THE REGULATORY CHALLENGES OF AUSTRALIAN INFORMATION SECURITY PRACTICE

Information security is not directly regulated in Australia and is instead subject to a patchwork of different legal and regulatory frameworks. How Australian information security practitioners construct and action information security therefore becomes important to the overall operation of a fragmented regulatory framework. How then do Australian information security practitioners understand information security and make compliance-oriented decisions? Our exploratory interview research examined how nine Australian information security practitioners understood and constructed their role as delegated regulators of organisational information security processes. Participants expressed a number of concerns that reveal a very different world to that traditionally portrayed as the discipline and practice of information security. We examine these concerns and discuss what they mean in the context of the Australian environment.

AUTHORS: MARK BURDON, JODIE SIGANTO AND LIZZIE COLES-KEMP

AUTHOR DETAILS:

Mark Burdon is a Senior Lecturer at the TC Beirne School of Law, The University of Queensland.
Jodie Siganto is a collaborator on the Cyber Security Cartogaphies project led by Dr Lizzie Coles-Kemp, Royal Holloway University of London, which is part of the United Kingdom's first Cyber Security Research Institute.
Lizzie Coles-Kemp is a Senior Lecturer at the Information Security Group, Royal Holloway University

Keywords: information security, data protection, data breaches, information security management.

1. INTRODUCTION

Information security, as a discipline, is portrayed as rational and control-oriented. The appropriateness of controls is derived through risk assessment frameworks that consider the contextual realities of the given organisation. In this paradigm, the role of the information security practitioner is to identify security risks that emerge and to design and implement appropriate controls. The practitioner then ensures those controls operate as expected and continue to address identified risks, as part of an iterative process. The implementation of information security therefore regards rational considerations that translate into actions that are accepted as reasonable by organisations. These organisations accept the value of information security as a self-serving good and one that has wider societal benefits from the broader minimisation of risks arising from security failures.[1]

[1] See e.g. Roger Clarke, 'The prospects of easier security for small organisations and consumers' (2015) 31(4) *Computer Law & Security Review* 538, 539.

It is therefore not surprising that a developing literature on practitioner perspectives is starting to develop.[2] Such 'human factors'[3] or 'human challenges'[4] studies highlight the dissonance between, on the one hand, the theory of information security as a purely control-oriented approach, and on the other, the practice of information security which is negotiated and individually constructed.[5] How practitioners construct and operationalise information security in practice is important to understand in order to assess the effectiveness of legal and regulatory application.

In Australia, understanding the day-to-day lives of practitioners, and their perspectives on information security, and its management, is particularly important because of the legal and regulatory structure employed. Information security is not regulated directly by a governing piece of legislation. Instead, a patchwork of different laws, guidelines and regulations provide a principled range of security obligations for both private and public sector organisations. A broad regulatory framework underpins this patchwork of legal obligation which is predicated on principles-based regulation (PBR).[6] In effect, the regulatory function is partly delegated from the regulator to the regulatee, in this case, the information security practitioner. As such, in a system of delegated regulation,[7] such as in a PBR framework, it is vital to understand practitioner perspectives of information security and how core concepts of information security are being constructed and actioned by delegated regulatory actors.

In this article, we report on findings from our exploratory interview research which examined how nine Australian information security practitioners understood and constructed their role as delegated regulators of organisational information security processes. Our findings reveal a very different world to that traditionally portrayed as the theory, discipline and practice of information security. Participants in our study had irregular working days and the 'average day' for all of our participants focused mostly on processes of interaction and negotiation. Definitions of information security also varied significantly which revealed a number of different understandings about the core

---

[2] See e.g. Eirik Albrechtsen, 'A qualitative study of users' view on information security' (2007) 26(4) *Computers & Security* 276; Eirik Albrechtsen and Jan Hovden, 'The information security digital divide between information security managers and users' (2009) 28(6) *Computers & Security* 476; Eirik Albrechtsen and Jan Hovden, 'Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study' (2010) 29(4) *Computers & Security* 432; Debi Ashenden, 'Information Security management: A human challenge?' (2008) 13(4) *Information Security Technical Report* 195; Debi Ashenden and Angela Sasse, 'CISOs and organisational culture: Their own worst enemy?' (2013) 39(11) *Computers & Security* 396; Lizzie Coles-Kemp, 'Information security management: An entangled research challenge' (2009) 14(4) *Information Security Technical Report* 181.

[3] Human factors in this sense ofter refers to insider actors as threats. See Carl Colwill, 'Human factors in information security: The insider threat – Who can you trust these days?' (2009) 14(4) *Information Security Technical Report* 186.

[4] Ashenden more broadly refers to human challenges in relation to the complex actions of information security actors. See Debi Ashenden, 'Information Security management: A human challenge?' (2008) 13(4) *Information Security Technical Report* 195

[5] Gurpreet Dhillon and James Backhouse, 'Current directions in IS security research: towards socio-organizational perspectives' (2001) 11(2) *Information Systems Journal* 127.

[6] See for an overview of PBR Julia Black, Martyn Hopper and Christa Band, 'Making a Success of Principles-Based Regulation' (2007) 1(4) *Law and Financial Markets Review* 191.

[7] See more broadly Cary Coglianese and David Lazer, 'Management-Based Regulation: Prescribing Private Management to Achieve Public Goals' (2003) 37(4) *Law & Society Review* 691.

constructs of information security, such as risk and risk assessment. Most importantly, compliance considerations also varied and it was clear that participants considered the application of law and regulation from different sources and in different ways. Our research therefore reveals a world and practice of information security that is not as ordered and structured as the control-oriented tradition of information security would have us believe.

Section 2 briefly outlines the legal and regulatory framework for information security in Australia. Section 3 details the research methodology employed in the study and Section 4 covers some key research findings. Section 5 provides some discussion in relation to what our study means for the legal and regulatory framework currently adopted in Australia and Section 6 concludes our article in relation to future directions.

2. REGULATING INFORMATION SECURITY IN AUSTRALIA

Information security in Australia is not directly regulated by a specific and governing piece of legislation that covers all public and private sectors. Government agencies are regulated by a range of both Commonwealth and state laws and guidelines. As a consequence, both federal and state governments have developed approaches to secure the information held in government-controlled systems.

Australian federal government agencies are covered by a specially designed framework comprised of the Protective Security Policy Framework (PSPF)[8] and the Information Security Manual (ISM).[9] The ISM is based on a series of high-level principles which are supported by a detailed controls manual. The first principle is information security risk management, which supports agencies making informed, risk-based decisions specific to their unique environments, circumstances and risk appetite (subject to the implementation of a number of controls which are stated to be mandatory). In addition, there is a range of more technology-specific principles dealing with topics including product security, media security, software security, email security, network security and cryptography.[10]

The Victorian Government in 2012 adopted the Commonwealth Government's PSPF and ISM.[11] Other state governments in Australia have adopted different approaches to ensuring

[8] The Commonwealth Attorney-General sets the Australian Government's protective security policy and has released the Protective Security Policy Framework, in pursuance of that responsibility. Attorney-General's Department, 'Government Response to the House of Representatives Standing Committee on Communications Report on the Inquiry into Cyber Crime ' (Commonwealth of Australia, 2010). See also Sharon Oded, *Corporate Compliance New Approaches to Regulatory Enforcement* ('Edward Elgar, 2013).

[9] The ISM is published by the Australian Signals Directorate pursuant to the *Intelligence Services Act 2001* (Cth). It is made up of a number of different publications. See Intelligence and Security Department of Defence, *Australian Government Information Security Manual - Principles* (2015); Intelligence and Security Department of Defence, 'Australian Government Information Security Manual - Controls' (2015) <http://www.asd.gov.au/publications/Information_Security_Manual_2015_Controls.pdf>.

[10] Intelligence and Security Department of Defence, 'Australian Government Information Security Manual - Controls' (2015) <http://www.asd.gov.au/publications/Information_Security_Manual_2015_Controls.pdf>, 37 – 60.

[11] Victorian Government standards include Victorian Government CIO Council, 'Information Security Management Framework' (2014) <http://www.enterprisesolutions.vic.gov.au//wp-content/uploads/2014/07/SEC-STD-01-Information-Security-Management-Framework.pdf>.

the security of the information that they hold, however, they all reference ISO 27001[12] and ISO 27002[13] (and its risk-based management system approach to information security) to some degree. The New South Wales Government has long supported compliance with ISO 27001 and IS0 27002.[14] The Queensland Government has re-issued a modified version of ISO 27001 as an 'information standard.'[15]

The situation regarding private sector coverage is more fragmented. Although there is little regulation, guidance has been issued by different regulators. The Australian Prudential Regulation Authority (APRA), adopted a Prudential Practice Guide regarding the management of security risk in information and information technology.[16] Similar to the ISM and the ISO 27001, APRA's guide employs a risk-based approach to information security management, through the development of an IT security risk framework. The Australian Securities and Investments Commission (ASIC) released a report in May 2015 aimed at assisting organisations regulated by ASIC in their efforts to improve cyber resilience[17] which report provides that regulated entities have 'legal and compliance obligations' that may require them to 'review and update' their cyber-risk management practices.[18] This report recommends that consideration be given to the adoption of the NIST Cybersecuity Framework,[19] as being of particular relevance to the particular regulated community.[20]

The key information security legal obligation for private sector organisations,[21] however, regards protections of personal information legislated by the Commonwealth *Privacy Act*.[22] Australian Privacy Principle 11.1 (APP 11.1) requires public and private sector entities to take reasonable steps to protect personal information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.[23] This broad legislative principle is supplemented by guidance provided by the Australian Privacy Commissioner in the Guide

---

12 International Standards Organisation, *ISO/IEC: 27001: 2013 Information technology – Security Techniques – Information security management systems- Requirements* (2013) ('ISO 27001').

13 International Standards Organisation, *ISO/IEC 27002:2013 Information technology – Security Techniques – Code of Practice for Information Security Management* (2013) ('ISO 27002').

14 NSW Government, 'Digital Information Security Policy' (2012) <http://arp.nsw.gov.au/sites/default/files/Digital_Information_Security_Policy_2012.pdf>.

15 Queensland Government Chief Information Office, 'Information Security - IS18' (2015) <http://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2704-information-security-is18policy>.

16 Australian Prudential Regulation Authority, 'PPG 234 – Management of security risk in information and information technology' (2010) <http://www.apra.gov.au/CrossIndustry/Documents/PPG_PPG234_MSRIT_012010_v7.pdf>

17 Australian Securities and Investments Commission '*Report 429: Cyber Resilience*' (2015).

18 Ibid, 7.

19 National Institute for Standards and Technology, '*Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*' (2014) <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>.

20 Above n. 7, 32.

21 It should be noted that not all private section organisations are regulated by the *Privacy Act*. Small businesses, for example, organisations with an annual turnover of less than $3 million per year are exempt from the Act. See *Privacy Act 1988* (Cth) s 6C.

22 *Privacy Act 1988* (Cth).

23 *Privacy Act 1988* (Cth) Sch. 1 Sub-cl. 11.1.

to Securing Personal Information.[24] The Guide provides guidance on the reasonable steps entities are required to take in order to be compliant with APP 11.1. However, ultimate compliance with APP 11.1 is a matter of interpretation and implementation by the regulated entity. The choice, design, construction and implementation of regulatory measures are therefore delegated to the regulated entity. Thus, at least the partial responsibility for developing inter and intra-organisational regulatory measures is delegated to information security managers and officers.

APP 11, and the guidelines highlighted above, are representative of a PBR framework which is at the heart of regulatory and legal development in this area. In introducing a privacy regime based on the OECD Privacy Guidelines,[25] the Australian Government accepted a principle-based regulatory model for the protection of personal information in Australia.[26] PBR was confirmed as the appropriate regulatory model for privacy on the introduction of the private sector provisions in 2000[27] and as part of the review by the Office of the Privacy Commissioner in 2005.[28] PBR was confirmed again by the Australian Law Reform Commission (ALRC) in its voluminous review of privacy law, which concluded in 2008, and resulted in the ALRC providing specific consideration to the issue.[29] Most recently, the Australian Government has recently referred to PBR generally as a type of 'light touch regulation', noting the benefits it provides through allowing maximum flexibility among the regulated community regarding how they achieve compliance.[30]

PBR requires the use of broad-based principles to achieve desired regulatory objectives. In legal frameworks of this type, the use of general principles can be distinguished from the employment of 'bright-line' and more complex and detailed rules.[31] A 'bright line' rule contains a single criterion of applicability. Their simplicity means bright line rules are straightforward and so easier to understand and apply than principles; however, they are susceptible to gaming and 'creative' compliance. The specificity of the rule means it may not be broad enough to capture all of the conduct that it is aimed at. Alternatively, an organisation may 'comply with the letter, but not the spirit, of the rule.'[32] A complex or detailed rule can provide a higher degree of certainty by providing greater detail about what is required for compliance. However, the greater degree of specificity means that

---

[24] Office of the Australian Information Commissioner, 'Guide to securing personal information' (2015) <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>.
For a critique of the Guide's foundational base see Roger Clarke, 'The prospects of easier security for small organisations and consumers' (2015) 31(4) *Computer Law & Security Review* 538, 545.

[25] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Information* (1980).

[26] Australian Law Reform Commission, '*For Your Information: Australian Privacy Law and Practice*' (2008), [2.4], [18.24].

[27] Commonwealth, Parliamentary Debates, House of Representatives, 8 November 2000, 22370 (D Williams, Attorney-General).

[28] Office of the Privacy Commissioner, '*Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*' (2005) ('Getting in on the Act').

[29] See Australian Law Reform Commission, above n. 26, Chapter 4.

[30] Australian Government, 'The Australian Government Guide to Regulation' (2014) <http://www.cuttingredtape.gov.au/sites/default/files/documents/australian_government_guide_regulation.pdf>, 28. See also Australian Law Reform Commission, 'above n.26, [18.35].

[31] Julia Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (London School of Economics and Political Science, 2007) 10.

[32] Australian Law Reform Commission, above n. 26, [18.28].

these rules are even more susceptible to manipulation and creative compliance than bright line rules.[33]

In comparison, a 'principle' articulates substantive objectives rather than specific compliance requirements.[34] The perceived benefits of principle-based regulation include being less susceptible to gaming and a 'tick box' compliance approach. Principles give firms 'increased flexibility to decide more often … what business processes and controls they should operate.'[35] It is believed that the devolution to the regulated community of the interpretation of compliance obligations will result in an industry that deals with regulatory issues in a more effective and efficient way. Principles are also seen as more flexible than prescriptive rules and therefore more durable in a rapidly changing environment.[36] It is this durability aspect that was stressed by the ALRC in its review of the appropriateness of the principle-based regulatory scheme, particularly when considering the challenges posed by new technology.[37]

The role of the regulator, in this case, primarily, the Office of the Australian Information Commissioner (OAIC), and the methods they use to engage with the regulated community to ensure compliance are important to PBR. One of the assumptions supporting principle-based regulatory theory is that the market is self-correcting and that responsible organisational management will ensure the adoption of appropriate systems and processes to meet the outcomes stated in the principles.[38] However, to ensure that the market operates in the expected way, there must be a close engagement between the regulator and the regulated in which regulatory goals are clearly communicated.[39] Hence the importance of regulatory guidelines to the operationalisation of information security practice in Australia.[40]

Black underlines the importance of close engagement between the regulator and the regulated community, referring to the need for a dense network of 'regulatory conversations' between the regulator and the regulated regarding the purpose and application of the principle, where the outcome is structured around the goal that the principle is trying to achieve.[41] Black notes that principles give the regulated more discretion in what they do, so that responsibility for ensuring that the objectives of the principles are met is shifted in part from the regulator to the regulated.[42] According to Black, this involves 'a significant shift in responsibility to firms and requires a substantially different set of skills on the part of inspectors and compliance staff to engage in the

[33] Ibid [18.30].
[34] Ibid [18.29].
[35] Financial Services Authority U.K., *Principles Based Regulation: Focusing on the Outcomes that Matter* (2007) 6 – 7.
[36] Australian Law Reform Commission, above n. 26, [18.55].
[37] Ibid, 235.
[38] Robert Baldwin, Martin Cave and Martin Lodge, *The Oxford Handbook of Regulation* (Oxford University Press, 2010) 302–303.
[39] Julia Black, 'Forms and paradoxes of principles-based regulation' (2008) 3(4) *Capital Markets Law Journal* 425.
[40] Australian Law Reform Commission, above n. 26 [4-59].
[41] Julia Black, '*The Rise, Fall and Fate of Principles Based Regulation*' (2010), LSE Legal Studies Working Paper No. 17/2010, 6.
[42] Ibid 7.

negotiations and qualitative judgement that are entailed.'[43] The shift in responsibility also involves a conscious and deliberate focus by the regulator on the firm's internal systems of management and controls.[44]

Finally, Black referred to the importance of regulators managing the greater interpretive risk for firms that arise from the use of principles, and minimising the effects of this risk through its enforcement approach.[45] Black's view was that if a regulator were to take a take a punitive approach to every minor infraction it would lead to a demand for rules. Enforcement therefore 'has to be responsive to the firm's own attitude and behaviour' and focus on outcomes.[46] In other words, PBR requires a closely engaged regulator using a responsive enforcement approach to achieve clearly communicated outcomes and goals as part of a two-way conversation, while focusing on the operation of organisational management systems and controls.

The key feature of PBR consequently involves delegation of traditional regulatory functions to the regulated entity. PBR therefore assumes that the regulated entity is best placed to understand its own environmental context and to meet principles-based statutory outcomes by being able to develop innovative forms of compliance that effectively manage the risks arising for the entity. Success of any PBR scheme is dependent upon a transfer of trust from the regulator to the regulated entity in the hope that the latter will have the competence and responsibility to self-observe and to regulate itself appropriately. This transfer of trust is ultimately likely to make its way through organisational hierarchies and eventually reside on the shoulders of information security practitioners. If practitioners do indeed bear the weight of delegated regulation then how practitioners construct, understand and action the practice of information security becomes important because the delegation of the regulatory function will be understood from the practice perspectives of practitioners. As such, a practitioner's 'average day' and the effectiveness of delegated responsibility are intimately linked.

3. RESEARCH METHODOLOGY

Our research findings are based on nine semi-structured interviews with individual information security practitioners. The nine interviewees were selected using convenience sampling[47] and from individuals who volunteered in response to a request for participants posted to the Australian Information Security Association (AISA) LinkedIn group. No attempt was made to select interviewees to reflect a representative group of practitioners based on national coverage or type of role. However, we did attempt to interview persons from different types of organisation and different industrial sectors to examine whether these factors had an impact on how information security is constructed by practitioners.

Although the specific job title and role specification of each practitioner differed, all interviews nevertheless identified themselves as information security practitioners. The

[43] Ibid 8.
[44] Ibid.
[45] Ibid 6 -7.
[46] Ibid 7-8.
[47] The first interviewees were known personally to the second author and these interviewees were further asked about other interviewees who would be interested in participating in the research.

interviewees included two females and seven males and were aged from their mid-30s to early 60s. Participants and details of their employees were anonymised to further encourage an open dialogue. Participants A to E were employed and interviewed in Brisbane and participants F to I were employed and interviewed in Melbourne. Four of the participants were Australian citizens and the remainder of participants were born in either continental Europe or the United Kingdom or Ireland. Again, we did not specifically recruit participants from different nationalities but we were interested in examining whether a participant's place of birth or education had an influence in terms of their construct of information security.[48] Similarly, participants were recruited from a range of industrial sectors including security consultants.

Interviews with participants varied in length from 60 minutes up to 90 minutes. Each interview was semi-structured, with each interviewee being asked to respond to a series of questions, supported by loosely constructed prompts, regarding a description of their role and an average recent day at work; how the participants communicated; the relationships they had in place; their view of trust; their definition of information security; their understanding of their compliance obligations; concerns about information security and things they liked about information security. The interviews were then transcribed verbatim and examined in Nvivo to identify recurring themes utilising a general inductive approach for analysing qualitative evaluation data.[49]

During the interview, each participant was asked to describe what they did, and were asked to consider a particular day (e.g. last Thursday) and describe to us what they did on that day. Participants also provided further descriptions about their everyday life in response to other questions posed by the interviewers, particularly those about interpersonal communications and relationships. This narrative approach enabled us to view the 'every day' standpoint of the information security practitioner from a number of different perspectives. It also assisted us to identify those themes upon which most or all of the participants agreed and allowed an insight into shared experiences and situations that could often be viewed as fragmented and ambiguous.[50] This aspect was important to our research because we wanted to identify the constructs of information security being generated, how those constructs were being influenced by the 'everyday' existence and the extent to which these aspects influenced constructs of compliance.

4. RESEARCH FINDINGS

Research findings from the study indicate that the participants' daily, working lives require quite different considerations to the control-oriented foundations of traditional perspectives of information security. The 'average day' for the participants was generally described as complex and one that involves numerous parties, spread over different teams and in

[48] Although this artice does not consider the impact of geography and background on participants, further research is being conducted which will contrast the experience of information security practitoners in different geographical locations.

[49] David R. Thomas, 'A General Inductive Approach for Analyzing Qualitative Evaluation Data' (2006) 27(2) *American Journal of Evaluation* 237.

[50] See Anne-Marie Søderberg, 'Sensegiving and sensemaking in an integration process: A narrative approach to the study of an international acquisition in Czarniawska and Gagliardi (eds.), *Narratives We Organize By* (John Benjamins, 2003).

different organisations. The participants' tended to describe the management of information security in their organisations as processes of negotiation rather than implementations of controls. The unpredictability of working days and environments may also have impacted on constructions of information security. Surprisingly, when asked about their definition of information security, the participants tended to provide us with different considerations. A similar situation arose when participants were asked to consider what 'risk' meant to them and how risk assessments operated in their organisation. Given the diffusion of responses, it became clear that different constructs of compliance were also in operation and that there was not really a core legal consideration that guided compliance oriented actions. We consider these points in more depth below.

4.1 UNPREDICTABLE DAYS AND ROLES

The nine interviewees held a range of jobs with varying job titles and descriptions. Three interviewees were independent consultants, while the rest worked in different capacities for a range of different types of organisations. Three of the non-consultant interviewees had responsibility for teams, one being a project manager and another being project security lead. One of the other interviewees had a similar role, acting as the information security expert adviser in regard to a particular project.

Some work has been done on establishing job profiles for workers in IT security, and using these profiles as the basis for a common understanding of and lexicon for cybersecurity work.[51] The intent of frameworks such as the U.S. Cybersecurity Workforce Framework is to describe cybersecurity work 'regardless of organizational structures, job titles, or other potentially idiosyncratic conventions.'[52] The US recognises that the creation of consistent definitions for the cybersecurity population 'using standardized terms is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce.'[53] The European Committee for Standardization has developed a similar framework which includes 23 job profiles in six areas of IT security: business management, technical management, design, development, service and operations, and support. These jobs also cluster into five segments, each driven by an action verb: manage, plan, build, run, and enable.[54]

[51] See, for example, National Initiative for Cybersecurity Education, 'National Cybersecurity Workforce Framework 2.0' (2014) <http://csrc.nist.gov/nice/framework/>.
[52] Ibid.
[53] Ibid.
[54] The EU framework is referred to in Frost & Sullivan, 'Critical Times Demand Critical Skills: An analysis of the skills gap in information security' (2013) <https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/GISWS-Skills-Gap-Analysis.pdf>, 2 which is based on the Global Information Security Workforce study, undertaken by Frost & Sullivan with (ISC)².

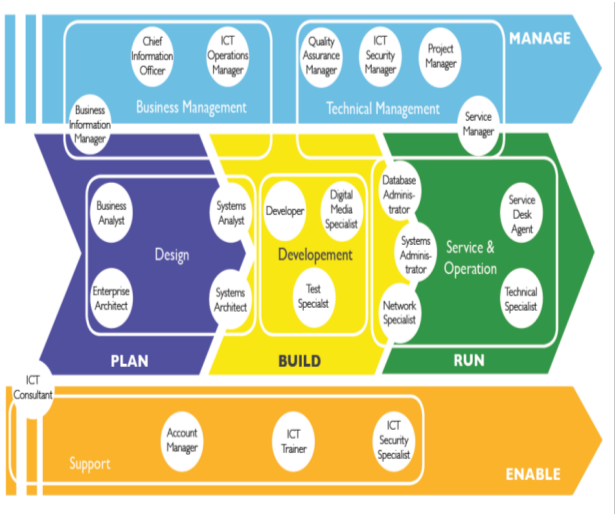

Figure 1: EU Committee for Standardisation Framework for IT Security

The roles of seven of the nine interviewees fit into the above framework (albeit clustered in the 'Business Management' and 'Plan' domains). However, there were a number of participants who do not seem to fit so neatly.

Two of the interviewees described their role as including responsibility for "governance, risk and compliance" and one was responsible for a team called "risk, security and compliance." The EU Framework makes no specific reference to governance or assurance, although again these functions might be assumed to be part of the business management function. Similarly, the EU framework makes no reference to compliance, other than perhaps through the reference to 'Quality Assurance Manager.'[55] These omissions could be a reflection of the framework having been developed for IT Security rather than information security. However, it is also worth noting that two of the interviewees who described their role as including responsibility for "governance, risk and compliance' made few reference to governance or compliance when discussing their every-days. This potentially points to the skills needed for this type of role being more fundamental than knowledge or technical skills with negotiation, conflict management and communications skills being key.

When asked to describe their day, a number of interviewees were keen to refer to their diaries or time sheets to help them recall what they had done on the day they had elected to describe. However, most were able to talk about a standard day without prompts.

Although all regarded themselves as information security practitioners, each of the interviewees described quite different "average days." It is interesting to note that the skills used in the typical every-day relate to communication skills, planning skills, relationship management skills and negotiation skills. These skills are not traditionally taught as part of an IT/IS training.

[55] These roles seem to fit more neatly into the NICE Draft Cybersecurity Workforce Framework 2.0 which includes a domain called 'Oversee and Govern' which includes roles such as risk management, security program management, strategic planning and policy development.

The most consistent narratives were provided by the consultants who referred to tasks such as 'trying to ask the right questions to tease out the information to support whether they meet the intent of that standard' with a view to 'understand and ascertain their compliance with the particular controls within the standard.' The interviewees who held manager positions within end user organisations described days where the focus was on interacting with their own teams, with the occasional reference to interactions with other parts of the business. This is consistent with their role as managers and being responsible for teams. Two of these interviewees had new teams and both were spending time to develop their own people. C referred to the need to set priorities for his team as there were many challenges that needed to be addressed and 'it was very easy to be drawn in to a big new task.'

As managers, these interviewees also described a greater number of different tasks as part of their average day than the consultant interviewees. For example, C's description of his day included strategic planning meetings with his own team, preparing for the next project governance board meeting, a number of meetings on the delivery of a new system and developing a briefing paper on cloud. He also had meetings with his own team to make sure they were on track. C commented 'I don't have many typical days; each day is pretty different to the next.'

It might be assumed that those with project team roles would have similar roles. However, again the three members of the group who might loosely be regarded as the security project team members were quite different in their every-days.

One project team member described his typical day (and his job) as 'making sure people know what I know, as soon as possible.' He gave a succinct summary of the object of his job which was to guide business and technology projects through a life cycle and to ensure that:

> [T]he security requirements are adequately catered for, designed for and then assessed properly at the end and any residual risks are signed off by the appropriate people with the appropriate authority.

Another project team member described an average day that had a clear overall outcome but with very limited interaction with other team members. It involved obtaining and reviewing documentation and developing a system security plan for security certification and accreditation purposes. At times there was interaction with other people, such as the involvement of other security people in risk assessment, or verifying positions with the audit team, but this seemed to be limited. It should be noted that this was probably reflective of the stage of the project, which was still very much at the design and documentation part of the cycle.

4.2 DIFFUSE CONSTRUCTS OF INFORMATION SECURITY

In response to the question about how they defined information security, we expected participants to largely support the commonly used definition of information security found, for example, in ISO 27001, namely, 'the preservation of confidentiality, integrity and

availability of information' ('CI&A').[56] A number of the participants did define security in these terms, but also added some qualification, referring to CI&A as 'the old classic' or the 'textbook' definition. Most commonly, information security was defined in terms of protection: protecting assets (both physical and digital) or protecting against unauthorised access. This could be argued as representing a data protection perspective on information security.

However, a number of the participants took a more subjective definition of information security. Rather than being about the protection of assets, for them, information security was more a way of being. B talked about information security as 'a way of life' that requires vigilant maintenance 'like milk in the fridge.' For A, information security was about 'doing the right thing' to minimise potential harms that can arise from security failings. In A's view his role as information security practitioner was to enable information and technology to be used for a good purpose, rather than stopping people doing things: 'as a profession we are now coming to the point where we have to add value, not prevent value.' This could be argued as representing an enablement perspective on information security.

A number of participants referred to the way that information security had changed over time. It was clear that a number of the participants believed that the change in the environment in which they operated provided at least part of the explanation as to why it was so difficult to provide a single universal definition of information security or why the traditional definition of CI&A may longer be appropriate.

One participant referred to information security as 'in the past' being about the protection of assets but now being about protecting services, because 'more things run now as services,' which means that information security is now much broader than it has been in the past. E, a consultant, who has worked in information security for over 20 years referred to the changing technological world and its effect on her concept of information security. When she first started working in security 'there was a closed environment' which meant that security was an internal issue which could be managed by the organisation itself. Now, security is 'looking at the whole wide world' and the issues for security were different to those which previously were developed and applied to the organisation's controlled environment. This interpretation reveals how information security has, for some, moved from being focused on protection to be being focused on enabling an organisation/individual to do something. It is a move from a more closed or negative "protection from" to a more positive or open "ability to". The skills and the capabilities that information security practitioners now need must reflect this more open position.

Similarly, G highlighted 'a real shift' caused by the Internet and new technology which has forced the information security discipline out of the world where it controlled the assets by 'keeping something locked away' and moved into a new world where information security is about ensuring that information 'gets used in the right way.' Participant I, another information security veteran, talked about how security had been seen as 'something in the

[56] See Harold F. Tipton and Micki. Krause, *Information security management handbook* (Auerbach Publications, 6th ed. 2007).

background' where there was no relationship with the business. Over time security moved 'out of the basement to become a much more business focused, business related area.''[57]

The idea that information security is now a much broader field was reflected in comments about the range of people now forming part of the information security community. In G's view the information security community, now extends beyond people who might call themselves information security practitioners and includes regulators and lawyers. For H, the information security community was 'all these people that now are doing things who have a stake in what you're doing or a requirement for your expertise.'

These findings, as to the changing and expanding nature of information security and what that means for information security practitioners, are important for a number of reasons. They indicate that the 'classic' definition of information security which underpins the standard approaches to information security may no longer be appropriate and that we need to re-conceptualise what information security has become. The findings also highlight how the change in the IT environment has moved information security from something that was controllable in the sense of the very clear boundaries around the IT infrastructure and the human interface with that infrastructure to something that is no longer controllable and which includes a far wider range of players.

4.3 NEGOTIATING RISK

All of the participants referred to risk and the use of risk in supporting the selection of security controls.

D saw risk and the discussion of risk with the business as a fundamental part of his role as an information security manager. In his view, his role was to help the business identify risk and then discuss the risk mitigation actions that could be put in place to deliver the solution in a secure way. Participant I thought risk was the best method of communicating the importance of security in a way that made sense to the business. For Participant I, risk made security more tangible to the business because 'you can get empirical evidence about threats and vulnerabilities and exposures and impacts.'

C worked for a large government organisation which had a well-established risk framework that allowed it to respond readily to risks such as natural disasters. C referred to the way his team would advise business of the security risks and then recommend actions to reduce the risks and then get the project or business owner to sign-off on the residual risk or agreement on treatment plans. As part of this process, the business would want to reduce the security team's assessment of the level of risk and not pay for the recommended risk treatments: 'They're not prepared to take those risks. But they don't want to fund the mitigations to them either.'

Risk, and its reliance on the need to protect assets from possible threats, may not be the only language that should be used by practitioners when talking about security with their stakeholders This is particularly the case where the need for information security comes

[57] The transition from information system focused security to business security has been noted in the literature. See e.g. Basie von Solms and Rossouw von Solms, 'From information security to…business security?' (2005) 24(4) *Computers & Security* 271.

into conflict with other organisational values, such as speed to market or cost savings. It in these situations of conflict that the practitioners' reliance on information security risk to support their position, or to 'concretise' the security issue seemed most problematic.

A number of the participants did not think that risk made security real or 'tangible' for the business. For some, couching the information security conversation in terms of profit (rather than risk) was a way of making the issue 'real.' According to one participant:

> There's no point in talking about hackers and breaches and weird and wonderful things that Hollywood portray to the CEO who really just cares about how he is going to make a profit next month.

However, the methods of "concretising" information security are fairly limited, indicating that further work could be done to visualise the different dimensions of information security.

The experience of many of the practitioners suggests that, in some cases, information security decisions may involve a contest that requires a much deeper understanding by information security practitioners of other organisational forces (such as politics) and the competing values that may underpin both information security and organisational decision-making and a more meaningful way to prioritise information security in management's agenda than the language of risk and the threat scenarios typically relied on.[58]

4.4 COMPLEX COMPLIANCE

A series of questions were asked around the regulatory frameworks applicable to the participants being interviewed. These questions included what legal obligations they needed to comply with and what benchmark they used to determine security the level of security required as part of their information security role.

There were no legal obligations that all of the participants universally regarded as being applicable to them in their daily work.

A small number of the participants referred to *Privacy Act* obligations. Although aware of the *Privacy Act* and understanding the requirements around it, A did not believe he was legally obliged to disclose any breach of that Act that he might uncover as a consultant. In his view, in his role as 'a trusted adviser' to his client he would raise a privacy issue with his client first and then work through it with them. By contrast, if he found evidence of fraud or paedophilia he would go straight to the CEO of his organisation and make a phone call with him to the authorities.

Participant E referred to compliance with US legislation that applied to her project but did not believe there was any other relevant legislation. I, who worked in the

[58] See also Debi Ashenden and Angela Sasse, 'CISOs and organisational culture: Their own worst enemy?' (2013) 39 *Computers & Security* 396 regarding the different discourses of information security from a CISO perspective and compliance as a 'driver' for information security.

telecommunications area, referred to regulations specific to telecommunication providers, which he described as 'not that prescriptive in terms of the security side of it.'

Similarly, there was no single benchmark referred to by all the participants, although a number referred to common standards, such as ISO 27001, PCI DSS and the Australian Information Security Manual (ISM).

For A, his benchmark for information security compliance is PCI DSS, which he believes is "pitched at about the right level in terms of its verboseness, its technical detail" although for those for do not understand "it becomes very overwhelming." Participant I referred to 'good sound practice' based on ISO 27001 and the ISM. He regarded these standards as not 'going over the top', and putting 'loads of controls in place' from a good corporate business practice point of view to 'give us a sound foundation for going forward from here.' E, working on a government project, had to comply with government standards and the ISM.

Another interviewee referred to a list of controls that 'you have in your head,' which he applied based on 'a judgment on how strong the control needs to be that you apply given the risks that you are facing.' H, who was in charge of a security operations centre, based security around metrics and a General Quality Management approach, asking questions like How much did it cost? What was the impact to the business? What was the time the business lost?

A number of participants saw standards as guides rather than prescriptive requirements. C said that standards give a general intent or 'vibe' rather than a prescriptive list of what the organisation can or cannot do. E referred to government standards and the ISM as 'minimum mandatory requirements.' If there was an opportunity to increase security then she would 'if it's within the scope of what we are doing and it's not going to cost a lot of money.'

For C, standards were not about providing a benchmark but about achieving better security as the outcome of process improvements. C was one of the only interviewees to explicitly refer to the importance of the continuous process improvement model which, together with risk, underpin ISO 27001 and other similar approaches to security (such as that adopted in the Australian Information Security Manual).

Only one of the interviewees referred to the Australian Privacy Commissioner's Guide to Security.[59]

A number of interviewees made the point that being compliant or being certified as compliant with a standard did not necessarily mean that an organisation was secure. For example, C referred to an assessment done of another organisation which 'had all the certifications' but which had security he described as 'appalling.' In his view, the organisation had 'fooled the compliance auditor' and taken a 'compliance journey' that 'achieved nothing.' B said that while compliance with standards may give a level of confidence you can still be vulnerable. For another interviewee, it was clear that 'compliance' was at a lower level than 'security' and more about 'ticking the box.' He said:

[59] Office of the Australian Information Commissioner, above n 24.

'People believe they want security and when they understand that they have a fair amount of work to get there, they just want compliance.'

5. DISCUSSION

We conclude the substantive part of our article with a brief discussion of some of the key issues emerging from our research findings. This brief discussion highlights areas of concern and possible future courses of action.

5.1 THE COMPLIANCE AND REGULATORY CONTEXT

The attitude of the practitioners to compliance with standards is an interesting finding given the focus on compliance in publications in the practitioner space.[60] More generally, these are important findings for the way that information security is regulated. There may be issues with regulatory frameworks which place responsibility on information security practitioners to act as delegated regulators and ensure a certain level of compliance, where there is little actual connection between the community and the regulators, there is little understanding of legal and regulatory compliance obligations and there is limited understanding of the contested environment that information security practitioners operate in.

In fact, one of the surprises from the research has been the absence of participant discussion about the legal requirements emanating from the *Privacy Act*. Given the Act is the primary source of information security legal obligation in Australia, we expected a much greater consideration and discussion of its application regarding the participants' working lives. This certainly was not the case and only a small number of participants mentioned the *Privacy Act* at all and none of the participants seemed to regard it as a significant factor.

As discussed above, PBR requires a closely engaged regulator to achieve clearly communicated outcomes and goals. There is little evidence of this from the interviews with participants and it was not possible to discern any sort of ongoing engagement between the OAIC based on the knowledge levels of participants. This is an important consideration. In theory, the principles adopted in a PBR framework should have the effect of shifting the responsibility for ensuring that the objectives of the principles are met from the regulator to the regulated, which in turn means that regulators must focus on the internal systems of management and control implemented by the regulated community.

The significant lack of understanding about *Privacy Act* compliance may be representative of an unwillingness on the part of the regulator to accept responsibility for overseeing the internal information security management systems that would be required in a substantive

[60] See e.g. Arif Mohamed, *Information security: The route to compliance* (2007) <http://www.computerweekly.com/feature/Information-security-The-route-to-compliance>; John Pavolotsky, *Compliance Best Practices for Information Security: A Perspective* (2011); SearchSecurity, *The Compliance and Security Balancing Act* (2014) <http://searchsecurity.rl.techtarget.com.au/data/document.do?res_id=1418834201_383&auth=YpOy5Aw6Wkw%3D>.

PBR system.[61] Moreover, it is very questionable as to whether the OAIC has the requisite resources, skills and understanding to be able to regulate the operation of these internal information security systems in the way contemplated by a PBR framework and a compliance-based approach.[62] As highlighted above, such a framework would require an active and highly engaged regulator that is driving an ongoing regulatory discourse.

It may be that PBR coupled with a compliance regulatory approach is the best regulatory system for the protection of personal information and the resolution of competing rights that are often implicit in privacy issues. However, it is not clear that this regulatory system when considered in the context of the resources and skills available to the OAIC is best suited to supporting the adoption of better security practices by Australian organisations and the requirements of information security practitioners as delegated regulators.

The extent that this is a study of potential regulatory failure in PBR frameworks is beyond the scope of this article but these are important issues that should be addressed further in the future. As regards the application of information security regulation, it is vital to determine whether in fact 'light touch' regulation results in 'no touch' understandings of the regulatory requirements expected of delegated regulators, in the form of information security practitioners.

5.2 AN INFORMATION SECURITY PROFESSION?

The fact that the information security practitioner group is so broad raises questions as to whether it is appropriate to group information security practitioners as a single group or profession. It may be that this single categorisation overly simplifies the differing roles of information security practitioners, obscuring the differences between them and making it difficult to identify the skills required for each of the different areas of competency.

Although the nine interviewees had different definitions of information security, there seemed to be general consensus that information security can be regarded as preventing the organisation achieving its business goals.

One interviewee said 'information security is quite often considered probably as a road blocker.' Another referred to a project that the security team became involved in where the security team 'kept asking questions' so that the business got upset and said that the security team were 'being obstructionist and stuff. It all got quite toxic really for some time.' C referred to how his team might sometimes be 'too forceful' when talking about information security. He said that often the 'people taking their advice' (being other internal teams), see that advice as a roadblock, which is not what is intended. Participant I said there was a need to get away from information security being seen as a 'pain' and

[61] See e.g. Jodie Signato and Mark Burdon, 'The Privacy Commissioner and Own-Motion Investigations into Serious Data Breaches: A Case of Going through the Motions?' (2015) 38(3) *University of New South Wales Law Journal* 1145.

[62] Ibid, 1178. It should also be noted that the OAIC's functions and resources have been severly cut back over the last two years. See for further details Richard Mulgan, 'The slow death of the Office of the Australian Information Commissioner', *The Canberra Times* (2015) <http://www.canberratimes.com.au/national/public-service/the-slow-death-of-the-office-of-the-australian-information-commissioner-20150826-gj81dl.html>.

information security people as giving more pain, causing issues and making life more difficult.

Notwithstanding the perception of information security as a road block, most of the interviewees saw their role as being to support the business or provide advice in a way that meant that security was seen as an enabler rather than a problem. One interviewee said he was not 'in the game of saying, "No"' but instead was interested in finding the best way to do something to have a business outcome.' C described his team's role as being about 'making sure that people understand that you are there to find a way to make something they want to do happen and not stop them.' D talked about how the role of the information security team was 'to enable business to do things' in a secure way, not to make the business 'put any activities on hold.' Another said that the security team are not there to make life difficult for the business but to provide support. Rather than 'taser-ing' people who do not comply with security policies, one security team now sends 'nicely-worded emails.'

This focus on positioning information security as an enabler rather than a road-block represented a shift by information security practitioners and therefore skills need to be re-considered for this more open approach to information security management. Overall, the findings from this research would suggest there is greater diversity amongst the practitioner community than currently thought, and there are opportunities to be gained from a better understanding of the diverse information security practitioner community. This diversity is much broader than the general differentiation between technical security practitioners and those with a management role which was referred to by a number of the participants, and perhaps also broader than existing workforce frameworks, such as the U.S. Cybersecurity Workforce Framework.[63]

Other research has referred to the complexity and diversity of the information security workforce, concluding in particular that the cybersecurity workforce in the US is 'too broad and diverse to be treated as a single occupation or profession.'[64] If cybersecurity or information security policy development is to be truly effective, then it is necessary to determine whether the same applies in Australia.

An extended study would help identify what the Australian information security community looks like, including the main positions, functions and roles of the range of information security practitioners working in Australia. Those findings could also be compared to the security community internationally, using existing studies.[65] This might help identify both shared and singular characteristics of different information security communities and perhaps sign post future development directions for those communities.

[63] NIST, above n. 51.

[64] Committee on Professionalizing the Nation's Cybersecurity Workforce, *Criteria for Future Decision-Making; Computer Science and Telecommunications Board; Division on Engineering and Physical Sciences; National Research Council, Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision Making* (National Academies Press, 2013), Conclusion 2, 2.

[65] See for example Frost and Sullivan, above n. 54, 36 which uses 39 categories of job roles in IT security taken from industry frameworks developed throughout the world but with a focus on frameworks from the European Union and the USA's National Initiative for Cybersecurity Education (NICE), as well as constructs in use in the United Kingdom and Japan.

This in turn would provide the evidence base to devise and offer a range of diversified training and skills development programs as well as creating and supporting interest groups that more closely fit the needs of the range of members of the Australian community, including pertinent regulators.

That said, it is important to note that the participants were either volunteers or people known to the researchers and comprised only a small sample of the information security community. Accordingly there may have been some gaps in terms of the skill sets of the people interviewed. For example, the interviewees did not include any person whose role might be regarded as within the "build" domain. This is one of the areas that should be addressed in future research.

In addition, the interviewees came from a range of different organisations including medium sized consulting businesses, a large non for profit organisation, af state government body and a large financial institution. It is likely that the roles and responsibilities of the interviewees were influenced by the size of the organisation and the sector it operated in. The relationship between different organisation types, the sectors they operate in and the types of security functions carried out within those organisations is also an aspect of this research that may be worth pursuing further. Again, an understanding of how information security is actually actioned in different sectors could provide the opportunity to provide tailored offerings for those different sectors.

5.3 FUTURE SKILLS?

As discussed above, a deeper understanding of the needs of the Australian practitioner community is likely to support the identification of the broad range of skills required by Australian practitioners to cope with the new and changing environment they are dealing with. This in turn would inform the development of policy, training and education most important to that community. From our research, and from the other studies detailed above, it seems that the major activities of most information security practitioners involve management, communication and negotiation type activities.

If this is the case then the main training needs for Australian information security practitioners (consistently with the recommendations from U.S. studies)[66] need to be more oriented towards the development of practitioner behavioural, interpersonal and management skills including. Programs for the development of these 'soft' skills for its members would also address comments made about the overly technical focus of the existing information security associations, which was a common feature of participant concern. Similarly, a common problem and concern identified by the participants was the view that the business did not understand information security or information security risk and that it was difficult to engage with the business. Again, suitably equipping information security practitioners with appropriate skills would assist them to communicate more effectively with 'business' components of organisations. The ability to get the 'message across' about the importance of information security will also enhance the depth of

[66] Ibid.

regulatory dialogue and thus assist information security practitioners to become the delegated regulators required of them by Australia's PBR framework.

6. CONCLUSION

Our findings have important implications for the ongoing development of information security regulation in Australia. We suggest that the effective regulation of information security, particularly in frameworks of delegated regulation, may have to be considered in a fundamentally different way. If information security practitioners are to be delegated regulators, they may need to be provided with a new skill set that enables them to adequately negotiate the complexities of information security regulation in a PBR environment. These skills are 'soft' in focus and orient towards processes of negotiation, conflict resolution and understanding institutional contexts. Building bigger and better controls is not the resolution here. In fact, such an approach may further isolate the security side from the business side in organisations. Furthermore, our research is not advanced enough to say whether our study is an example of the failure of Australia's PBR framework. However, as with skills, perhaps a whole new range of regulatory tools are required to assist the dense discourse required between regulators and delegated regulators to clearly relate the context of regulation to information security practitioners.

ACKNOWLEDGEMENTS

This research is part funded by the Australian Information Security Association (AISA) and an internal TC Beirne School of Law grant. We gratefully acknowledge funding from both sources.