Attacker-Centric Thinking in Security — Perspectives from Financial Services Practitioners

Caroline Moeckel
Royal Holloway, University of London
Egham, UK
caroline.moeckel.2012@live.rhul.ac.uk

ABSTRACT

In response to diverging perspectives on the usefulness of attacker-centric approaches in security, this paper examines the current role of such thinking in security, incorporating 12 in-depth interviews with senior financial services practitioners working in the areas of security, fraud and risk. The presentation of results is supported by a condensed systematic literature review on the topic and followed by the provision of a list of suggested guidelines on practical implementation strategies, enabling further theoretical reframing and extension.

CCS CONCEPTS

• **Security and privacy** → *Web application security*; *Human and societal aspects of security and privacy*;

KEYWORDS

attacker-centric security, attacker, adversary, threat modelling, financial services, usable security, human-computer interaction

ACM Reference format:
Caroline Moeckel. 2020. Attacker-Centric Thinking in Security — Perspectives from Financial Services Practitioners. In *Proceedings of The 15th International Conference on Availability, Reliability and Security, Virtual Event, Ireland, August 25–28, 2020 (ARES 2020),* 11 pages.
DOI: 978-1-4503-XXXX-X/XX/XX

1 INTRODUCTION

While threat modelling methods currently in existence use various foci and levels of formalisation [39], taking an attacker-centric approach seems contested in literature: over the last decade, Adam Shostack as a central figure in threat modelling and author of several key works in the field [40] has been a strong advocate against approaches requiring security professionals, developers and other stakeholders to 'think like an attacker'; stating that most security professionals will not be able to effectively and effciently threat model based on a relatively unstructured list of attackers or by simulating how a mostly unknown attacker is likely to think or act (potentially also introducing own bias [1, 40] p.41.

ARES 2020, Virtual Event, Ireland

DOI: 978-1-4503-XXXX-X/XX/XX

Other academic works in the area of threat modelling (e.g. Meland et al. [26]) follow this line of thinking, giving preference to asset-/risk- or system-centric views for their ability to model on existing elements such as data flows or stores. In contrast, Mead et al. [25] saw encouraging results for attacker-centric methodologies in their evaluation efforts in using attacker-centric 'persona non grata' representations of "archetypal users who behave in unwanted, possibly nefarious ways". The positive value of attacker-centric threat modelling is recognised by others, e.g. by Kayem et al. [19] in their comparative analysis of threat modelling approaches. 'Thinking like an attacker' has also seen wide uptake in the professional security community [13], with attacker-centric thinking also forming part of university courses [14]. However, many approaches to threat modelling, whether formal or informal, flex between different foci and perspectives, with e.g. Mead et al. [25] suggesting combining system- and attacker-centric modelling into a hybrid approach and Atzeni et al. [1] calling on attacker personas to prevent potential modeller bias encountered in other methods (e.g. attack trees). Deriving from user stories in agile software development, Hurlbut [15] describes the usage of attacker-based stories to support system-centric threat modelling in a commercial context. And despite his issues with attacker-centric threat modelling, Shostack includes attacker lists and personas in his book [40].

Inspired by this identified divergence in perspectives on attacker-centric approaches in security literature, this work seeks to provide an initial insight into attacker-centric thinking in practice. For this purpose, an interview study involving 12 senior financial services practitioners is carried out, inviting their opinions and ideas on such approaches in semi-structured, relatively open-ended and informal conversations. In addition to learning more about the ways these approaches are used as part of their daily work routines, their benefits and limitations as well as future potential are investigated in collaboration with the practioners. While the primary intention of this work is to reflect on the practical value, usage and limitations of attacker-centric approaches in security as a relatively narrow 'niche' topic, it is also hoped that the insights and data derived from the interviews with an elite group will support other researchers in their work and encourage critical discussions at an academic or industry level on this specific topic in the future.

To document this research, this paper is structured as follows: first, a condensed systematic literature review is presented. Secondly, the methodology employed, including the exact data collection and analysis methods, is outlined. This is followed by the presentation of the results from the primary data analysis — to help aid the reader, these are grouped around five emerging themes. An attempt is made to synthesise these results into tentative, but tangible guidelines and reflections on attacker-centric thinking.

2 BACKGROUND

In preparation to the practitioner interviews, a dedicated systematic literature review on the topic of attacker-centric approaches in security was carried out, using the works of Kitchenham et al. [21] on systematic literature reviews in software engineering and the recent example of a systematic literature review on threat analysis of software systems by Tuma et al. [45] as a guide. Topics researched included the level of research activity observed in the last decade, research directions, benefits and limitations as well as future potential indicated. Ten databases and platforms (e.g. ACM Digital, SpringerLink and Google Scholar) were scanned, using the search terms "attacker/adversary centric/-centred/-centered"; "threat modelling" AND "attacker" and "attacker model". Additionally, reference lists were reviewed for potentially related materials ('reverse snowballing'). Following review and selection[1], 32 papers in total were reviewed — due to the limitations of this paper, this section provides an overview on the topic in form of a compressed version with a selection of references from this review (available in full at [30]).

Understanding of 'attacker-centric' — Interestingly, no exact definitions of 'attacker-centric' beyond explanations such as the "perspective of an attacker's tools, motivations and objectives" [38] can be found in the sample. Overall however, an attacker-centric perspective seems to be understood and valued in two ways. Firstly, no attacks are ever committed without an attacker: "the adversarial element is an intrinsic part of the design of secure systems" [1]. Secondly, many studies mention an element of 'think like an attacker' or assuming the role of an attacker through attacker-centric perspectives (e.g. in Tariq et al. [42] or Yuan et al. [47]), with several authors also discussing this approach critically (e.g. Shostack [40]).

Techniques, tools and vehicles used — Attacker-centric threat modelling and risk assessments can be carried out and supported using a large number of techniques, tools and vehicles. This is also strongly reflected in the sample, confirming the many ways that attackers may form part of threat modelling and analysis approaches, ranging from widely recognised threat modelling elements such as STRIDE [47], attack-trees [24], misuse cases and (anti-)scenarios [47], misuse maps and diagrams [26], anti-scenarios [42] to truly attacker-focussed approaches such as attacker personas [1] or similarly the 'persona non grata' in Mead et al. [25].

Perceived benefits of attacker-centric approaches — The number of explicitly stated benefits of using an attacker-centric lens is limited in the sample. There seems to be an underlying perception however that understanding or modelling attackers behind past or potential future attacks is beneficial, e.g. for assessing and subsequently prioritising threats [41], designing and testing countermeasures [6] or forensics purposes [35] or to "provide general insight into the attacker's mind" [6]. Several authors see the creation of reusable threat agent or attacker reference libraries as useful for future security practice [6]. But attacker representations are also considered extremely valuable to stakeholders: they may support their decision-making and provide confidence in "emergency response situations" [35], but also aid day-to-day communications. Yuan et al. [47] and Tariq et al. [42] also see an attacker-centric perspective as a vehicle of collaboration — enabling and engaging developers, security professionals and other stakeholders to consider illegitimate use cases in product designs, but also to better understand the implications on security caused by their design decisions.

Validation efforts — Most studies have included a validation approach, with many based on case studies, e.g. Fraunholz et al. [11] amongst many others. Other validation strategies include comparisons to similar approaches in literature (also [11]) or exemplary illustrations and demonstrations (without a specific real-world case study, e.g. [24, 47]). Several authors will use tool support for their validation effort: Meland et al. [26] use the threat modelling tool 'SeaMonster', while Faily & Fléchais [10] use their CAIRIS platform. Valuation efforts are however not limited to this: interviews with stakeholders, explorative surveys with subject matter experts or heuristics are mentioned as ways to assess and validate the quality of threat models [40, 42].

Limitations and issues identified — Despite these validation attempts, authors in the sample have identified a number of limitations to their studies — not all of these are specific to the attacker aspect in threat modelling, but highlight overall current methodological weaknesses identified in the sample. Firstly, attacker-centric approaches and tools like attacker lists or personas may not offer enough structure for modellers to reliably identify threats [40] — they demand a very good, often unrealistic understanding of potential attackers, making them prone to error or bias from the person undertaking the modelling. There may also be problems with validation and quality assurance: here, an overreliance on case studies and illustrations and lack of measurements for assessing the quality of outcomes for threat modelling processes is seen as problematic [27, 45]. Additionally, many diverging directions are already in existence, which prompts Karpati et al. [17] to suggest that "new modelling methods should be extremely well motivated by challenges for or limitations of existing methods" [26]. The issue of reusability is also brought up here — reusing threat models and their results are viewed as beneficial "for knowledge sharing and to achieve a general increase in efficiency and quality" to the process by Meland et al. [26] — efforts in this direction seem limited to date.

Implications for practitioners identified in literature — Many of the limitations identified will have direct impact on practitioners and their ability to use attacker-centric approaches effectively. Ease of adoption and continuous usage may be hindered by the limited tool support and guidelines [45]. In particular, small and medium sized organisations with limited resources are thought to seldomly employ threat modelling practices [44]. Expectations towards practitioners set by threat modelling may also be unrealistic: asking practitioners such as developers and engineers 'to think like an attacker' may be a challenge [25, 40, 44]. Karpati et al. [17] also note that current threat modelling methods may not satisfy all stakeholder requirements in the best way, for example support them optimally when communicating with other (senior) stakeholders in their organisation. In contrast, threat modelling is seen to help optimise security investment and lead to cost-effective security in organisations, along the lines of 'how secure is secure enough?' [40].

[1] Originally, 94 items were identified for potential selection. Inclusion and exclusion criteria include relevance to subject area, adequate detail on how attacker behaviour and characteristics are used as well as sufficient quality and reliability (B rating in CORE database [45]).

3 METHODOLOGY

To examine how digital banking professionals consider attackers in their daily practice, a qualitative data collection through 12 semi-structured interviews with senior practitioners at a case company was carried out. In their well-structured study on UX professionals working in an agile context, Bruun et al. [4] view such a case study approach as "appropriate for developing an understanding of a contemporary phenomenon in its real-life context" (attacker-centric thinking in banking). The case company is a large European banking organisation with over 50,000 employees, covering retail, business and corporate banking with a dedicated security and risk function.

The author is aware of the restriction to one individual company and resulting potential implications (e.g. bias to specific organisational practices) — at this point in time however, the results were deemed as insightful and conclusive enough to warrant interim publication. An update involving practitioners from additional financial services companies may be of value in the future.

3.1 Data collection

Managers at middle, senior and executive level in financial services institutions working in all fields of security, fraud or risk functions form a corporate elite[2]. This group can be difficult to access and recruit for in-depth interviews due to organisational gatekeeping, time constraints or lack of compelling reason to participate ("what's in it for me anyway?" in Thomas [43]).

The researcher benefitted from a unique position of being affiliated with a large financial services institution, which provided an entry point for recruitment and initial access to a small group of senior practitioners who were also prepared to introduce the researcher to some of their contacts in the organisation. The positionality of the researcher can be described as follows: while the researcher was an employee and therefore colleague of the participants (an insider), she was also an outsider as she didn't know any of the individuals personally and had never worked with them before or even in the same area. Rather than taking a binary insider/outsider position, the researcher aimed for a collaborative, transitional perspective, incorporating both relative objectivity (outside view) and organisational and subject knowledge (inside view) [31]. In addition, it was made clear throughout all stages that the position of the researcher was the one of an academic rather than a colleague at this point ('student role' [23]). At the same time, the study and work with the researcher was positioned as a two-way relationship, where the researcher would feed back on the results and establish a longer-term dialogue with the participants if of interest ('consultant role' [23]).

The individuals initially approached held various security-related positions in the organisation and had diverse backgrounds (e.g. theoretical computer science degrees or extensive professional experience in the area of fraud) as well as levels of seniority, which ensured an initial 'sample seed diversity' [20]. A first round of four initial interviews was held at this point (August 2018) and analysed (while two further interviews were held at the time, the interviewees choose not to participate). Given the encouraging results, a further round of eight interviews was undertaken in early 2019, also looking to broaden the scope of participants in areas like fraud and risk (as recommended by first round participants).

Table 1: Overview of study participants*

#	Role	Area	Seniority
1	Threat Intelligence	Security	Manager
2	Threat Intelligence	Security	Senior Manager
3	General security	Security	Senior Manager
4	General Security	Security	Executive
5	Threat Intelligence	Security	Manager
6	Operational Risk Mgmt.	Risk	Senior Manager
7	Operational Risk Mgmt.	Risk	Manager
8	Operational Risk Mgmt.	Risk	Senior Manager
9	Fraud Strategy	Fraud	Executive
10	Fraud Strategy	Fraud	Executive
11	Fraud Strategy	Fraud	Senior Manager
12	Fraud Strategy	Fraud	Manager

**in order interviewed*

In total, 12 semi-structured, qualitative interviews were conducted (refer to Table 1), based on the guidelines on qualitative interviews in Patton [34] and more specifically in an HCI context from Blandford et al. [3]. The interviews lasted between 45 to 90 minutes, either face-to-face on company premises where possible, via video conferencing or on the phone.

An interview guide built around 3 themes (refer to Table 2) was used by the researcher, enabling a conversational interview style without compromising on consistency — the aim was to enable senior practitioners in financial services to share their own thoughts and opinions freely, however with a level of control from the researcher (avoiding a 'power shift' where the participant dominates and directs the interview [43, 46]).

Adhering to company guidance to avoid audio recordings, extensive notes were taken throughout the interviews by the researcher (a process participants were very familiar with from other internal interviews, e.g. for recruiting purposes). The exact write-up of these notes was shared back with the participants for review and sign-off, firstly, to aid confirming the reliability of the data collected ('member checking'[3]), but also to support the process of gaining consent in writing from all participants. This was viewed as highly important given the sensitive nature of this study, where senior members of an organisation would potentially discuss security-related aspects of their role and every day work [29].

[2]In this study, the following understanding and definition of the term elite brought forward by Welch et al. [46] in their work on working with international business elites is largely agreed on: "[...] occupies a senior or middle management position; has functional responsibility in an area which enjoys high status in accordance with corporate values; has considerable industry experience and frequently also long tenure with the company; possesses a broad network of personal relationships [...]".

[3]Member checking is a form of participant validation — results, for example from interviews, are returned to the participants/interviewees for them to check their accuracy and the provided results matching their experiences [2]. At this point, participants/interviewees may also request to alter certain details (e.g. due to misinterpretation) or ask for information to be removed (e.g. to ensure they remain anonymous).

Table 2: Overview of interview process and structure

Stage	Activities and content theme
Pre-interview: first contact	Introduction of researcher and planned study; Share general study information sheet; Decision to participate/exclusion from study by the researcher
Pre-interview: second contact	Option for further questions regarding study; Arrange interview practicalities (e.g. time/date, means); Share participant information sheet; Decision to participate/exclusion from study by the researcher
Interview: theme 1	Participant's role in organisation; Career pathway, education
Interview: theme 2	Attacker-centric thinking in daily work practices of the participants; Usage of informal or formal attacker representations (e.g. personas/taxonomies); Examples of such representations
Interview: theme 3	View on the future potential of attacker-centric thinking; Future security trends or emerging threats in relation to an attacker focus
Feedback: first stage	Share conversation notes and re-share participant information sheet; Participants to provide consent to use data or request changes (via email)
Feedback: second stage (optional)	Share amended conversation notes for participant consent (if any changes made); Further opportunity for follow-up questions or sharing of further materials from the researcher/participants

No security countermeasures or protection approaches explicit to the organisation were discussed and included in the results, thus mitigating the risk of negative implications for the organisation or individuals. To protect the confidentiality of the participants, all data was used anonymously and identifying information was removed or anonymised. The study was completed following the relevant ethics review process of the researcher's academic institution (under Full-Review-1194-2018-08-29-11-07-PWAI216 and -1624-2019-04-02-21-21-PWAI216).

3.2 Data analysis

A flexible and largely explorative, yet structured method of data analysis was required to not restrict the open-ended nature of this research, but without losing track of the underlying research questions posed. For this purpose, thematic analysis as a primarily inductive, iterative analysis process to identify, analyse, organise, describe and report patterns (themes) found in the data collated [8] was chosen (see Figure 1 for examples). Thematic analysis is frequently used in qualitative academic HCI and commercial UX research, e.g. in the case study research by Bruun et al. [4] investigating the role of UX professionals in agile development practices.

NVivo was used as a software package to support the organisation and coding of the conversation notes, review of the code structure and for the ongoing reflective memo writing. A number of different coding methods (based on the profiles provided in the coding manual by Saldaña [37]).

Analysis and coding were initially completed for the first four interviews of the first round, followed by an academic peer review (by three senior researchers in the field of information security). The relatively low number of interviews however meant that theoretical saturation (where no new data and ideas emerge from the data collection [7] ch.1), had not been reached at this point in time, prompting the need for further data collection (second round of interviews). Similar themes and elements kept re-occurring approximately after a total of 10 interviews had been completed, indicating a level of theoretical saturation (with the sample restriction to one case company).

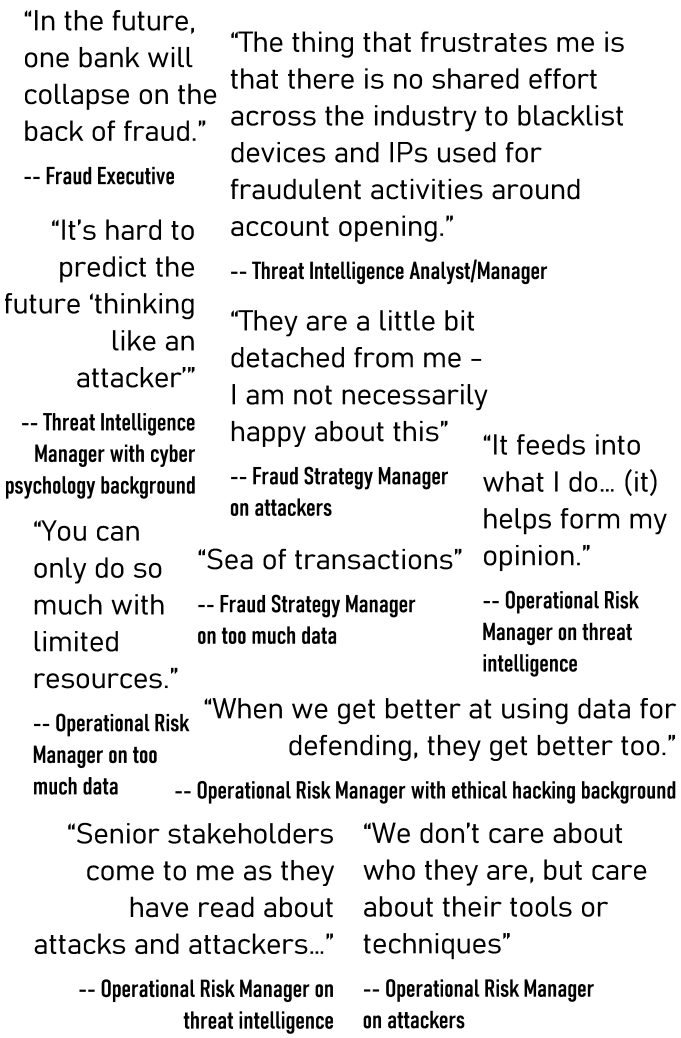

Figure 1: Examples of practitioner quotes from interviews

4 RESULTS

4.1 The underlying basis: threat intelligence

Building a comprehensive picture of the threat landscape — threat intelligence, which can be defined as "the output of analysis based on identification, collection, and enrichment of relevant data and information" to inform security decision-making [36], is viewed as paramount for understanding and modelling threats against an organisation — this also includes intelligence on attackers. The interviewed practitioners were aware or actively using a number of threat intelligence approaches and resulting data insights, mentioning e.g. initiatives to source contextual attacker data to trace actors on the darknet via research and intelligence suppliers, but also more generic attacker profiling efforts referring to e.g. attack methods and tools or demographic factors including the geographic origin of attacks — basic attacker profiling was mentioned by almost all participants. In this context however, limitations were described as to what data and information banks could source for their threat intelligence programmes. Furthermore, the right organisational setup regarding threat intelligence mattered to one participant: in banking, many attacks and crimes cross the line between the cyber and physical world — it therefore made sense to move from separate intelligence teams to an aligned team spanning physical and cyber security, including ATM and mobile security (threat modelling senior manager).

Information gathering, sharing and reassurance — threat intelligence also plays a key part in informing (and reassuring) senior stakeholders about current threats, as for example told by an operational risk manager: "senior stakeholders come to me as they have read about attacks and attackers...". Other security, risk and fraud teams across the organisation will heavily depend on threat intelligence teams and their analysis as a way of thinking about attackers in their everyday roles, e.g. through threat radars and assessments (as mentioned by a threat intelligence manager).

Open source information: defenders vs. attackers — while open source information (e.g. social media networks such as Twitter) is an extremely important intelligence source for defenders, the same logic applies for attackers: they will also be using open source intelligence, for example to find out about new attack surfaces into banks or their suppliers. This 'arms race' between these two groups was discussed in detail by one of the risk managers with an ethical hacking background, e.g. "when we get better at using data for defending, they get better too". Open source information may also have a far more direct attacker focus: one participant mentioned the possibility of identifying vague direct threats against the banking organisation through open source monitoring (e.g. a planned attack could be announced or arranged via social media). Similarly, media impact and reporting on (potential) attacks and attackers was also seen as a key aspect to be monitored by one of the security executives.

4.2 Purpose and gains of an attacker focus

Supporting a strategic view — in terms of benefits gained from an attacker-centric perspective, an attacker focus was seen as more helpful for a "tactical level security perspective" (fraud senior manager) or a "broad and shallow macro-level strategic view" (operational risk manager) rather than modelling threats directly on attackers. The threat modelling senior manager and security strategist in the participant group stated "there is a tendency to look at things at a very granular level rather than from a strategic point of view", preferring a strategic view as a proactice approach to identify and assess potential future threats. Furthermore, using exemplary attacker group representations was seen as beneficial for taking a "proactive approach to identify and assess potential future threats". These statements are certainly related to the criticism exercised against attacker-centric modelling by Shostack ([40] p.40) — while using attacker information or representations to model specific threats and attack techniques might not work very well, using such information for taking a more strategic, long-term view may be a more efficient starting point. This assumption seemed generally supported in the sample, e.g. by a threat intelligence manager: "it's hard to predict the future thinking like an attacker" or by an operational risk manager: "we don't care about who they are, but care about their tools/techniques".

Another strategic aspect around 'knowing your enemy' was also mentioned: rather than informing exact countermeasures and mitigations to be used, the nature of the expected attacker (group) behind an attack may define the strategic defence approach, i.e. organisations under attack could decide to focus on 'damage limitation' only if up against powerful nation state attacks (as told by the security executive) and also by a threat intelligence manager: "...knowing who is behind the attacks may help to understand how far they will go". This is likely to refer to organisations focussing their efforts to maintain or restore minimum services during or after an attack (and communicate the chosen approach appropriately to the public, as mentioned by an operational risk manager) rather than trying to fully return to the pre-attack state too quickly.

Understanding the criminal business model — gathering as well as analysing attacker information was largely seen as helpful in understanding the business model of organised groups, supporting a holistic view of the overall security ecosystem,"making sense of what's happening" (threat intelligence manager). Specifically, "understanding people" is seen "as likely to mean a better understanding of cyber operations" and business models (as told by a threat intelligence manager). The attribution of the globally devastating WannaCry ransomware attacks to North Korean state-sponsored hackers was used as an example to illustrate this: explaining WannaCry as an attack from a nation state actor rather than an independent group "made sense" to them (due to the large scale of the attack and the previously unclear motivation behind it). It was also seen as helpful for future modelling purposes, where such group examples could then be included, e.g. in threat scenarios.

Similarly, understanding further business model elements such as 'hackers for hire' was mentioned in this context by a security executive, with a senior manager distinguishing between 'hands-on' attackers and 'criminal managers' recruiting or contracting services for large scale attacks (explicitly mentioning the NSCS report on understanding the online business model behind cybercrime [32]). Here, the complexity of criminal business models was further hinted at: the same hackers for hire may be recruited by different criminal groups (or identical or at least similar malware may be purchased or commissioned as mentioned by a threat intelligence manager) — meaning that the same attack patterns and signatures may be

present across various groups and attacks. Overall, participants seemed to talk confidently about the business model employed by attackers, e.g. a fraud senior manager speaking of "massive organised criminality with call centre-scale type operations: huge, organised, sophisticated and successful at scale", "trying to run a business just like we are".

4.3 Considerations for practice

Attacker modelling in practice: view of existing groups — considering attacker groups and relationships seems to form an important element in modelling attackers in the organisation, as evidenced by two participants talking about this aspect. Group information is seen as more relevant than information on single attackers: "[threat intelligence] doesn't usually go down to the individual, but group levels" (threat intelligence manager). This is supported by a threat intelligence senior manager describing threat scenarios often modelling attackers on past experiences or incidents as well as existing groups, employing a neutral label rather than an exact group name. As an example of an existing group used as a blueprint for practical modelling, Lazarus is mentioned in the interview (refer to [18]).

Attacker modelling in practice: threat libraries, scenarios and attack path maps — a number of approaches including attacker-centric aspects are mentioned by the practitioners in the sample. A threat intelligence manager describes working with a customised cyber threat lists created through collaborative industry efforts, but also the usage of existing databases and libraries such as the MITRE Common Vulnerabilities and Exposures (CVE) list [28]. Threat scenarios are mentioned (albeit without specific procedural detail): "thinking through a scenario from an attacker's perspective and trying out what they could do" (threat intelligence senior manager). This is in line with existing approaches in the banking sector — Green for example introduces a structured approach to 'cyber scenario planning' based on threat actors and impact analysis for a number of scenarios [12]. Three of the participants also describe the importance of mapping the attack path, considering potential or previously observed entry points exploited by attackers at either an individual user or at an organisational level — industry-wide efforts may also support this through sharing such maps and experiences, e.g. at which layer of defence the attack was ultimately stopped (as told by a threat intelligence manager).

Representations of the human attacker — an interest in attacker profiling including demographics like geographic location or nationality is displayed by several interview participants, with a number also referring to specific groups: "I am aware of different attacker profiles such as internal fraudsters, members of a gang..." (fraud strategy manager) or "...distinct attacker groups are used e.g. political/ideological, organised crime..." (security executive). Four of the participants also mention the concept of attacker personas, e.g. "human representations such as personas may help to serve as a baseline and help to design against a large group of people/fraudsters, understand them better and visualise the knowledge we already have" (fraud strategy manager) or specifically for the case of money mules: "money mule data, risk profiles and demographics are known... usage of datapoints/analytics to identify money mules and fraudulent accounts can help to create persona profiles" (security executive). Human attacker profiles are also viewed as beneficial for practical aspects such as security awareness or to train staff (operational risk manager) or to compare patterns of malicious attacker and genuine customer behaviour for pattern analysis in fraud prevention (fraud senior manager). Lastly, one participant (security executive) also mentions support for victims as crucial, based on "cybercriminals harming people, not just banks".

Attacker determination as a new profiling dimension — another valuable insight resulting from an attacker-centric approach is attacker determination, as mentioned in two of the interviews (security executive/threat intelligence manager). While motivation of the attackers is considered in most attacker categorisations, determination is not mentioned specifically. But according to the interviews, the level of determination in the attacker, as well as the nature of motivation, is seen as important for defence. Knowing who is behind attacks is seen to help understand how far they will go, with for example nation state actors and other 'officials' as attackers likely to behave differently to professional criminals — this level of risk taking and behaviour is explained due to them being most likely to be in less danger of being prosecuted in combination with an assumed high levels of available resources.

4.4 Integrating into the business environment

Work routines and attacker focus — most participants acknowledge the presence of some level of attacker-centric thinking, methods or techniques in their everyday work: attackers may play a role in job routines e.g. "as part of threat radars and assessments" (threat intelligence manager) or when working with tools, e.g. for fraud analysis and monitoring. Two of the participants also mentioned the problem of "too much data" in this context, making analysis at an individual attacker level difficult. When describing their roles, most participants also talked about the importance of collaboration to distribute attacker information across different functions of the organisation, e.g. through providing threat intelligence data, helping business areas through providing consultancy or by creating a proactive, "generative" risk culture to be "channeled into risk teams and the wider bank" (operational risk senior manager). As already indicated, attacker information may support such a collaborative culture, e.g. by helping to raise security awareness or to train staff (as told by an operational risk manager). However, a fraud strategy manager also made clear that he 'realistically had no time to think about attackers/adversaries on an everyday basis in his role' and that attackers therefore felt "a little bit detached to me... I am not necessarily happy about this". In direct relation, he and another participant (threat intelligence manager) emphasised the importance of "time to think (and not necessarily as a brainstorm/group thinking exercise)" and to "slow down" to "make things better" and "accommodate security and balance customers needs/wants/expectations". A fraud strategy manager also stressed that, just like with other organisational aspects, skills, experiences and knowledge relation to attackers, are difficult to record and retain in modern workplaces undergoing constant change (including staff movements).

Balancing business, customer and security needs — attacker information naturally only forms a small part of everyday routines and task of the digital banking practitioners interviewed: they are balancing a number of perspectives and stakeholders, focussing on business needs and meeting regulatory requirements. While

security solutions, mitigations and the plugging of control gaps and their impact need to be costed up internally (security executive), external factors such as regulatory developments but also the competitive landscape (a senior fraud manager mentions the example of "recent industry developments which may have an impact on customers, e.g. the latest 'fraud guarantee' initiative from a competitor") make this a complex environment to operate in and apply attacker-centric security principles to. On balancing risk and security with business requirements and customer needs, a risk senior manager views "cybercrime and cyberwarfare as a continuous and growing risk also for banks — this and rising customer expectations (better/faster) need competent people and the right controls". He underlined this customer focus taken by the organisation by describing a "fix-and-learn-approach" (fix it for the customer first and conduct a post-review) as part of an ongoing and iterative review of security controls.

Mapping and securing digital customer journeys — the concept of the digital customer journey and its relation to attackers is discussed by almost all participants: it signifies the path users and potential customers take to move through service and product sequences offered via the banks' digital channels including online and mobile banking. An operational risk manager working in technology explains that a "further move towards a 'digital bank' means external threats become more important... so further understanding of attackers would be useful". To accommodate this, "threat modelling of the customer journey at a transactional level (end-to-end including user registration)" is described by a fraud senior manager, and a threat intelligence manager has worked with "fraud process end-to-end mapping" where various user and attacker types (or personas) can be inserted into the sequence ('follow the money'). As individual elements of the journey may deter or encourage fraudsters, e.g. the login element or registration and account opening processes, they need to be analysed in detail, including related user behaviour, e.g. push notifications fatigue (as told by a fraud senior manager and security executive).

Changes and new innovation to the customer journey may have a 'knock-on effect on fraud', therefore requiring risk assessments of the new functionality and "a look across the entire digital ecosystem as a potential fraud aggregator" — this is "in contrast to a generic model to explain fraud occurrences, but specific to customer journeys" with the aim to 'build security in' (as told by two fraud senior managers). Potential and previously encountered entry points of attackers can be mapped against the digital banking ecosystem and specific customer journeys, also considering non-digital, traditional elements like branches as vulnerabilities (e.g. for opening new mule accounts as mentioned by a security executive). However, a threat intelligence manager is critical of this approach in the future as "the question around which entry route an attacker could use becomes non-feasible/obsolete with increase in large, complex and interconnected technologies" (and the related difficulty to accurately and completely map the related customer journey).

4.5 Future directions

Data-driven attacker modelling — practitioners in the sample generally expect attacker information to play a role in their future work, but with a strong focus on data patterns rather than informal human attacker descriptions. "Because ultimately, defining and making these exact attacker profiles useful is so difficult" — the overall expectation for a fraud senior manager is to see more data-driven initiatives which may also include attacker information, e.g. data tracking digital footprints of devices or other biometric information for profiling. Several participants mention machine learning as a future opportunity to watch in this field, e.g. "data has always been in the focus to understand and prevent fraud and cybercrime patterns, but it will get even better (for example through machine learning to build fraud profiles)" (fraud senior manager). A security executive also recognises the potential to detect money mules and related patterns with the help of machine learning. At a more generic level, a (not further defined) "development towards scientific modelling for cyber risk" is expected by an operational risk manager in this context.

Emerging technologies as a risk and opportunity — in contrast to the last point, machine learning (ML) and artificial intelligence (AI) is also seen as a potential attack vector in the future: "another potential risk lies in the area of ML/AI: if this is not truly understood, unintended circumstances may arise from this. There is a risk for 'machine bias' and 'bots getting too clever'. Further difficulties in this area may be the difficulty to prove to the regulator what underlies decision-making. Lastly, there is the opportunity for manipulation (unintended or malicious)" (as told by a risk senior manager). Attacker-centric views are seen to likely play a role in designing new controls around emerging threats and changing threat landscape, and to understand new security economics by an operational risk manager in the sample. Not directly related to attackers, participants mention other aspects on their professional 'roadmap' for the near future, e.g. secure customer authentication or regulatory requirements. A threat intelligence manager explicitly highlights future thinking around attacks against internet-of-things and home devices or blockchain applications already presented in theoretical academic literature, but in his opinion requiring further definition of specific business cases and scalability. Lastly, data sharing between banks and other companies is viewed as a new opportunity (e.g. insights and business opportunities) and challenge (e.g. privacy, data protection and customer expectations that can't be met), with a risk senior manager citing the example of a UK challenger bank offering the switching of energy suppliers in-app to their customers.

Increasingly complex and interconnected systems — the digital banking environment of the future is complex, with pressures added by competitors, regulators, customers as well as technology and security requirements to be met: "it's only going to get harder to understand and will become more complex the more interconnected systems get. There is a number of significant influences such as cultural, technological, customer needs and wants or fraud risk. Examples would include third party systems such as Apple/Google Pay having an impact on internal processes or timelines" (as told by a fraud strategy manager).

Threat readiness and proactive attitude — the question on using attacker-centric approaches in the future yields limited insights, but attacker information is seen to play a role going forward in threat readiness. Threat readiness as a discipline can be explained

as looking into 'unlikely' threats and establishing probable mitigations and solutions for them. In regard to future threats, potential data breaches are identified as something to analyse further (as mentioned by a threat intelligence senior manager) — here, an attacker focus is seen as useful, addressing questions about what data would attackers be most interested in and what seems most valuable to them. Three participants also talk about levels of insecurity around emerging risks, e.g. an operational risk manager: "...while we often encounter the same risks, the landscape is changing, with new risks emerging and risks we have never seen — leading to an uncomfortable position". At the same time, they advocate a proactive attitude to threats and risk, e.g. a threat intelligence manager stating that "as with all the models in the world, if you are not ready for something new, they are not helpful" or an operational risk manager demanding more decisive dealings with threats.

5 DISCUSSION

Based on the insights and learnings brought forward so far, a list of 12 recommendations and guidance points on the usage of attacker-centric approaches in security is attempted in this section. The second part of this section reflects on the key findings in this paper, also looking into the future of the research topic.

5.1 Recommendations and guidance notes

(1) *Consider attacker-centric approaches to develop a strategic view on threats and security.* A key insight gained from the analysis in this work is the usage of attacker-centric approaches in a strategic sense. Using models of attackers or attacker groups (even informal ones) and related threat scenarios may potentially help to develop a strategic view on current and future threats. While the actual implementation for such an approach is likely to vary across organisations and further research would be beneficial, this realisation seems to be of significant practical value. It also aligns with the understanding that attacker-centric threat modelling is often ineffective (acknowledged in the next point). It may ultimately be better suited for another purpose like supporting a strategic view on security.

(2) *Recognise and accept limitations for attacker-centric approaches.* While this paper has focussed on attackers and attacker-centric approaches, the limitations of such approaches need to be understood if they are to be used effectively. Although these limitations may differ for the context of application, one of the most important realisations is certainly the perceived ineffectiveness of attacker-centric approaches for structured threat modelling — here, approaches deconstructing the system and data flows may provide better guidance to most modellers.

(3) *As an academic, learn from security practitioners (and vice versa).* The analysis in this work shows a discrepancy between academic research themes and topics that matter most in daily practice: while formalisations and frameworks dominate the academic space, daily security practice includes threat intelligence approaches and far more informal modelling efforts. It is felt that both sides would benefit from bridging this disparity, with an interest in academic research also indicated in the practitioner interviews.

(4) *Benefit from attacker-centric approaches to understand attacker ecosystem and criminal business models.* While this point was highlighted by practitioners, it was not evaluated in much detail in reviewed academic materials — this seems like a missed chance and further research in this area would be of value, for example to assess the exact benefit provided by such approaches, but also potential methods and procedures that can be used in this context.

(5) *Choose from a range of attacker-centric approaches with varying levels of formality and required effort.* To integrate attackers into daily security practice or academic research, there are a variety of methods and techniques to choose from, for example abstract attacker models, attack path maps, attack trees, misuse cases and threat scenarios, but also attacker personas or typologies. It is also crucial to realise that attacker-centric approaches can be implemented to varying degrees — they may supplement existing methods or form a fundamental part of a security programme.

(6) *Use attacker-centric approaches as a communication or training tool.* Given the stated strategic benefits and the often visual nature of attacker-centric approaches like attacker personas, typologies or digital journey maps may help to explain current security trends to senior stakeholders, e.g. provide assurance around media reports or to make a case for security spending. These attacker-centric tools may also play a role in training exercises with security and non-security teams, e.g. to raise security awareness or evaluate current work practices.

(7) *Actively look for and address potential biases present in security teams.* Personal bias may be present in security teams when thinking about attackers — individuals may for example over- or underestimate the threat originating from certain attackers or attacker groups (based on experience or knowledge). This potential presence should first be acknowledged and secondly countered if possible — personas are seen as a method to address such biases in user-centred design and hence may also be of benefit in an information security context.

(8) *Consider attacker entry points in the (online and offline) digital customer journey.* Practitioners working in the area of digital banking in our interviews place great emphasis on the model and visualisation of the digital customer journey as a series of steps customers will move through when completing a bank service or sales processes. Mapping attackers, their activities and resources (for example in the form of attacker typology types, personas or path maps) against this sequence may help to identify potential vulnerabilities and attack entry points when assessing existing journeys, but also changes to be made or entirely new innovations.

(9) *Integrate attacker-centric thinking into the assessment of emerging technologies.* As ML and AI have moved from theoretical concepts into practice used by banks, attacker-centric thinking may also help when identifying and assessing threats, risks and the related need for new security controls.

(10) *Start thinking about how attackers and threat modelling can be built into agile ways of working.* As agile ways of working with multidisciplinary teams become more widespread across organisations around the world, ways of integrating threat

modelling into these processes need to be identified. Davoust [9] has suggested for teams in organisations to be trained to use agile and continuous threat modelling and uses an attacker profiling exercise to support this. Collaboration within and between teams throughout the development process seems crucial in this context, recognising that everyone is responsible for security and it needs 'to be built in' rather than 'bolted on'. While no comprehensive frameworks around this have been found here, concepts such as evil user stories ("As a hacker, I can send bad data in HTTP headers, so I can access data and functions for which I'm not authorized", in OWASP [33]) seem like an interesting starting point to combine attacker-centric and agile approaches to security.

(11) *Collaborate around attacker-centric thinking and share attacker-related information.* Threat intelligence and the sharing of attacker information should underlie the concept of attacker focus in practice across the organisation, and beyond where possible. This should be extended into collaboration efforts around attacker focus, both within organisations (e.g. through agile working sessions and workshops examining journey maps and related attacker entry points) or in the form of industry-wide initiatives and working groups. Tools and techniques enabling such sharing and collaboration efforts effectively have also been discussed widely in literature, e.g. attacker typologies or personas, but also threat and attack pattern libraries (e.g. Intel Threat Agent Library [16] or CAPEC [5]) — re-using such existing frameworks can also enable scalability, comparability and reduce duplication of efforts.

(12) *Lastly, publicise insights and learnings in this area to support others.* Given the limited amount of research currently presented, further practical and academic efforts seem required to advance this field of research. Considering the amount of valuable statements from only a small number of initial interviews, there seems to be significant potential for further insight to be gained. It is therefore crucial that practitioners consider making some of their learning and experiences public, for example through presentations at industry-specific or academic conferences.

5.2 Reflection

(1) *Further definition of expected benefits required* — exact benefits and outcomes associated with the usage of attacker-centric approaches often remain unclear, as evidenced by the reviewed literature items in this research. There seems to be an underlying assumption that knowing more about attackers is helpful in the context of modelling threats and supporting security practice in general, although the exact motivation and the 'why?' behind using attacker-centric approaches are often ill-defined. While this research provides an initial step into this direction (e.g. the move towards a higher-level strategic view over granular modelling efforts), this current shortcoming should be acknowledged and ideally be featured in future research.

(2) *Many different methods in existence currently* — current approaches which use attacker information or employ an attacker focus vary significantly in terms of effort required as well as rigour and detail involved. Hence, there seems to be a significant potential for unification and formalisation of tools and techniques, with the aim of establishing realistic and efficient options for reusability, comparability and shareability.

(3) *Changing perspectives to a more strategic outlook* — the proposition of using attacker-centric approaches to support a macro-level strategic view of practitioners is certainly worth considering. It is in contrast to the principle of using attacker information for threat modelling at a granular level — an approach which has been criticised over recent years as ineffective in comparison to system- or security-focussed efforts. Assigning a specific purpose to attacker-centric approaches could also help to solve the first two issues mentioned here, potentially supporting consolidation and further concentration of existing methods. Beyond this research, there are certainly signs that this could be the future direction for attacker-centric approaches. Krebs [22] for example sees actor attribution as a key intelligence aspect as malware evolves.

(4) *Cautious, but positive outlook on attacker personas in theory and practice* — while previous work has highlighted the ability of attacker personas to 'bring attackers to life' and make them more accessible, tangible and realistic to a wide range of security stakeholders, they may also be used as a support tool for communication and collaboration [42] or to help mitigate potential bias in organisations [1]. While practitioners in this work show interest in using attacker personas, experiences of working with them seem limited — here, aligning them to representations already used teams across the agile organisation like digital journey maps may provide an entry point for future research.

(5) *Integrating security into digital experience management* — practitioners placed high importance on business requirements, but also user needs, related to the digital journey and experience of (potential) customers to the bank. In this context, visualisation and mapping techniques such as customer journey maps, attack path maps and attacker personas are mentioned to support the alignment of business, user and security needs, also fitting into research areas of usable security or human-computer interaction for security. Additionally, such approaches may be of use for security disciplines such as threat modelling.

6 CONCLUSION

In summary of this paper, thinking about attackers plays some role in the daily work routines for financial services practitioners. It may however take a number of forms, e.g. through threat intelligence reports distributed across the organisation, usage of threat scenarios or examples of attacker groups, also depending on the individual job description. It is important to understand that this role is limited — reasons mentioned are e.g. time constraints and different focus in the practitioner's overall job role, but also a lack of perceived practical value or related tools available to them. Further academic enquiries into the potential of attacker-centric approaches in practical settings may hence be of value — future research directions may include e.g. work on visualisations ot tools such as attacker personas or integration into the practical discipline of digital customer experience management, in the area of banking and beyond. For this particular research, a future extension with additional case companies should be considered.

REFERENCES

[1] Andrea Atzeni, Cesare Cameroni, Shamal Faily, John Lyle, and Ivan Fléchais. 2011. Here's Johnny: A methodology for developing attacker personas. In *Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security (ARES'11), Vienna, Austria, 22–26nd of August, 2011*. IEEE, 722–727.

[2] Linda Birt, Suzanne Scott, Debbie Cavers, Christine Campbell, and Fiona Walter. 2016. Member Checking: A Tool to Enhance Trustworthiness or Merely a Nod to Validation? *Qualitative Health Research* 26, 13 (2016), 1802–1811. DOI: https://doi.org/10.1177/1049732316654870 arXiv:https://doi.org/10.1177/1049732316654870

[3] Ann Blandford, Dominic Furniss, and Stephann Makri. 2016. *Qualitative HCI Research: Going Behind the Scenes*. Morgan & Claypool Publishers.

[4] Anders Bruun, Marta Larusdottir, Lene Nielsen, Peter Axel Nielsen, and John Stouby Persson. 2018. The Role of UX Professionals in Agile Development: A Case Study From Industry, In Proceedings of the 10th Nordic conference on Computer-Human Interaction (NordiCHI '18). *Proceedings of the 10th Nordic conference on Computer-Human Interaction (NordiCHI '18)* (2018), 352–363". DOI: https://doi.org/10.1145/3240167.3240213

[5] CAPEC. 2020. Common Attack Pattern Enumeration and Classification (CAPEC) — a community resource for identifying and understanding attacks. https://capec.mitre.org. (2020). Last accessed 20th April 2020.

[6] Timothy Casey, Patrick Koeberl, and Claire Vishik. 2010. Threat Agents: A Necessary Component of Threat Analysis. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '10)*. ACM, New York, NY, USA, Article 56, 4 pages. DOI: https://doi.org/10.1145/1852666.1852728

[7] Kathy Charmaz. 2014. *Constructing Grounded Theory* (2nd ed.). SAGE.

[8] Virginia Braun & Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. DOI: https://doi.org/10.1191/1478088706qp063oa

[9] N. Davoust. 2018. Agile and Continuous Threat Models. https://published-prd.lanyonevents.com/published/rsaus18/sessionsFiles/8172/DEV-R04-Agile-and-Continuous-Threat-Models.pdf. (April 2018). AT RSA Conference 2018. Last accessed 20th April 2020.

[10] S. Faily and I. Fléchais. 2010. Barry is not the weakest link: Eliciting Secure System Requirements with Personas. *24th BCS Interaction Specialist Group Conference* (2010).

[11] D. Fraunholz, S. Duque Anton, and H. D. Schotten. 2017. Introducing GAMfIS: A generic attacker model for information security. *25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)* (2017).

[12] Ian Green. 2013. Extreme cyber scenario planning and fault tree analysis. https://www.nist.gov/document/040813cbapart2pdf. (2013). At RSA Conference 2013. Last accessed 20th April 2020.

[13] Craig Harber. 2019. How to Think Like an Attacker. https://www.bankinfosecurity.com/interviews/how-to-think-like-attacker-i-4492. (Oct. 2019). Last accessed 20th April 2020.

[14] Elisa Heymann, Barton P. Miller, and Loren Kohnfelder. 2019. Introduction to Software Security — University of Wisconsin course materials. https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/. (2019). Last accessed 20th April 2020.

[15] Robert Hurlbut. 2019. User-Story Driven Threat Modeling (presentation recording and notes). https://www.youtube.com/watch?v=oEfOKK895Q8 or https://roberthurlbut.com/r/CM19USTM. (2019). Last accessed 20th April 2020.

[16] Intel Information Technology White Paper. 2007. Threat Agent Library Helps Identify Information Security Risks. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Intel-Threat-Agent-Library-Helps-Identify-Information-Security-Risks.pdf. (2007).

[17] Peter Karpati, Andreas L. Opdahl, and Guttorm Sindre. 2010. HARM: Hacker Attack Representation Method. *5th International Conference on Software and Data Technologies* 170 (2010).

[18] Kaspersky Lab. 2018. Lazarus under the hood. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf. (2018). Last accessed 20th April 2020.

[19] Anne Kayem, Rotondwa Ratshidaho, Molulaqhooa L. Maoyi, and Sanele Macanda. 2014. *Information Security in Diverse Computing Environments*. IGI Global, Chapter Experiences with Threat Modeling on a Prototype Social Network, 19.

[20] Julian Kirchherr and Katrina Charles. 2018. Enhancing the sample diversity of snowball samples: Recommendations from a research project on anti-dam movements in Southeast Asia. *PLoS One* 13, 8 (Aug. 2018). DOI: https://doi.org/10.1371/journal.pone.0201710

[21] Barbara Kitchenham, O. Pearl Brereton, David Budgen, Mark Turner, John Bailey, and Stephen Linkman. 2008. Systematic literature reviews in software engineering — A systematic literature review. *Information and Software Technology* 51 (2008), 7–15.

[22] Brian Krebs. 2015. Malware Evolution Calls for Actor Attribution? https://krebsonsecurity.com/2015/05/malware-evolution-calls-for-actor-attribution/. (May 2015). Last accessed 27th August 2018.

[23] Dorte Lønsmann. 2016. *Negotiating Positionality in Ethnographic Investigations of Workplace Settings: Student, Consultant or Confidante?* Palgrave Macmillan UK, London, 13–36. DOI: https://doi.org/10.1057/9781137507686_2

[24] S. Mauw and M. Oostdijk. 2005. Foundations of Attack Trees. *International Conference on Information Security and Cryptology* (2005).

[25] Nancy R. Mead, Forrest Shull, Krishnamurthy Vemuru, and Ole Villadsen. 2018. *A Hybrid Threat Modeling Method*. Technical Report CMU/SEI-2018-TN-002. Carnegie Mellon University Software Engineering Institute, https://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=516617. Last accessed 20th April 2020.

[26] P.H. Meland, I.A. Tøndel, and J. Jensen. 2010. Idea: Reusability of Threat Models — Two Approaches with an Experimental Evaluation. *International Symposium on Engineering Secure Software and Systems* (2010).

[27] Drake Patrick Mirembe and Maybin Muyeba. 2008. Threat Modeling Revisited: Improving Expressiveness of Attack. *2nd UKSIM European Symposium on Computer Modeling and Simulation, 8-10 Sept. 2008, Liverpool, UK, IEEE.* (2008). DOI: https://doi.org/10.1109/EMS.2008.83

[28] MITRE Corporation. 2020. Common Vulnerabilities and Exposures (CVE) List. https://cve.mitre.org/. (2020). Last accessed 20th April 2020.

[29] Caroline Moeckel. 2019. Researching Sensitive HCI Aspects in Information Security: Experiences from Financial Services. https://pure.royalholloway.ac.uk/portal/en/persons/caroline-moeckel(cc765b08-a56e-4a71-8348-c32c1edb580e).html. (May 2019). Sensitive Research, Practice, and Design in HCI Workshop (CHI'19): ACM CHI Conference on Human Factors in Computing Systems - Glasgow, United Kingdom.

[30] Caroline Moeckel. 2020. Public profile/repository at Royal Holloway, University of London. https://pure.royalholloway.ac.uk/portal/en/persons/caroline-moeckel(cc765b08-a56e-4a71-8348-c32c1edb580e).html. (April 2020).

[31] Beverley Mullings. 1999. Insider or outsider, both or neither: some dilemmas of interviewing in a cross-cultural setting. *Geoforum* 30 (1999), 337–350.

[32] National Cyber Security Centre (NCSC). 2017. Cyber crime: understanding the online business model. https://www.ncsc.gov.uk/news/ncsc-publishes-new-report-criminal-online-activity. (2017). Last accessed 20th April 2020.

[33] OWASP. 2011. Agile Software Development: Don't Forget Evil User Stories. https://dzone.com/articles/adding-appsec-agile-security. (Aug. 2011). Not available online - last accessed 27th August 2018. Further information available under e.g. https://dzone.com/articles/adding-appsec-agile-security, last accessed 20th April 2020.

[34] M. Q. Patton. 2002. *Qualitative Research & Evaluation Methods* (3rd ed.). Sage Publications.

[35] X. Peng and H. Zhao. 2010. A Framework of Attacker Centric Cyber Attack Behavior Analysis. *5th International Conference on Software and Data Technologies* (2010).

[36] Recorded Future. 2016. What Is Threat Intelligence? Definition and Examples. https://www.recordedfuture.com/threat-intelligence-definition. (Sept. 2016). Last accessed 20th April 2020.

[37] Johnny Saldaña. 2012. *The Coding Manual for Qualitative Researchers* (2nd edition ed.). Sage.

[38] S.D. Applegate and A. Stavrou. 2013. Towards a Cyber Conflict Taxonomy. *5th International Conference on Cyber Conflict* (2013).

[39] Nataliya Shevchenko. 2018. Threat Modeling: 12 Available Methods. https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html. (Dec. 2018). Last accessed 20th April 2020.

[40] Adam Shostack. 2014. *Threat Modeling: Designing for Security*. John Wiley & Sons, UK.

[41] Adam Steele and Xiaoping Jia. 2008. Adversary Centered Design: Threat Modeling Using Anti-Scenarios, Anti-Use Cases and Anti-Personas. In *Proceedings of the 2008 International Conference on Information and Knowledge Engineering (IKE'08), Las Vegas, NV, US, 14–17th of July*. CSREA Press, 367–370.

[42] M.A. Tariq, J. Brynielsson, and H. Artman. 2012. Framing the Attacker in Organized Cybercrime. In *European Intelligence and Security Informatics Conference (EISIC), Odense, Denmark, 22–24th of August*. 30–37.

[43] R. J. Thomas. 1993. Interviewing important people in big companies. *Journal of Contemporary Ethnography* 22, 80–96 (1993).

[44] I. A. Tøndel, T.D. Oyetoyan, M.G. Jaatun, and D. Cruzes. 2018. Understanding challenges to adoption of the Microsoft Elevation of Privilege game. *5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security* (2018).

[45] K. Tuma, G. Calikli, and R. Scandariato. 2018. Threat analysis of software systems: a systematic literature review. *Journal of Systems and Software* 144 (2018), 275 – 294. DOI: https://doi.org/10.1016/j.jss.2018.06.073

[46] Catherine Welch, Piekkari Rebecca, Heli Penttinen, and Marja Tahvanainen. 2002. Corporate elites as informants in qualitative international business research. *International Business Review* 11 (10 2002), 611–628. DOI: https://doi.org/10.1016/S0969-5931(02)00039-2

[47] X. Yuan, E.B. Nuakoh, I. Williams, and H. Yu. 2015. Developing Abuse Cases Based on Threat Modeling and Attack Patterns. *Journal of Software* 10 (2015).