Inside/Outside: International Relations as Political Theory*. Cambridge University Press, 1993. 231, 232

[769] S. Walklate. Risk and criminal victimization: A modernist dilemma? *The British Journal of Criminology*, 37(1):35–45, 1997. 61, 62, 76, 96, 176, 201

[770] D. S. Wall. CYBERCRIME AND THE CULTURE OF FEAR: Social science fiction(s) and the production of knowledge about cybercrime. *Information, Communication & Society*, 11(6):861–884, Sept. 2008. 39

[771] B. Warf and E. Fekete. Relational geographies of cyberterrorism and cyberwar. *Space and Polity*, 20(2):143–157, May 2016. 40, 44

[772] M. Weber. *The Theory of Social and Economic Organization*. Free Press of Glencoe, 1964. 146

[773] P. Weill and J. W. Ross. *IT Governance : How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business Press, Boston, Mass., 2004. 31

[774] B. Weiner. A cognitive (attribution)-emotion-action model of motivated behavior: An analysis of judgments of help-giving. *Journal of Personality and Social Psychology*, 39(2):186–200, Aug. 1980. 68, 69

[775] C. Welch, R. Marschan-Piekkari, H. Penttinen, and M. Tahvanainen. Corporate elites as informants in qualitative international business research. *International Business Review*, 11(5):611–628, Oct. 2002. 101

[776] R. Werlinger, K. Hawkey, and K. Beznosov. An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, 17(1):4–19, Mar. 2009. 19, 21

[777] R. Werlinger, K. Hawkey, D. Botta, and K. Beznosov. Security practitioners in context: Their activities and interactions with other stakeholders within organizations. *International Journal of Human-Computer Studies*, 67(7):584–606, July 2009. 15, 19, 20, 21, 101

[778] J. R. Westby. Governance of Cybersecurity: 2015 Report, 2015. 90

[779] P. J. Whalen. The uncertainty of it all. *Trends in Cognitive Sciences*, 11(12):499–500, Dec. 2007. 68

[780] W. Whitely, T. W. Dougherty, and G. F. Dreher. Relationship of Career Mentoring and Socioeconomic Origin to Managers' and Professionals' Early Career Progress. *The Academy of Management Journal*, 34(2):331–351, 1991. 99

[781] M. Wikgren. Critical realism as a philosophy and social theory in information science? *Journal of Documentation*, Feb. 2005. 82

[782] H. L. Wilensky. *Organizational Intelligence: Knowledge and Policy in Government and Industry*. Quid Pro, LLC, 2015. 169

[783] R. Wiles, G. Crow, S. Heath, and V. Charles. The Management of Confidentiality and Anonymity in Social Research. *International Journal of Social Research Methodology*, 11(5):417–428, Dec. 2008. 119

[784] C. Wilkinson and J. Dare. Shades of Grey: The Need for a Multi-Disciplinary Approach to Research Investigating Alcohol and Ageing. *Journal of Public Health Research*, 3(1):jphr.2014.180, Mar. 2014. 112

[785] I. Wilkinson. Social Theories of Risk Perception: At Once Indispensable and Insufficient. *Current Sociology*, 49(1):1–22, Jan. 2001. 67

[786] M. C. Williams. Hobbes and International Relations: A Reconsideration. *International Organization*, 50(2):213–236, 1996. 225, 234, 235

[787] D. Winder. Facebook Privacy Update: Mark Zuckerberg's Response To Cambridge Analytica Scandal One Year On. https://www.forbes.com/sites/daveywinder/2019/03/17/facebook-privacy-update-mark-zuckerbergs-response-to-cambridge-analytica-scandal-one-year-on/. 58

[788] S. S. Wolin. *Hobbes and the Epic Tradition of Political Theory.* Los Angeles : William Andrews Clark Memorial Library, University of California, Los Angeles, 1970. 217

[789] D. Woods, I. Agrafiotis, J. R. C. Nurse, and S. Creese. Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services and Applications*, 8(1):8, July 2017. 21

[790] J. Woodward. *Industrial Organization: Theory and Practice.* Oxford University Press, 1965. 64

[791] F. Xue. Attacking antivirus. In *Black Hat Europe Conference*, 2008. 198

[792] A. Yazdanmehr and J. Wang. Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, 92:36–46, Dec. 2016. 23, 24

[793] S. Ybema, T. Keenoy, C. Oswick, A. Beverungen, N. Ellis, and I. Sabelis. Articulating identities. *Human Relations*, 62(3):299–322, Mar. 2009. 45, 49, 52, 54, 57, 143, 177

[794] M. Zachariadis, S. Scott, and M. Barrett. Methodological Implications of Critical Realism for Mixed-Methods Research. *MIS Quarterly*, 37(3):855–879, 2013. 83

[795] A. Zanutto, B. Shreeve, K. Follis, and A. Rashid. The Shadow Warriors: In the no man's land between industrial control systems and enterprise {IT} systems. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 2017. 20, 24, 176

[796] M. Zhivitskaya. *The Practice of Risk Oversight since the Global Financial Crisis: Closing the Stable Door?* PhD thesis, The London School of Economics and Political Science (LSE), Sept. 2015. 28, 71, 206

[797] M. J. Zimmerman. Is moral obligation objective or subjective? *Utilitas*, 18(4):329–361, 2006. 40, 235

[798] H. Zuckerman. *Scientific Elite: Nobel Laureates in the United States.* Transaction Publishers, 1977. 87, 118

Appendix A

Methodological findings

A.1 Introduction

In this Appendix, I detail findings from the study that are methodological in nature. These do not relate to the overarching research question, and hence were not included in Chapters 4, 5 and 6. However, they may be of interest for future scholarship, and provide further insight into the research that underpins the thesis.

A.2 Methodological findings

A.2.1 Interaction between interviewer and participants

The analysis of the interview data resulted in different types of interactions being coded. These included physical gestures and activities, such as participants making notes, as well as indications of (bi-directional) rapport, such as laughter and other social bonding. The latter included in one case, an explicit interest in confirming that the interview had been helpful (CEO2), as well as a CISO (CISO12) asking me "how did that make you feel?" after I mentioned one of my experiences as a CISO. I also coded notable behaviours such as interruptions. The latter was particularly prevalent with one participant (CEO1), who interrupted me on a number of occasions, but, in one case, I interrupted a different participant (CEO2), which I also coded. At the time, I considered the latter to be related to my excitement regarding the conversation we were having, and the level of rapport we shared, and the former to be domineering and discourteous, but I acknowledge the bias that is likely in that value judgement.[1]

I now briefly describe some other notable interactions.

[1] All such instances were coded in the same way, as interruptions, without a value judgement being assigned.

Quid pro quo. Quid pro quo was indicated in both directions, with me, as the interviewer, on certain occasions offering to provide future collaboration or discussion, and participants explicitly asking for information back from me. The latter was observed from both CISOs and non-CISOs, with some of these requests being more detailed than others. For example, when discussing a specific cyber-security control, CFO1 asked “I’m interested in your view”, which led to a conversation about my experiences with that control, and CEO2 and CISO9 both asked questions regarding my reporting line and the cyber-security arrangements at my employer.

Categorisation of interviewer by participant. In several cases, I was explicitly categorised by the participants as a security professional. This included being referred to as “people like you” (CEO2) and comments such as “you’re probably familiar with it” (CISO13) and “I don’t need to tell you” (CISO14). This indicates that a level of knowledge and experience on my behalf was being assumed by these participants, and suggests that a different interviewer is likely to have had different interactions with these participants. CISO11 described how it was “a lot easier to have a discussion with a fellow CISO than it is with perhaps others”. This indicated not just a categorisation of myself as a “fellow CISO” but also highlights the level of comfort that the participant had in taking part in a research interview with someone who performed the same role.

In some cases, a level of equivalence was articulated, such as CIO1 describing how a security-related topic was “understood but not to the level that you or I would understand that”. The most common indications of equivalence were from the CISO participants, with examples such as “I think we have a very similar experience” (CISO2) and “I’m sure your experience is similar” (CISO4). In one case, my specific professional experience was also called out by one participant who stated “I know you’ve worked in the [redacted] sector”(CISO5). This suggests both a level of familiarity with me as an individual but also an assumed knowledge associated with that work experience, which not only contributed to rapport but also affected the language and terminology used by the participant.

In some cases, I noted a more implicit categorisation occurring, which I coded using a subtext code [653, p. 146] of ‘one of us’. These included references to security industry-specific terms or abbreviations which the participant did not explain, assuming I understood what they were referring to, as well as more rapport-related statements such as “fun and games” (CISO6) and “I won’t go into why we did that [laughter]” (CISO8). These indicated to me that I was being both categorised (as a security professional) and trusted (as a *fellow* security professional). In one case, this trust was called out explicitly, where CISO2 stated “yeah, if I can’t trust you! [laughs]”, and also indicated by sharing of sensitive information, such as specifics regarding security incidents and security controls. These interactions suggest that I was not only being trusted as an individual, but that the role I performed, and the identity I inhabited, resulted in me being trusted with such knowledge. A different interviewer may have had different results.

A.2.2 Impact of the interviews

There were indications that the interviews had a beneficial impact on the participants. In a number of cases, participants expressed gratitude for the interviews having prompted their own reflexivity. This included CFO2 who stated that the interview had “given **me** some food for thought [laughter] ... so thank you very much for prompting it” (emphasis captured in transcript) and CISO15 who noted “oh this is good therapy Joseph thank you [laughs]”. CISO12 described the interview as “very thought provoking” and stated that they were going to

> “use some of the points we raised [in the interview] to ask questions from my exec[utive]s, but also to perhaps try to put into words the value that we provide to to the business ... actually we don’t do that in our roles do we, we don’t ask, you know, ‘what do you think about the role’, ‘what do you see my role being’ and we don’t really ask the question of ‘what do you think would [happen] if my role didn’t exist’ ”.

Earlier in the interview, the same participant had taken down some notes of questions to ask of their executives, again indicating that there was benefit to them arising from the interview. A similar impact was noted from CFO2 who described how they would

> “actually go back to my home organization and make sure we all have a common understanding of what that role [i.e., the CISO] is and sometimes asking that very obvious question is extremely helpful to just [understand] ... have we done a good job on that and how does that individual feel”.

Most of the indications of positive impact were prompted by a question I asked participants at the end of the interview regarding how they had found the experience, but a number were unprompted.

A number of participants indicated that the interviews had motivated them to reflect, both upon aspects of cyber security and their own roles. This included CISO12 questioning whether they should attend all future governance meetings (“should I be there every time?”) and CIO1 describing how they “rarely reflect on on what we’ve done in the past”. CEO2 described how the interview had caused them to “reflect on it [cyber security] ... it would be a bigger issue than perhaps I'd previously thought at this point" and how they "hadn't thought about [a cyber-security function that didn't report into an IT function] ... but I can see why, it does make sense, otherwise people are marking their own homework aren't they?". This suggests that the participant had engaged with an aspect of the interview that not only had they not considered previously but also could potentially lead them to make changes in their own organisation.

A.2.3 Research process

Finally, I briefly summarise some general, but notable, findings relating to the research process itself.

- Two participants requested a review of any quotes utilised from their interviews prior to publication. These requests have been complied with.
- During one remote interview, a participant was interrupted by one of their colleagues sending them a message and inadvertently mentioned their name due to the notification that had appeared on their computer. Another participant was interrupted by a call from their manager which they paused the interview in order to handle.
- In one case, I noted unanticipated crossover between organisations, whereby it became apparent from the annual report analysis that one organisation shared a board member with another organisation in this study.
- Throughout the analysis stage,[2] I utilised both a thesaurus and a dictionary to help refine my thoughts. This included engaging with the etymology of certain words, which influenced my decisions around the use, and deliberate avoidance, of certain words and phrases in both coding and analysis.[3]
- A number of participants made reference to impacts on both themselves and their businesses relating to the Covid-19 pandemic. This included the level of demand they were experiencing in terms of business volumes and aspects of remote working that impacted on them personally and on the security posture of their organisations.
- A number of typographical errors were identified in multiple annual reports.

[2] And the writing up stage.

[3] This included the deliberate avoidance of 'lifting the veil', a phrase with sexual, and sexist, connotations of which I had not previously been aware.

Appendix B

Analytic diagrams

B.1 Introduction

In this Appendix, I present a number of analytic diagrams that provide a snapshot of the coding and analysis stages described in Chapter 3. These provide insight into the research conducted and the analytical rigour that has been present throughout. As with the previous diagrams in this thesis, all are included as high-resolution images that allow zooming in when accessing this document digitally, as they will be difficult to read, particularly in printed format.

B.2 Analytic diagrams

The following diagrams are intended to provide snapshots of the analytic process and indicate the rigour that was present throughout. The development of these diagrams both prompted and supplemented analytic memos, which were produced throughout the analysis phase.

B.2.1 Development of themes

Figures B.1 and B.2 were used when developing the themes highlighted in Chapter 3. They indicate the mapping between codes and categories and the themes and sub-themes established during the analysis. Each diagram was developed iteratively, with putative themes and sub-themes being proposed as a summary of the analysis that I was performing. Diagrams such as these were produced for each theme, however, only two examples are shown for reasons of space.

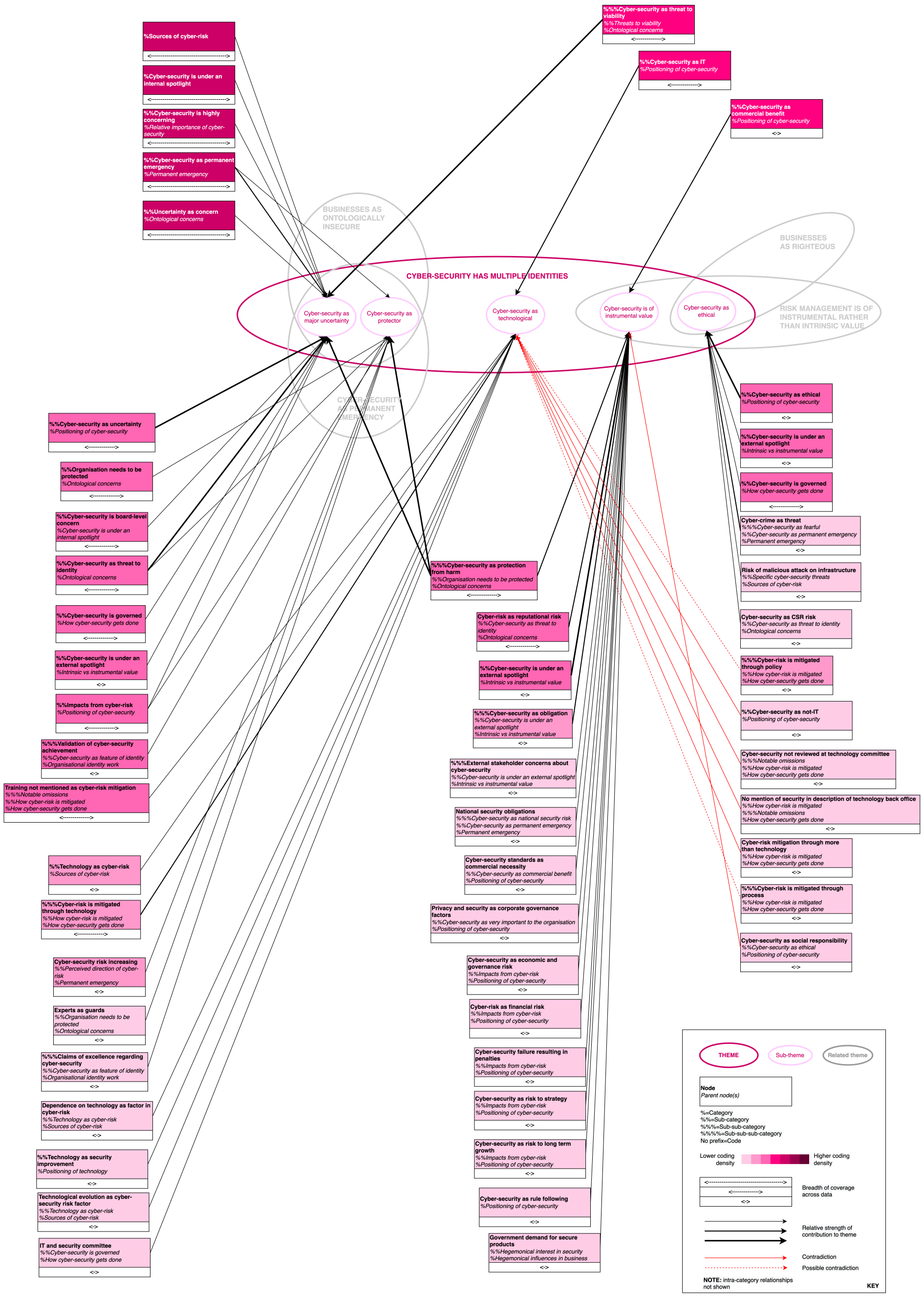

%Sources of cyber-risk
%Cyber-security is under an internal spotlight
%%Cyber-security is highly concerning
%Relative importance of cyber-security
%%Cyber-security as permanent emergency
%Permanent emergency
%%Uncertainty as concern
%Ontological concerns
%%%Cyber-security as threat to viability
%%Threats to viability
%Ontological concerns
%%Cyber-security as IT
%Positioning of cyber-security
%%Cyber-security as commercial benefit
%Positioning of cyber-security
BUSINESSES AS ONTOLOGICALLY INSECURE
BUSINESSES AS RIGHTEOUS
CYBER-SECURITY HAS MULTIPLE IDENTITIES
Cyber-security as major uncertainty
Cyber-security as protector
Cyber-security as technological
Cyber-security is of instrumental value
Cyber-security as ethical
RISK MANAGEMENT IS OF INSTRUMENTAL RATHER THAN INTRINSIC VALUE
CYBER-SECURITY AS PERMANENT EMERGENCY
%%Cyber-security as uncertainty
%Positioning of cyber-security
%%Organisation needs to be protected
%Ontological concerns
%%Cyber-security is board-level concern
%Cyber-security is under an internal spotlight
%%Cyber-security as threat to identity
%Ontological concerns
%%Cyber-security is governed
%How cyber-security gets done
%%Cyber-security is under an external spotlight
%Intrinsic vs instrumental value
%%Impacts from cyber-risk
%Positioning of cyber-security
%%%Validation of cyber-security achievement
%%Cyber-security as feature of identity
%Organisational identity work
Training not mentioned as cyber-risk mitigation
%%%Notable omissions
%%How cyber-risk is mitigated
%How cyber-security gets done
%%Technology as cyber-risk
%Sources of cyber-risk
%%%Cyber-risk is mitigated through technology
%%How cyber-risk is mitigated
%How cyber-security gets done
Cyber-security risk increasing
%%Perceived direction of cyber-risk
%Permanent emergency
Experts as guards
%%Organisation needs to be protected
%Ontological concerns
%%%Claims of excellence regarding cyber-security
%%Cyber-security as feature of identity
%Organisational identity work
Dependence on technology as factor in cyber-risk
%%Technology as cyber-risk
%Sources of cyber-risk
%%Technology as security improvement
%Positioning of technology
Technological evolution as cyber-security risk factor
%%Technology as cyber-risk
%Sources of cyber-risk
IT and security committee
%%Cyber-security is governed
%How cyber-security gets done
%%%Cyber-security as protection from harm
%%Organisation needs to be protected
%Ontological concerns
Cyber-risk as reputational risk
%%Cyber-security as threat to identity
%Ontological concerns
%%Cyber-security is under an external spotlight
%Intrinsic vs instrumental value
%%%Cyber-security as obligation
%%Cyber-security is under an external spotlight
%Intrinsic vs instrumental value
%%%External stakeholder concerns about cyber-security
%%Cyber-security is under an external spotlight
%Intrinsic vs instrumental value
National security obligations
%%%Cyber-security as national security risk
%%Cyber-security as permanent emergency
%Permanent emergency
Cyber-security standards as commercial necessity
%%Cyber-security as commercial benefit
%Positioning of cyber-security
Privacy and security as corporate governance factors
%%Cyber-security as very important to the organisation
%Positioning of cyber-security
Cyber-security as economic and governance risk
%%Impacts from cyber-risk
%Positioning of cyber-security
Cyber-risk as financial risk
%%Impacts from cyber-risk
%Positioning of cyber-security
Cyber-security failure resulting in penalties
%%Impacts from cyber-risk
%Positioning of cyber-security
Cyber-security as risk to strategy
%%Impacts from cyber-risk
%Positioning of cyber-security
Cyber-security as risk to long term growth
%%Impacts from cyber-risk
%Positioning of cyber-security
Cyber-security as rule following
%Positioning of cyber-security
Government demand for secure products
%%Hegemonical interest in security
%Hegemonical influences in business
%%Cyber-security as ethical
%Positioning of cyber-security
%%Cyber-security is under an external spotlight
%Intrinsic vs instrumental value
%%Cyber-security is governed
%How cyber-security gets done
Cyber-crime as threat
%%%Cyber-security as fearful
%%Cyber-security as permanent emergency
%Permanent emergency
Risk of malicious attack on infrastructure
%%Specific cyber-security threats
%Sources of cyber-risk
Cyber-security as CSR risk
%%Cyber-security as threat to identity
%Ontological concerns
%%%Cyber-risk is mitigated through policy
%%How cyber-risk is mitigated
%How cyber-security gets done
%%Cyber-security as not-IT
%Positioning of cyber-security
Cyber-security not reviewed at technology committee
%%%Notable omissions
%%How cyber-risk is mitigated
%How cyber-security gets done
No mention of security in description of technology back office
%%How cyber-risk is mitigated
%%%Notable omissions
%How cyber-security gets done
Cyber-risk mitigation through more than technology
%%How cyber-risk is mitigated
%How cyber-security gets done
%%%Cyber-risk is mitigated through process
%%How cyber-risk is mitigated
%How cyber-security gets done
Cyber-security as social responsibility
%%Cyber-security as ethical
%Positioning of cyber-security
THEME
Sub-theme
Related theme
Node
Parent node(s)
%=Category
%%=Sub-category
%%%=Sub-sub-category
%%%%=Sub-sub-sub-category
No prefix=Code
Lower coding density
Higher coding density
Breadth of coverage across data
Relative strength of contribution to theme
Contradiction
Possible contradiction
NOTE: intra-category relationships not shown
KEY

Figure B.1: Analytic diagram indicating the linkages between codes/categories and the theme 'Cyber security has multiple identities'.

Figure B.1 demonstrates the multiplicity of codes and categories that were synthesised into the theme of 'Cyber security has multiple identities', as explored in Chapters 4, 5 and 6. This includes the relative coding densities and breadth of coverage, which were recorded and used as an input to the analysis, but were not determining factors in the development of themes. Figure B.2 indicates similar linkages used in the development of another theme.

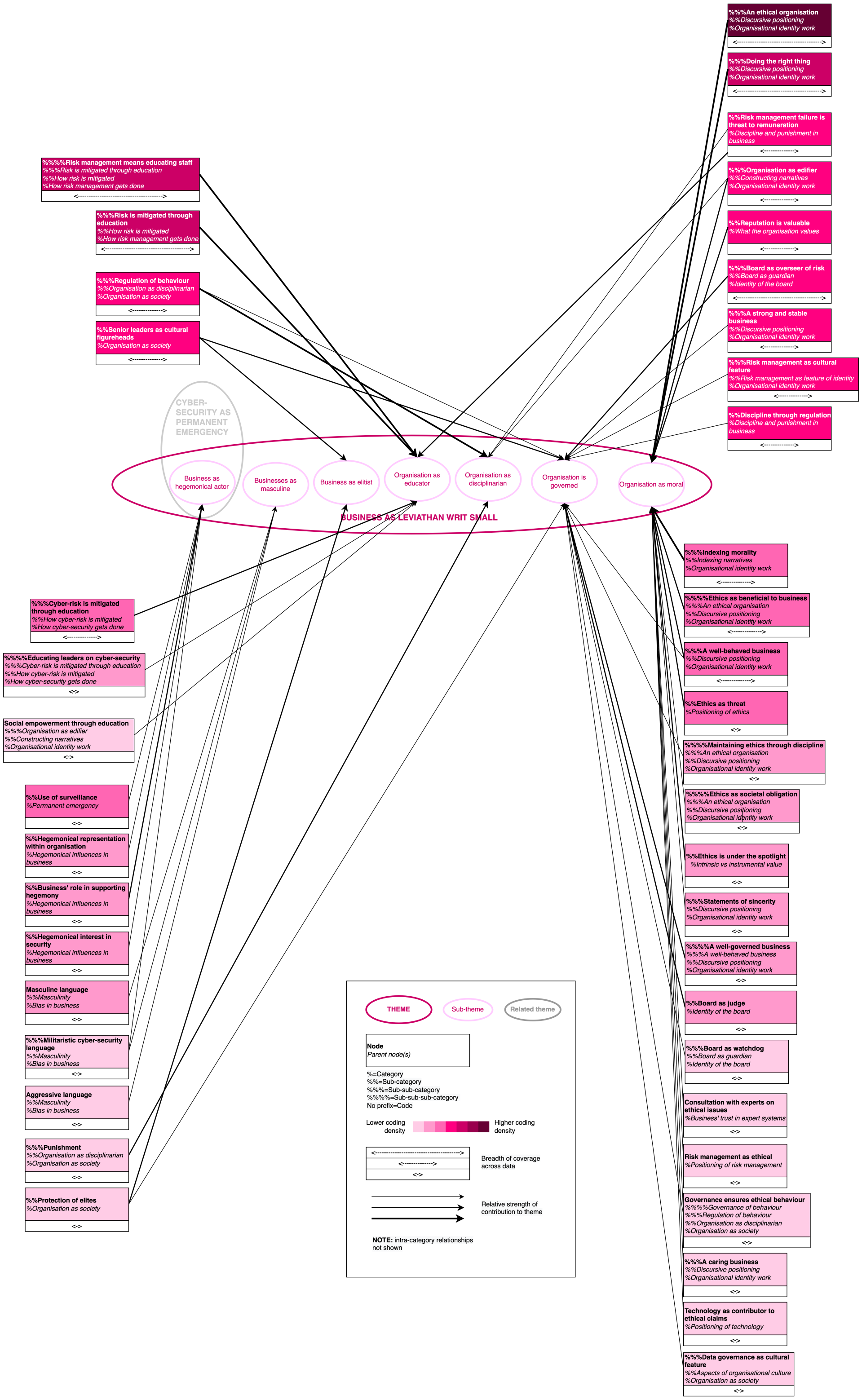

%%%An ethical organisation
%%Discursive positioning
%Organisational identity work
%%%Doing the right thing
%%Discursive positioning
%Organisational identity work
%%Risk management failure is threat to remuneration
%Discipline and punishment in business
%%%Organisation as edifier
%%Constructing narratives
%Organisational identity work
%%Reputation is valuable
%What the organisation values
%%%Board as overseer of risk
%%Board as guardian
%Identity of the board
%%%A strong and stable business
%%Discursive positioning
%Organisational identity work
%%%Risk management as cultural feature
%%Risk management as feature of identity
%Organisational identity work
%%Discipline through regulation
%Discipline and punishment in business
%%%%Risk management means educating staff
%%%Risk is mitigated through education
%%How risk is mitigated
%How risk management gets done
%%%Risk is mitigated through education
%%How risk is mitigated
%How risk management gets done
%%%Regulation of behaviour
%%Organisation as disciplinarian
%Organisation as society
%%Senior leaders as cultural figureheads
%Organisation as society
CYBER-SECURITY AS PERMANENT EMERGENCY
Business as hegemonical actor
Businesses as masculine
Business as elitist
Organisation as educator
Organisation as disciplinarian
Organisation is governed
Organisation as moral
BUSINESS AS LEVIATHAN WRIT SMALL
%%%Cyber-risk is mitigated through education
%%How cyber-risk is mitigated
%How cyber-security gets done
%%%%Educating leaders on cyber-security
%%%Cyber-risk is mitigated through education
%%How cyber-risk is mitigated
%How cyber-security gets done
Social empowerment through education
%%%Organisation as edifier
%%Constructing narratives
%Organisational identity work
%%Use of surveillance
%Permanent emergency
%%Hegemonical representation within organisation
%Hegemonical influences in business
%%Business' role in supporting hegemony
%Hegemonical influences in business
%%Hegemonical interest in security
%Hegemonical influences in business
Masculine language
%%Masculinity
%Bias in business
%%%Militaristic cyber-security language
%%Masculinity
%Bias in business
Aggressive language
%%Masculinity
%Bias in business
%%%Punishment
%%Organisation as disciplinarian
%Organisation as society
%%Protection of elites
%Organisation as society
%%%Indexing morality
%%Indexing narratives
%Organisational identity work
%%%%Ethics as beneficial to business
%%%An ethical organisation
%%Discursive positioning
%Organisational identity work
%%%A well-behaved business
%%Discursive positioning
%Organisational identity work
%%Ethics as threat
%Positioning of ethics
%%%%Maintaining ethics through discipline
%%%An ethical organisation
%%Discursive positioning
%Organisational identity work
%%%%Ethics as societal obligation
%%%An ethical organisation
%%Discursive positioning
%Organisational identity work
%%Ethics is under the spotlight
%Intrinsic vs instrumental value
%%%Statements of sincerity
%%Discursive positioning
%Organisational identity work
%%%%A well-governed business
%%%A well-behaved business
%%Discursive positioning
%Organisational identity work
%%Board as judge
%Identity of the board
%%%Board as watchdog
%%Board as guardian
%Identity of the board
Consultation with experts on ethical issues
%Business' trust in expert systems
Risk management as ethical
%Positioning of risk management
Governance ensures ethical behaviour
%%%%Governance of behaviour
%%%Regulation of behaviour
%%Organisation as disciplinarian
%Organisation as society
%%%A caring business
%%Discursive positioning
%Organisational identity work
Technology as contributor to ethical claims
%Positioning of technology
%%%Data governance as cultural feature
%%Aspects of organisational culture
%Organisation as society
THEME
Sub-theme
Related theme
Node
Parent node(s)
%=Category
%%=Sub-category
%%%=Sub-sub-category
%%%%=Sub-sub-sub-category
No prefix=Code
Lower coding density
Higher coding density
Breadth of coverage across data
Relative strength of contribution to theme
NOTE: intra-category relationships not shown

Figure B.2: Analytic diagram indicating the linkages between codes/categories and the theme ‘Business as Leviathan writ small’.

This diagram presents the codes and categories used to develop the meta-theme of 'Business as Leviathan writ small', which was discussed in Chapter 6.

B.2.2 Category relationship diagrams

During the analysis, it was apparent that there could be relationships between categories of data. These were explored using a different type of diagram, as shown in Figures B.3 and B.4, which extended a number of ideas from Saldaña [653, p. 280].[1] Figure B.3 was instrumental in the analysis of aspects of soothsaying and ontological insecurity discussed in Chapter 4.

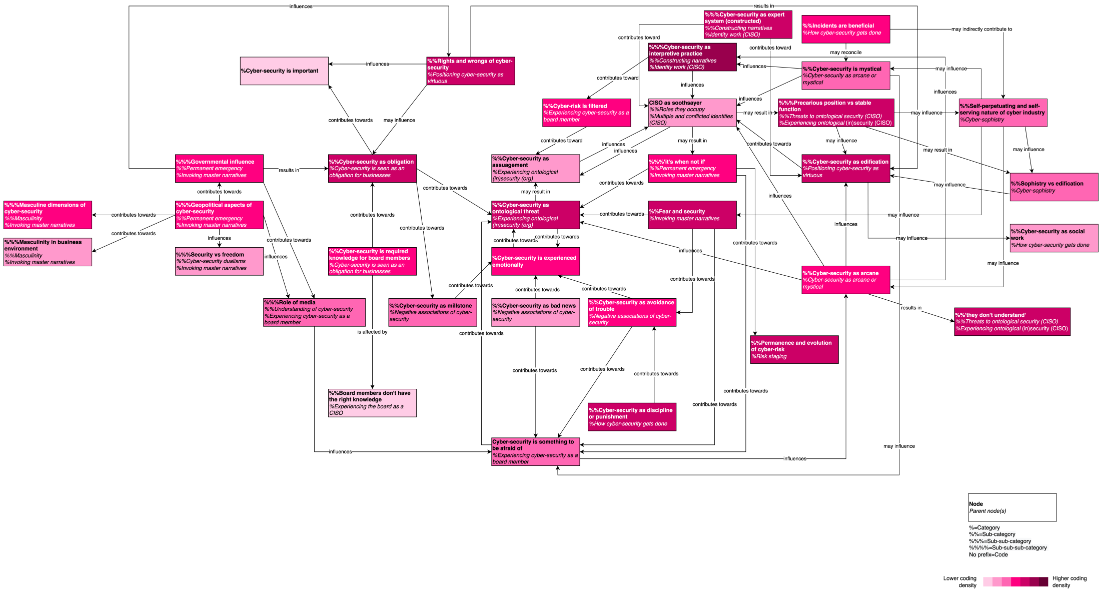

%Cyber-security is important
%%Rights and wrongs of cyber-security
%Positioning cyber-security as virtuous
%%%Governmental influence
%%Permanent emergency
%Invoking master narratives
%%Cyber-security as obligation
%Cyber-security is seen as an obligation for businesses
%%%Masculine dimensions of cyber-security
%%Masculinity
%Invoking master narratives
%%%Geopolitical aspects of cyber-security
%%Permanent emergency
%Invoking master narratives
%%%Masculinity in business environment
%%Masculinity
%Invoking master narratives
%%%Security vs freedom
%%Cyber-security dualisms
%Invoking master narratives
%%Cyber-security is required knowledge for board members
%Cyber-security is seen as an obligation for businesses
%%%Role of media
%%Understanding of cyber-security
%Experiencing cyber-security as a board member
%%Cyber-security as millstone
%Negative associations of cyber-security
%%Board members don't have the right knowledge
%Experiencing the board as a CISO
%%%Cyber-security as expert system (constructed)
%%Constructing narratives
%Identity work (CISO)
%%%Cyber-security as interpretive practice
%%Constructing narratives
%Identity work (CISO)
%%Incidents are beneficial
%How cyber-security gets done
%%Cyber-security is mystical
%Cyber-security as arcane or mystical
%%Cyber-risk is filtered
%Experiencing cyber-security as a board member
CISO as soothsayer
%%Roles they occupy
%Multiple and conflicted identities (CISO)
%%%Precarious position vs stable function
%%Threats to ontological security (CISO)
%Experiencing ontological (in)security (CISO)
%%Self-perpetuating and self-serving nature of cyber industry
%Cyber-sophistry
%%Cyber-security as assuagement
%Experiencing ontological (in)security (org)
%%%'it's when not if'
%%Permanent emergency
%Invoking master narratives
%%Cyber-security as edification
%Positioning cyber-security as virtuous
%%Sophistry vs edification
%Cyber-sophistry
%%Cyber-security as ontological threat
%Experiencing ontological (in)security (org)
%%Fear and security
%Invoking master narratives
%%Cyber-security as social work
%How cyber-security gets done
%Cyber-security is experienced emotionally
%%Cyber-security as arcane
%Cyber-security as arcane or mystical
%%'they don't understand'
%%Threats to ontological security (CISO)
%Experiencing ontological (in)security (CISO)
%%Cyber-security as bad news
%Negative associations of cyber-security
%%Cyber-security as avoidance of trouble
%Negative associations of cyber-security
%%Permanence and evolution of cyber-risk
%Risk staging
%%Cyber-security as discipline or punishment
%How cyber-security gets done
Cyber-security is something to be afraid of
%Experiencing cyber-security as a board member
influences
results in
contributes towards
contributes toward
may influence
may result in
may reconcile
may indirectly contribute to
is affected by
Node
Parent node(s)
%=Category
%%=Sub-category
%%%=Sub-sub-category
%%%%=Sub-sub-sub-category
No prefix=Code
Lower coding density
Higher coding density

Figure B.3: Analytic diagram suggesting relationships between a number of data categories.

This diagram enabled further exploration of these relationships and motivated further analytic memos based on the putative connections made. Similarly, Figure B.4 presents another set of relationships.

[1] Again, multiple diagrams were produced but only two examples are shown below.

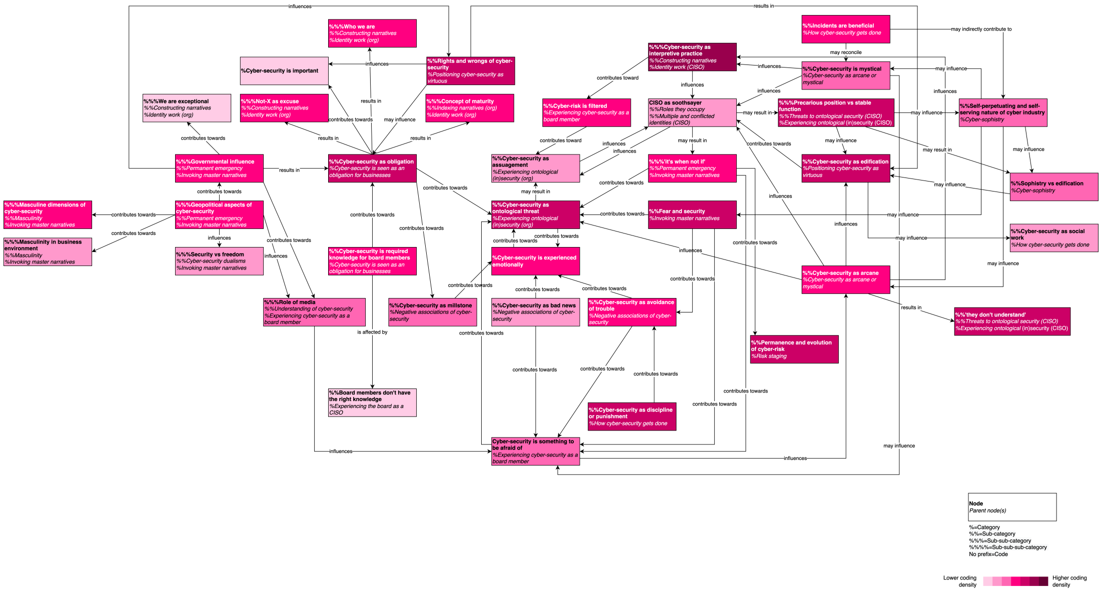

%%%Who we are
%%Constructing narratives
%Identity work (org)
%Cyber-security is important
%%Rights and wrongs of cyber-security
%Positioning cyber-security as virtuous
%%%We are exceptional
%%Constructing narratives
%Identity work (org)
%%%Not-X as excuse
%%Constructing narratives
%Identity work (org)
%%%Concept of maturity
%%Indexing narratives (org)
%Identity work (org)
%%%Governmental influence
%%Permanent emergency
%Invoking master narratives
%%Cyber-security as obligation
%Cyber-security is seen as an obligation for businesses
%%%Masculine dimensions of cyber-security
%%Masculinity
%Invoking master narratives
%%%Geopolitical aspects of cyber-security
%%Permanent emergency
%Invoking master narratives
%%%Masculinity in business environment
%%Masculinity
%Invoking master narratives
%%%Security vs freedom
%%Cyber-security dualisms
%Invoking master narratives
%%Cyber-security is required knowledge for board members
%Cyber-security is seen as an obligation for businesses
%%%Role of media
%%Understanding of cyber-security
%Experiencing cyber-security as a board member
%%Cyber-security as millstone
%Negative associations of cyber-security
%%Board members don't have the right knowledge
%Experiencing the board as a CISO
%%%Cyber-security as interpretive practice
%%Constructing narratives
%Identity work (CISO)
%%Cyber-risk is filtered
%Experiencing cyber-security as a board member
CISO as soothsayer
%%Roles they occupy
%%Multiple and conflicted identities (CISO)
%%Cyber-security as assuagement
%Experiencing ontological (in)security (org)
%%%'it's when not if'
%%Permanent emergency
%Invoking master narratives
%%Cyber-security as ontological threat
%Experiencing ontological (in)security (org)
%%Fear and security
%Invoking master narratives
%Cyber-security is experienced emotionally
%%Cyber-security as bad news
%Negative associations of cyber-security
%%Cyber-security as avoidance of trouble
%Negative associations of cyber-security
%%Cyber-security as discipline or punishment
%How cyber-security gets done
Cyber-security is something to be afraid of
%Experiencing cyber-security as a board member
%%Incidents are beneficial
%How cyber-security gets done
%%Cyber-security is mystical
%Cyber-security as arcane or mystical
%%%Precarious position vs stable function
%%Threats to ontological security (CISO)
%Experiencing ontological (in)security (CISO)
%%Self-perpetuating and self-serving nature of cyber industry
%Cyber-sophistry
%%Cyber-security as edification
%Positioning cyber-security as virtuous
%%Sophistry vs edification
%Cyber-sophistry
%%Cyber-security as social work
%How cyber-security gets done
%%Cyber-security as arcane
%Cyber-security as arcane or mystical
%%'they don't understand'
%%Threats to ontological security (CISO)
%Experiencing ontological (in)security (CISO)
%%Permanence and evolution of cyber-risk
%Risk staging
influences
results in
may indirectly contribute to
may reconcile
may influence
may result in
contributes towards
contributes toward
is affected by
Node
Parent node(s)
%=Category
%%=Sub-category
%%%=Sub-sub-category
%%%%=Sub-sub-sub-category
No prefix=Code
Lower coding density
Higher coding density

Figure B.4: A further analytic diagram suggesting relationships between a number of data categories.

This diagram was key to exploring the aspects of obligation (and recreancy) relating to cyber security that were discussed in Chapter 5.

B.2.3 Operational model diagrams

The final type of diagram included is based on a method from Saldaña known as “operational model diagramming” [653, p. 226]. This technique was helpful at an early stage of the analysis to help make connections between the phenomena I was identifying and to progress from coding to deeper levels of analysis.

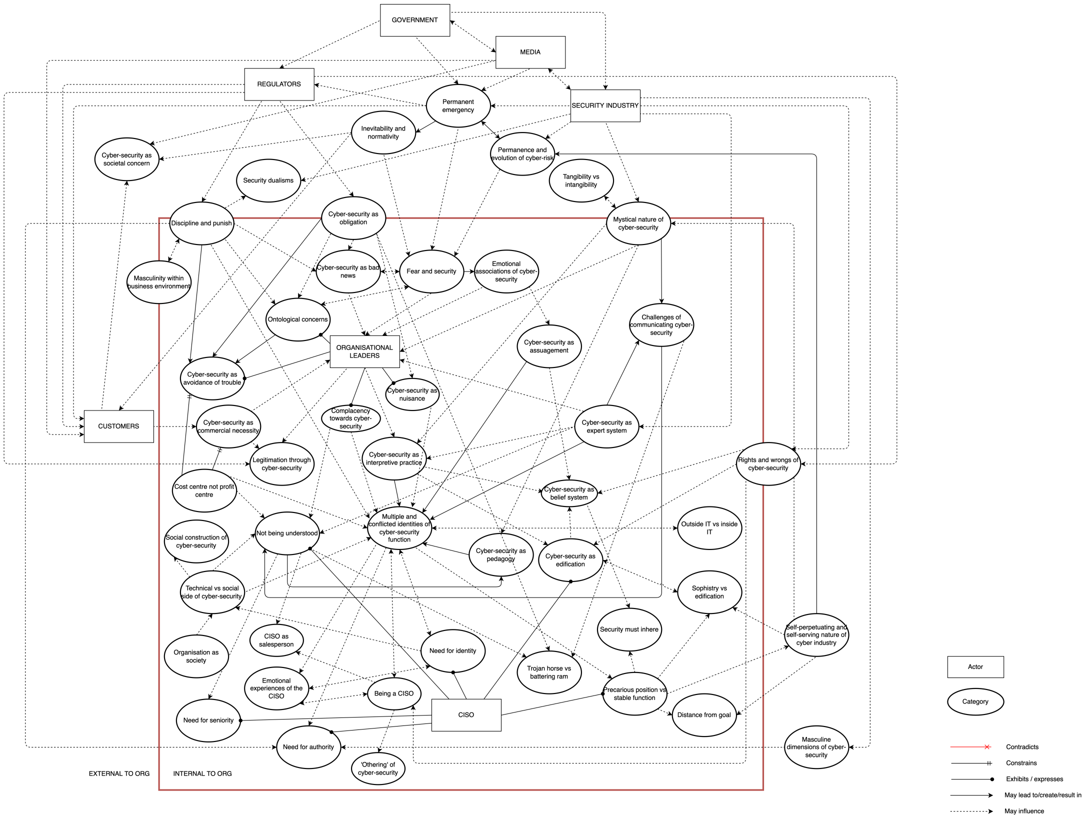

GOVERNMENT
MEDIA
REGULATORS
SECURITY INDUSTRY
Permanent emergency
Inevitability and normativity
Cyber-security as societal concern
Permanence and evolution of cyber-risk
Security dualisms
Tangibility vs intangibility
Discipline and punish
Cyber-security as obligation
Mystical nature of cyber-security
Masculinity within business environment
Cyber-security as bad news
Fear and security
Emotional associations of cyber-security
Ontological concerns
Challenges of communicating cyber-security
ORGANISATIONAL LEADERS
Cyber-security as assuagement
Cyber-security as avoidance of trouble
Cyber-security as nuisance
Complacency towards cyber-security
CUSTOMERS
Cyber-security as commercial necessity
Cyber-security as expert system
Legitimation through cyber-security
Cyber-security as interpretive practice
Rights and wrongs of cyber-security
Cost centre not profit centre
Cyber-security as belief system
Multiple and conflicted identities of cyber-security function
Outside IT vs inside IT
Social construction of cyber-security
Not being understood
Cyber-security as pedagogy
Cyber-security as edification
Technical vs social side of cyber-security
Sophistry vs edification
Security must inhere
Self-perpetuating and self-serving nature of cyber industry
CISO as salesperson
Need for identity
Organisation as society
Trojan horse vs battering ram
Emotional experiences of the CISO
Being a CISO
Precarious position vs stable function
CISO
Distance from goal
Need for seniority
Need for authority
Masculine dimensions of cyber-security
'Othering' of cyber-security
EXTERNAL TO ORG
INTERNAL TO ORG
Actor
Category
Contradicts
Constrains
Exhibits / expresses
May lead to/create/result in
May influence

Figure B.5: An analytic diagram used to explore connections between categories, actors and wider contexts.

The proposed linkages between categories shown in Figure B.5 were useful prompts for analytic memos, enabling exploration of potential relationships. The "rhizomatous" [653, p. 228] nature of this diagram is also useful in demonstrating the complexity of the environment, and the multiplicity of actors, in which the CISO operates.

Appendix C

Interview guides

C.1 Introduction

This Appendix details the interview guides that supported the participant interviews. It is split into two sections, Section C.2 which presents the topic guide used for the CISO interviews and Section C.3 which presents that used for the non-CISOs.

C.2 Interview topic guide: CISOs

In this section I present the themes and example interview questions that were asked of CISO participants. Following Hermanowicz, these questions were not intended to be "an inflexible list that the interviewer follows rigidly" [405, p. 483]; rather, they provided a series of prompts to direct the conversation.

Interview prompts

References are included where questions have been adopted verbatim from existing work.

- Could you describe your role for me?
- How long have you been in that role (at this organisation)?
- What do you consider to be the overall purpose of the cyber-security function?
- "Who or what is being secured?" [701, p. 487]
- How have your views about the cyber-security function changed over the years?
- To whom do you report?
- What is your opinion on your reporting line?
- What information relating to cyber-security do you provide to the board?

- Do you consider that information to be useful? How do you think that information helps the board?
- What do you think they appreciate about the cyber-security function?
- How would they describe its purpose?
- What do you think they find frustrating about it?
- What do you think the perception of top management on cyber security is?
- How would you describe your responsibility with regard to cyber security?
- What would be the impact to the organisation if it did not have a dedicated cyber-security function?
- What would your impression be of an organisation in your industry that did not have a dedicated cyber-security function?
- In relation to cyber security, "I would finally like to ask about something you are most proud of. What stands out as something that has left a strong positive impression on you?" [406, p. 646]
- Request permission to use anonymised verbatim quotes
- Request for optional and anonymised demographic information

C.3 Interview topic guide: non-CISOs

This section details the themes and example interview questions that were asked of non-CISO participants. As above, these were prompts to direct the conversation rather than a fixed list.

Interview prompts

References are included where questions have been adopted verbatim from existing work.

- Could you describe your role for me?
- How long have you been in that role (at this organisation)?
- What are the main challenges of being a board member?
- What does cyber security mean to you?
- From where do you tend to hear about cyber-security issues?
- Tell me about the organisation's cyber-security function
- If they don't have anyone responsible for cyber security – is that a conscious decision? any particular rationale?
- What do you consider to be the purpose of the cyber-security function?
- Why do you think the function is important to the organisation?

- From your perspective, "[w]ho or what is being secured?" [701, p. 487]
- How have your views about the cyber-security function changed over the years?
- What responsibility do you consider the board to have regarding cyber security?
- What would you consider to be the biggest cyber-security risk to your organisation?
- How would you rank cyber security versus other risks to the organisation? Has that changed? Do you anticipate that changing in future? If so, why?
- How would you know about cyber risk if you didn't have someone in the organisational responsible for it? Is that different to any other risk?
- Have you experienced any significant cyber-security incidents?
- Are there any technological advances/changes that you anticipate affecting the cyber security of your organisation?
- Are you confident that the cyber-security function is effective?
- How do you know they're doing a good job / the right thing?
- What information relating to cyber security do you receive?
- What do you consider to be the goal of that information?
- Do you think you get enough information on cyber security? Or too much?
- What do you think the organisation has done particularly well with regard to cyber security?
- How could the cyber-security function be improved?
- How is cyber security governed?
- How would you describe the rest of the board's perspective on cyber security?
- What visibility of the cyber-security function do you have?
- How do you feel about cyber risk?
- How do you feel when you hear about cyber-security incidents affecting other companies?
- How would you describe the responsibility that the CISO has with regard to cyber security?
- What would be the impact to the organisation if it did not have a dedicated cyber-security function?
- What would your impression be of an organisation in your industry that did not have a dedicated cyber-security function?
- What do you consider the future to look like with regard to cyber security?
- Do you have any other thoughts on cyber security that we haven't covered today?
- Request permission to use anonymised verbatim quotes
- Request for optional and anonymised demographic information

Appendix D

Participant information sheet

D.1 Introduction

This appendix presents the information sheet provided to each participant prior to the interviews to enable them to make a decision on whether or not to take part in the research.

D.2 Participant information sheet

Note that the research questions shown below were subsequently refined to become those in Chapter 1.

Invitation to take part

You are being invited to take part in a research project. Before you decide whether or not you would like to take part it is important for you to understand why the research is being done and what it will involve. Please read the following information carefully and discuss it with others if you wish. If you have any questions or particular concerns, please let us know. You will find the relevant contact details on the last page of this document.

Why is this research being done?

This research aims to:

1. understand the purpose and benefit of a cyber-security function within a commercial organisation, as perceived by the leaders of that function and the leaders of the overall organisation (including how that may differ)

2. explore how commercial organisations structure their cyber-security functions and how those structures reflect the purpose of the function

This project is intended to complete by 2022.

Who is doing the research

The researcher is Joseph Da Silva, a full-time Chief Information Security Officer and part-time PhD student. It is entirely self-funded.

Why have I been chosen?

You have been chosen on the basis of your job role, either as a Chief Information Security Officer or as a senior leader within a commercial organisation that has a senior listing on the London Stock Exchange. This study intends to capture input from across a broad range of industries and the target number of companies surveyed is 20-40.

Do I have to take part?

No. It is up to you to decide whether or not to take part. If you do decide to take part, you will be asked to sign a Consent Form. You can withdraw during the interview at any time without giving a reason and your data will be removed from the study. Once the interview has finished you can still withdraw your data up to the point where the data has been analysed and anonymised, so that your identity cannot be determined. Your decision to take part or not to take part will involve no penalty or loss, now or in the future.

What will taking part involve?

Taking part will involve participating in a one-hour interview with the researcher. The interview will be recorded using an encrypted digital recording device. You may also be asked to provide related documentation such as organisational charts or policy documents. Details on how data will be protected are shown below. You may subsequently be invited to take part in a focus group to share your feedback on the results; a separate information sheet will be provided in this event.

What are the possible benefits and/or disadvantages of taking part?

One benefit of taking part is that you contribute to academic research that will be beneficial to future researchers and businesses; by understanding how the purpose and structure of a cyber-security function differs across industries and company types, reusable models or common measurements may be possible and it may be possible to infer from this analysis which models suit which scenarios. You may also benefit from the reflection that will take place as part of the interview process which may provide insights to your own business or role that prove useful.

Other than giving up your time to take part, no disadvantages to taking part in this research are foreseen. There is a small risk of identification from narrative quotation which is explained further below.

Will my taking part be kept confidential?

All the information collected about you during the course of the research will be kept strictly confidential in accordance with current data protection regulations (for more information, please see Royal Holloway's Data Management Policy[1]). Data storage and access will also be managed in line with the General Data Protection Regulation (GDPR) (for more information on your rights when it comes to accessing interview-related data, please see Royal Holloway's Data Protection Policy[2]). You will not be identifiable in any reports or publications without specific consent. All data will be identified only by a code, with personal details kept on a secure computer, accessible only by the researcher.

All interviews will be recorded using a digital recording device where audio is encrypted at the point of capture. Backup recordings will be captured on another encrypted device and deleted once the primary recording has been confirmed as successful. Recordings will be transferred to an encrypted drive for storage and transcription purposes and then deleted from the recording device. Interviews will be transcribed verbatim and anonymised; sensitive information will be redacted during transcription. Anonymisation will be performed using a random assignment of a pseudonym; mapping to company and role will be recorded on an encrypted spreadsheet stored on an encrypted drive, accessible only to the researcher and stored in a locked safe when not in use. Any company documentation provided will also be stored on an encrypted drive, accessible only to the researcher and stored in a locked safe.

You will be asked specifically if you consent to the use of anonymised verbatim quotations in the final thesis; although anonymised, there is a risk of identification in the event that you use (or have used) a similar narrative in any public material, whether in the past or in future. If you decline, then no verbatim quotations from your

[1] https://intranet.royalholloway.ac.uk/staff/assets/docs/pdf/research/researchdatamanagementpolicy-1amendedan19.10.2018.pdf

[2] https://www.royalholloway.ac.uk/about-us/more/governance-and-strategy/data-protection

contribution will be published.

What will happen to the results of the research project?

Results will be written up as part of the researcher's PhD thesis. Results will be presented in terms of themes arising, with comparisons across industry segments. If any individual data are presented, the data will be completely anonymous, without any means of identifying the individuals involved, subject to the limitation described above if quotations are used. Anonymised results or analysis of these results may appear in future academic publications.

Ethical review of the study

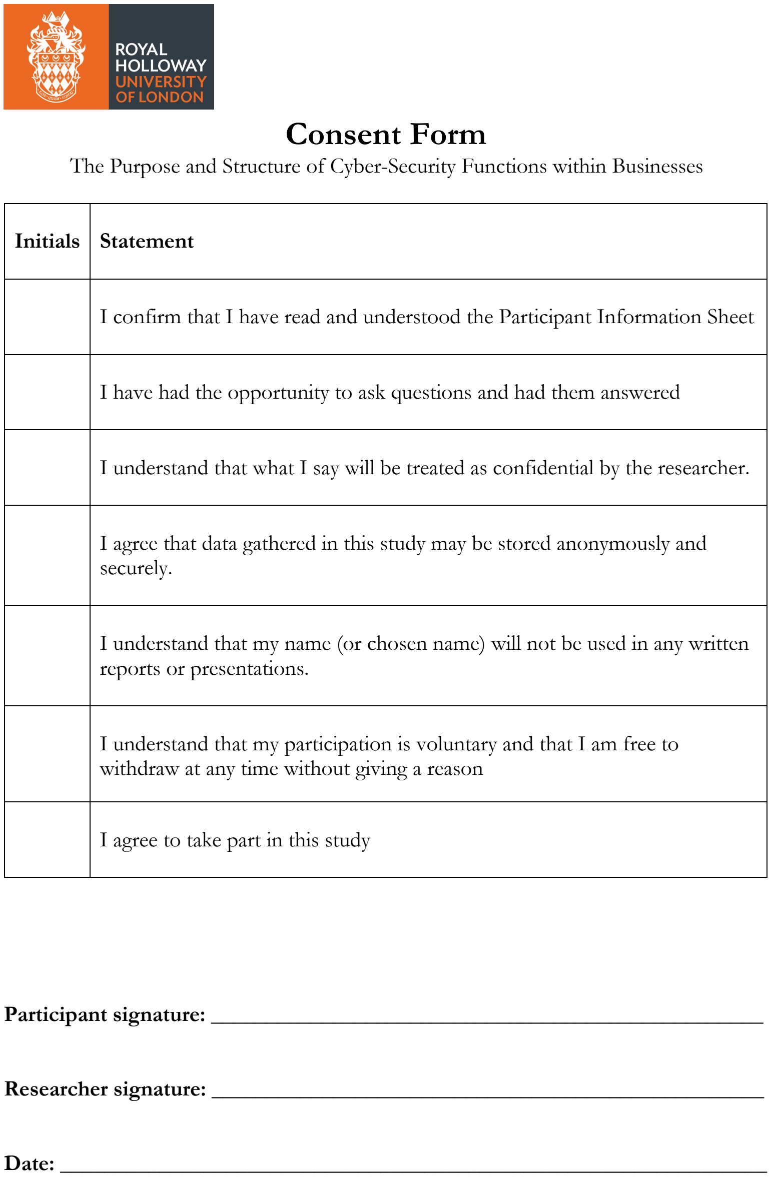
The project has been self-certified by the researcher as compliant with Royal Holloway University of London's Research Ethics requirements.

Contact for further information

Researcher: Joseph Da Silva joseph.dasilva.2018@live.rhul.ac.uk
Supervisor: Dr Rikke Jensen rikke.jensen@rhul.ac.uk

D.3 Consent form

This section presents the form that was provided to each participant prior to the interviews for them to indicate their consent to participating in the research.



ROYAL
HOLLOWAY
UNIVERSITY
OF LONDON

Consent Form

The Purpose and Structure of Cyber-Security Functions within Businesses

Initials	Statement
	I confirm that I have read and understood the Participant Information Sheet
	I have had the opportunity to ask questions and had them answered
	I understand that what I say will be treated as confidential by the researcher.
	I agree that data gathered in this study may be stored anonymously and securely.
	I understand that my name (or chosen name) will not be used in any written reports or presentations.
	I understand that my participation is voluntary and that I am free to withdraw at any time without giving a reason
	I agree to take part in this study

Participant signature: ______________________________

Researcher signature: ______________________________

Date: ______________________________

Figure D.1: The consent form provided to participants.

Appendix E

Optional anonymous demographic information

E.1 Introduction

This Appendix presents the form that was provided to participants to capture optional and anonymous demographic information, as mentioned in Chapter 3.

E.2 Optional anonymous demographic information

Age (please circle):

18-25 | 26-35 | 36-45 | 46-55 | 56-65 | over 65

Highest level of education attained (please circle):

Doctorate | Master's | Bachelor's | HND/NVQ | A-level or equivalent | GCSE or equivalent | No formal educational qualifications

Ethnic origin (please write in block capitals):

Gender identity (please write in block capitals):

Appendix F

Codebooks

F.1 Introduction

This Appendix presents snapshots of the codebooks that were developed during the analysis stage described in Chapter 3. Only two categories are shown in each snapshot for reasons of space. Links to the complete codebooks are provided at the end of each section.

F.2 Interview data codebook

Table F.1 provides examples of the codes and categories that were utilised in the analysis of the interview data. As explained in Chapter 3, codes were initially developed inductively, and were subsequently categorised and rationalised using a deductive approach. Categories are indicated with a prefix of a single percentage sign, with further levels of coding hierarchy depth indicated by additional percentage sign prefixes. Those without prefixes are the lowest level of code/sub-code. A prefix of SUB indicates a subtext code, following Saldaña [653, p. 146]. In vivo codes are indicated by single quotation marks.

Table F.1: Interview data codebook excerpt

Node	**Files coded**	**References coded**
%Being a CISO	18	166
%%means being disheartened and isolated	15	101
%%%means ‘you can never win’	9	23
%%%%Being stoic	4	6

‘fun and games’	1	1
‘it goes with the job really’	1	1
‘we can interrogate you’	1	1
‘you can never win’	1	1
Always on call	1	2
%%%%Feeling overwhelmed	6	12
Pressure and stress	3	8
Signal vs noise	3	4
%%%%Fighting a battle	4	5
‘I found it a really really hard slog’	1	1
‘not everyone was going to be happy’	1	2
Cyber security can’t please everyone	1	1
Dealing with strong personalities	1	1
%%%means being misunderstood	5	13
%%%%Adjusting approach or fitting in	1	4
Need for flexibility	1	4
Creating the rod to be beaten with	1	1
Frustration	3	4
SUB Dissatisfaction with how cyber security is perceived	1	1
SUB Feeling hard done by	1	1
SUB Why does no-one else get it	1	2
%%%means feeling vulnerable	13	65
%%%%Feeling exposed	5	13
‘my god, it actually works’	1	1
Lack of confidence in self	2	6
SUB Lack of confidence	1	1
SUB Lack of confidence in own knowledge	1	1
Regret	3	3
SUB Feeling exposed	1	1
SUB Guilt	1	2
%%%%Feeling isolated	4	6

‘it can be very lonely in security’	1	1
SUB Feeling peripheral	1	2
SUB I can’t win	1	1
SUB not feeling supported	1	2
%%%%Feeling threatened	10	23
‘they don‘t like to hear the answers’	1	1
Experiencing conflict	1	1
‘people can be a bit more unreasonable than that’	1	1
Justification for role	2	5
Legitimation of self	1	1
Need for legitimation	3	5
Need for external authority	1	2
Relief	1	1
SUB Concerned about being judged	1	1
SUB Getting a hard time	2	4
SUB Need for justification	2	2
SUB Under attack	1	1
Walking a tightrope	1	1
%%%%Feeling undervalued	8	15
SUB Feeling insignificant	1	2
SUB Feeling unloved	6	10
SUB Need for validation	1	2
SUB Need to be wanted	1	1
%%%%Feeling unsupported	5	8
Dissatisfaction with organisational backing	4	7
SUB Dissatisfaction with current situation	4	5
SUB Dissatisfaction with size of team	1	1
Importance of support from senior leaders	1	1
%%means being part of something bigger	7	16
%%%Elitist nature of cyber security	3	8

‘you might not put him in front of the board of directors’	1	1
Cyber security as clique	1	2
Cyber-security community	3	4
Elite aspects of cyber security	1	1
Collaboration in cyber industry	3	7
Knowledge sharing	1	1
%%means believing in what you do	10	25
‘it was rewarding’	1	1
‘it’s quite satisfying’	1	1
Improvements made by CISO	7	16
Changes I have made	1	1
Pride in effectiveness of controls	2	3
SUB Passion	1	1
SUB Pride	2	3
%%means feeling superior	2	2
SUB I know better	2	2
%%means leading not doing	3	8
‘I can’t do it on my own’	1	1
‘I don’t do any security really anymore’	2	3
‘my knowledge is generally so out of date’	1	1
Dependency on others to succeed	1	2
Leading the team vs doing the work	1	1
%%means needing encouragement	6	10
‘the CISO feels very supported’	1	1
Executive support	2	2
Need for strong leadership	1	1
SUB Need for recognition	3	6
%%means needing to change things	1	1
Transformational role	1	1
%%means not feeling challenged	3	3
‘run of the mill’	1	1
‘still responding to phishing’	2	2
%Cyber security as arcane or mystical	16	51
%%Bringing security out into the open	7	10

Governance of cyber security	6	8
Transparency of risk	2	2
%%Cyber security as arcane	15	29
%%%Cyber security is difficult to communicate	14	25
%%%%Metaphor	8	12
‘I use a lot of analogies’	1	1
Analogy	1	1
Cyber security as safety	2	3
‘communications problem’	1	2
‘more exciting and engaging’	1	1
‘not everything can be distilled down’	1	1
‘the more I keep saying it the more it’s going to sink in’	1	1
‘we don‘t share the good news stories’	1	1
Age as a factor in cyber-security knowledge	1	1
Communication of cyber security	3	3
Managing individual stakeholders differently	1	1
Need for simplicity	1	1
Visualisation of risk	1	1
Cyber security as foreign language	3	3
Cyber security as sensitive subject	1	1
%%Cyber security as mystical	4	9
‘a dark art’	2	2
‘opaque and pervasive’	1	1
‘very hard to see how the issue will manifest’	1	1
Desire for objectivity	1	2
Intractability of cyber-threat	1	3
‘you can’t influence it’	1	1
%%Tangibility vs intangibility	2	3
‘some of these other things that we use feel a little bit more tricky to get your arms around’	1	1

‘sometimes it can feel quite intangible’	1	1
Tangiblility vs intangibility	1	1

A snapshot of the codebook produced from the analysis of the interview data.

The full codebook is located at https://royalholloway.figshare.com/articles/dataset/Interview_data_codebook_from_Da_Silva_doctoral_research/19738339.

F.2.1 Illustrative example

As encouraged by Seale [669, p. 155], brief examples of coded data are shown below. The first excerpt was contained within the subcategory of *%%%%Being stoic*. Other codes within this category were all in-vivo, and hence are not shown, as they appear in Table F.1.

> “I wasn’t pleased about getting the phone call at quarter past midnight, luckily I hadn’t gone to bed.”

This was coded as *Always on call*.

The following excerpts were contained within the subcategory of *%%%%Feeling overwhelmed*. Not all of the excerpts coded thus are shown for reasons of space.

> “*[Interviewer]* And how are you finding it?”
>
> “*[Participant]* Erm honestly? A little overwhelming.”

> “I wanna go back to fixing servers, that was much easier.”

> “There’s always this sense that you don’t want to create too much burden on people and I do get that pressure a lot all the time, it’s like ‘let’s not create too much’ and the business will be quick to complain.”

The three excerpts above were coded as *Pressure and stress*. The following three excerpts were also contained within the subcategory of *%%%%Feeling overwhelmed*.

> “It monitors probably on on a quarterly basis anywhere between 150 to 350 billion events coming off our estates at the moment, some of it’s a bit noisy because, you know, getting all of your auditing policies and logging policies tuned takes time.”

> “It is noisy.”

> “We’ve got too much noise coming in.”

These excerpts were coded as *Signal vs noise*.

F.3 Annual report data codebook

Table F.2 provides examples of the codes and categories that were utilised in the analysis of the interview data. As described in Chapter 3, this coding was more deductive than that performed for the interview data, due to the reuse of as codes and concepts determined from the latter. As in Section F.2, categories are indicated with a prefix of a single percentage sign, with further levels of coding hierarchy depth indicated by additional percentage sign prefixes. Those without prefixes are the lowest level of code/sub-code. In vivo codes, some of which have been paraphrased to preserve anonymity, are indicated by single quotation marks.

Table F.2: Annual report data codebook excerpt

Node	**Files coded**	**References coded**
%Bias in business	11	19
%%Masculinity	9	13
%%%Militaristic cyber-security language	2	3
‘red team’ exercises	1	1
‘war gaming’	1	1
creation of ‘red team’	1	1
Aggressive language	3	3
Masculine language	6	6
Technology committee predominantly male	1	1
%%Primacy of financial measurement	4	5
Cyber-security attack as ‘less predictable’ financial impact	1	1
Dependency on IT for accurate financial reporting	1	1
Impacts measured in financial terms	1	1

IT general controls failure as financial risk	1	1
Regulation as financial risk	1	1
Association of expertise with age	1	1
%Business’ trust in expert systems	10	20
%%Trust in external experts	2	2
Board requirement for ‘external expert perspectives’	1	1
External perspectives in Internal Audit	1	1
%%Trust in internal experts	10	17
‘business ethics team’	1	1
‘managed by professionally staffed teams’	1	1
Board updates from ’internal specialists’	1	1
Dedicated ‘internal control department’	1	1
Dedicated Ethics and Compliance personnel in each Business Unit	1	1
Expert systems	4	8
Importance of specialists to business	1	1
Specialist teams	3	3
Consultation with experts on ethical issues	1	1

A snapshot of the codebook produced from the analysis of the annual report data.

The full codebook is located at https://royalholloway.figshare.com/articles/dataset/Annual_report_codebook_from_Da_Silva_doctoral_research/19738354. No illustrative examples of annual report coding are provided to avoid the risk of identification, as it would be trivial to de-anonymise the organisations involved due to the public nature of annual reports.