Anticipation of adverse events in cybersecurity as a social process

Gennadiy Belenkiy | LUND UNIVERSITY

Anticipation of adverse events in cybersecurity as a social process

Gennadiy Belenkiy, MSc

Under the supervision of John Allspaw, MSc

Lund 2025

Anticipation of adverse events in cybersecurity as a social process

Gennadiy Belenkiy

Number of pages: 57
Illustrations: 2

Keywords
Cybersecurity, prospective sensemaking, anticipation, incident, risk.

Abstract
In modern society with its ever-increasing interconnectedness and digitalisation, cybersecurity becomes a prominent issue with tangible ramifications beyond the cyber space. To effectively counter attacks, organisations and their cybersecurity managers must anticipate potential adverse events.
Most public research in cybersecurity is concentrated on technology; however, some literature suggests that the highest potential for progress in the field can be in the social and collaborative factors, including understanding of managerial decision-making. This research is informed by ethnographic studies and adopts a social constructionist point of view. Based on nine qualitative interviews with cybersecurity managers, four themes were produced: construction of foresight, preparing for adverse events, collectivity of anticipation, and assurance-giving. The analysis suggests that anticipatory work is a socio-political process, which challenges the dominant narratives in cybersecurity that focus on technology and adversarial interplay. It uncovers hidden demands of cybersecurity managers' role, requiring competencies in storytelling, political negotiation, and trust-building. The phenomenon of anticipation in cybersecurity is an ongoing collective process of meaning-making, contingent on organisational politics and power relations, performing confidence and control in the face of ambiguity.

Riskhantering och samhällssäkerhet
Lunds tekniska högskola
Lunds universitet
Box 118
221 00 Lund

http://www.risk.lth.se

Telefon: 046 - 222 73 60

Division of Risk Management and Societal Safety
Faculty of Engineering
Lund University
P.O. Box 118
SE-221 00 Lund
Sweden

http://www.risk.lth.se

Telephone: +46 46 222 73 60

Dedication

This work is dedicated to the late Dr Richard Cook, who completely changed my view of how complex systems fail and inspired me to take a plunge into the world of messy details of the "work as done". Thank you for hinting in an email that eventually I would be tempted to join Lund University's Human Factors and Systems Safety program. It was a pleasure meeting you, thank you for your kindness and the inspiration.

Acknowledgements

Firstly, I would like to thank my wonderful wife Sumie for making it possible to join this program and spend hours at night and on weekends doing the assignments and thesis work. It was especially brave of you to let me travel halfway across the world to join a Learning Lab while looking after a newborn. Thank you to my in-laws who flew in and helped to hold the household together once we had an addition to the family, making it possible to study. Thank you to my children Kaito and Yuto, who patiently waited for me while I was wrapping up the next assignment or a chapter of the thesis.

Secondly, I would like to thank my tutors: Noel Hengelbrook, Carsten Busch, and John Allspaw for challenging me and providing new perspectives. Thank you to my peer reviewers and especially to Laura Nolan, I always looked forward to getting feedback from you. I would also like to thank Ruth Parris for providing guidance and encouragement throughout the difficult parts of the thesis work.

Lastly, I would like to say thank you to John Allspaw again for staying all the way with me during my prolonged thesis. I really appreciate your help.

Contents

List of Figures

List of Tables

Glossary

ATM – Automatic Telling Machine

CISO – Chief Information Security Officer

CSM – Cybersecurity Manager

CSO – Chief Security Officer

DDoS – Distributed Denial of Service

MFA – Multi-Factor Authentication

SIEM – Security Information Event Management

STEM – Science, Technology, Engineering, and Mathematics

1. Introduction

With the ever-increasing interconnectedness and digitalisation, in 2025 it is perhaps a truism to say that cybersecurity as a domain is particularly important. The ramifications of cyber incidents are tangible in the real world. Examples include the Colonial Pipeline disruption and panic fuel buying in the US (Australian Broadcast Corporation, 2021), paralysis of Maersk container shipping, disrupting the global supply chain (Greenberg, 2018), and hospital system struggling to treat patients (British Broadcast Corporation, 2017).

To effectively thwart attacks, organisations and their cybersecurity managers are required to foresee the actions of the threat actors and deploy defences against them. This means that cybersecurity managers play a role in the organisation's cybersecurity adaptation.

While the problem of cybersecurity is pervasive in modern society, and it has become everyone's problem in one way or another, this research has a specific focus on cybersecurity professionals in leadership roles (e.g. a CISO, a CSO) to better understand their anticipatory practices. By the nature of their position in the organisational hierarchy, they are responsible for making strategic decisions directing scarce resources and have an extended time horizon (Klein, 1998, p. 156). Borrowing from Cook et al. (1998, p. 13), the research is focused on the managers at the blunt end, rather than on the practitioners at the sharp end.

This thesis is a contribution to broadening the cybersecurity research agenda, advancing the literature on anticipatory practices in the cybersecurity domain. The research is based on lived experience, exposing real-world constraints and enablers that define anticipatory practices of cybersecurity managers in organisations.

1.1 Research Question

The central question of this research project is: How do cybersecurity managers anticipate adverse events? What is an adverse event in this case is defined by cybersecurity managers and depends on the context of their organisations. The goal of the research is to find out how cybersecurity managers anticipate such events, find patterns and generate themes of what makes sense for people to do in such roles, given the pressures from the changing shape of threats, time horizon and the limited resources of their organisations.

1.2 Object of Study

The object of study is anticipation of adverse events in a particular domain of work, cybersecurity. Poli (2019, p. v) defines anticipation as "the process of using the future in the present, which includes a forward-looking stance and the use of that forward-looking stance to effect a change in the present". Since my research question is focused on what people do, it is also appropriate to describe it as anticipatory behaviour (Poli, 2017, p. 1) or anticipatory practice; something people do when they "use" the future to guide their present decision-making.

1.3 Motivation and Purpose

This research is inspired by the thesis of a recent Lund graduate – Colette Alexander (Alexander, 2024), who explored how Quantitative Risk Assessments (QRA) are used in the domain of cybersecurity. This research takes a more foundational perspective, setting out to explore what happens before the QRA appears.

In their paper on anticipation in cybersecurity, Ahrend and Jirotka (2019, p. 1562) lament that academic researchers have difficulty accessing the field, which results in "scarcity of empirical data about cyber-defenders' local practices". This thesis aims to bridge the gap between academic research and cybersecurity practice by examining how cybersecurity managers develop anticipation of adverse events.

Further, Beznosov and Beznosova (2007, p. 421) found that over 94% of public research in cybersecurity is concentrated on technology. Authors suggest that the highest potential for progress in understanding the attacker-defender interplay might be in the broader research that incorporates social and collaborative factors. Ceric and Holland (2019, p. 175) expressed similar concerns more than a decade later, noting the limited understanding of managerial decision-making in relation to cyber defence preparedness. Tapinos and Pyper (2018) identify a gap in the literature on how anticipation and foresight are done by people in practice (researching without formalised techniques, like Delphi) – for example, how signals, weak and strong attract the attention of decision-makers.

A gap in literature has been identified: limited research addresses the non-technical practices of cybersecurity managers, particularly social and collaborative practices, decision-making, and creation of foresight. This research seeks to address this gap by looking at lived experience of cybersecurity practitioners and answering the research question.

2. Literature Review

The literature review looks at anticipation as a concept and then elaborates on it across several interrelated domains of study relevant to this research: cybersecurity and risk management, complex systems, cognitive science, safety science, and sociology.

2.1 Anticipation as a Concept

Poli (2017, p. 3) notes that anticipation as an object of study or a concept appears within several different fields, including biology, and the cognitive and social sciences – and, under different guises, in the domains like anthropology, futures studies, management, political science, engineering, cultural studies, and philosophy. In simple terms, anticipation is related to looking into the future and informing and shaping the present. Roberto Poli, referring to the work of Robert Rosen (Poli, 2017, p. 20) claims that the anticipation is pervasive and immanent to most, is not all systems, it is a "general feature characterizing many different families of systems".

The term "anticipation" can also be used as a qualifier in the expression "anticipatory system" Poli (2017, p. 1). Poli notes, referring to Rosen (Rosen, 2012, pp. 8, 313, as cited in Poli, 2017, p. 2) that "an anticipatory system is a system containing a predictive model of itself and/or its environment which allows the system to change state at one instant in accord with the model's predictions pertaining to a later instant." Poli (2017, p. 2) notes that such a system depends on models, internal and external, adding that internal models are especially important to understand the behaviour or organisations, people, groups, and institutions (Poli, 2017, p. 2). Difficulty in updating mental models is one of the reasons for surprising incidents in IT (Woods, 2017). In cybersecurity, models are also used in anticipatory or predictive contexts – for example, as threat models (Shostack, 2014) that help identify risks, or models of adversaries and their capabilities.

Anticipation needs to be distinguished from forecasting, as forecasting by itself does not constitute or directly lead to decision-making. Poli (2017, p. 1) illustrates: "A weather forecast in itself is not anticipatory in the sense used by this book. Watching a weather forecast and as a consequence taking an umbrella before going to work is instead an anticipatory behavior."

Johansen et al. (2015, p. 334) write about anticipatory work – something people and organisations do, identifying two distinct stages: short term and long term. Arguing for a socio-technical epistemology, Johansen et al. (2015, p. 334) propose a broader perspective of anticipatory work: it is not just cognitive or social but also involves external artefacts and tools. Borrowing from Hutchins (1995), it is socio-technically distributed.

2.2 Anticipation in Cybersecurity

Branlat (2011, p. 120) in his analysis of an adversarial cyber exercise at the Idaho National Labs, argues that anticipation, as a cognitive function, is a characteristic of expert behaviour, a critical component for adaptation in the cybersecurity domain:

> As a form of feed-forward control, anticipation is especially critical to keep with the pace of events, by avoiding failures to adapt in time, before perturbations cascade. In the adversarial context of cyber security, anticipation means understanding and making projections regarding what the other side is targeting. (Branlat, 2011, p. 120).

Ahrend and Jirotka (2019, p. 1562) argue that cybersecurity literature consistently describes anticipation and anticipatory practices as "ideas of a future to act in the present, with a broad focus on technology to support, or automate this decision-making." Anticipation might be studied through a range of practices in cybersecurity – threat modelling, risk assessment, and threat intelligence. Threat intelligence can take different forms – from an ongoing supply of IP addresses and domain names suspected to be involved in malicious activities, to a targeted analysis of communications in the dark web that attempt to map out potential moves of the threat actors (Ahrend and Jirotka, 2019, p. 1575). Defenders, envisaging possible attack vectors, not only build their defences and deepen the understanding of their own infrastructure, but also remain attentive to broader attack observations. Doing so is challenging due to uncertainties and ambiguities of the cybersecurity domain, however improving the anticipatory capability may improve overall decision-making (Ahrend and Jirotka, 2019, p. 1560). Practices that encourage defenders to "think like an attacker", penetration testing, and similar approaches, are already part of the cybersecurity defender repertoire, and artificial intelligence and machine learning can provide additional support to defenders (Ahrend and Jirotka, 2019, p. 1580).

2.3 Anticipation and Complex Systems

Even a start-up company may operate an internet-connected infrastructure comprising hundreds of servers running millions of lines of code. Within such systems, components can be tightly coupled, tangled in an internal network of interconnectivity. This infrastructure – an "opaque sea of automation" (Allspaw, 2016), is connected to the ocean of the internet, processing billions of connections a day. Amid these billions of connections and interactions some are initiated by cyber adversaries. In addition, the change is ongoing, people continually reshape the infrastructure. Furthermore, new knowledge about unanticipated software behaviour and vulnerabilities emerge. Consequently, uncertainty can take several forms and is endemic (Woods, 2017). Branlat reflects on this in his study of a staged adversarial cyber interplay:

> These various forms of uncertainty make it challenging to make sense of actions observed and anticipate future actions. The capacity to understand the situations experienced is nonetheless essential both for the management of adversarial interplay and for cooperative activity.

> Furthermore, the potential impact of actions on a large and complex network is difficult to evaluate or anticipate. (Branlat, 2011, p. 117)

Within such an environment, conceptualised as a complex adaptive system, Branlat (2011, p. 117), referring to Hollnagel and Woods' (2005, Woods & Branlat, 2010) idea of being in control of a complex adaptive system, defines anticipation as one of the core activities: "being in control means: – anticipating how adverse events may evolve in order to take advantage of the window of opportunity on the defensive side" (Branlat, 2011, p. 117). Similarly, Woods (2018, p. 447) links high graceful extensibility with the ability to anticipate emerging challenges and a changing shape of threats to prepare to respond and adjust the readiness to respond to future challenges, thereby strongly connecting anticipation with adaptation.

2.4 Anticipation as Cognitive Work

Anticipation can be viewed as a type of cognitive work, Klein et al. (2011, p. 235) define anticipatory thinking as: "the process of imagining how unexpected events may affect plans and practices. ... Anticipatory thinking lets us guard against or forestall potential threats." Anticipatory thinking is not just about predicting future events but involves an active act of preparation and positioning for possible future states" (Klein et al., 2011, p. 236), which echoes the definition of anticipation proposed by Poli (2017, p. 1). Klein et al. (2011, pp. 237-239) have identified three non-exhaustive patterns of anticipatory thinking:

- Pattern matching
- Trajectory tracking, and
- Convergence

Klein et al. (2011, p. 235) propose that anticipatory thinking can be seen as a macrocognitive ability, a future-oriented form of sensemaking, which they link to the work of Weick (1995, pp.24-30) on sensemaking. Anticipatory thinking relates to decision-making, expectancy generation, and mental simulation, and it is also a form of problem detection (Klein et al., 2011, p. 239).

2.5 Anticipation and Prospective Sensemaking

Klein et al. (2011, p. 235), as discussed above, suggest that anticipation is a form of sensemaking. MacKay (2009, p. 97) further notes a crucial nature of sensemaking for cybersecurity managers in senior positions, such as CISO and CSO: "sensemaking processes are particularly important for senior executives".

Traditionally, sensemaking is about retrospective construction, that is, about assigning meaning to past events. However, Tapinos and Pyper (2018), Rosness et al. (2016), Wright (2005), in their works, extend this to include a future-looking version – "prospective sensemaking". Rosness et al. (2016, p. 55) define prospective sensemaking as "sensemaking processes where the attention and concern of people is primarily directed at events that may occur in the future". Tapinos and Pyper (2018, p. 292) referring to the work of Weick (1995, pp. 24-30) on sensemaking, elaborate further by defining two modalities of

prospective sensemaking: Weickian or "future-perfect" and post-Weickian or "future-oriented". The future-perfect modality suggests that prospective sensemaking occurs by constructing an image of the future and then working backwards to interpret it, examining how it can emerge (Tapinos & Pyper, 2018, pp. 293, 295), it operates as if the future has already arrived. Tapinos and Pyper labelled this process "predictive hindsight" (2018, p. 295). Pitsis et al. (2003, p. 574, citing Weick, 1979, p. 179) defined the future-perfect sensemaking as follows: "the forward-looking projection of ends is combined with a visualization of the means by which that projected future may be accomplished."

The future-oriented form of prospective sensemaking is characterised by a forward progression, moving step by step while justifying the analysis, and by developing a mental "system of relationships" (Tapinos & Pyper, 2018, pp. 296, 299).

MacKay (2009, p. 91) notes the pre-determinism of the future-perfect modality: "In future perfect processes, agents will project their actions into the future as if they have already happened. The future is treated as predetermined. This enables them to make retrospective sense out of anticipated future events." Tapinos and Pyper (2018, p. 295) further elaborate this critique: the future-perfect modality is better suited to stable environments.

Rosness et al. (2016, p. 54), studying surgical operations, acknowledge that prospective sensemaking is not just a social process; technological artefacts are also players on the surgical team, thereby explicitly framing prospective sensemaking in that context as a socio-technical process, consistent with Johansen et al. (2015, p. 334). In their study, Rosness et al. (2016, p. 67) specifically focused on unremarkably successful operations, noting the role of anticipatory work in achieving such success. Prospective sensemaking was viewed as a critical part of anticipatory practices that helps achieve success – the "dynamic non-event" (Weick, 2011) in healthcare (Rosness et al., 2016).

Wright (2005, p. 91) proposes that prospective sensemaking is an ongoing process "involving both an attitudinal and task response that involves acts of exploration and interpretation in an imagined future", thereby equating it with anticipation as defined by Poli (2019, p v). Importantly, Wright (2005, p. 90) notes that, while sensemaking is a social process, meaning is produced individually.

3. Research Design

3.1 Methodology

This research seeks to discover how people in charge of an organisation's cybersecurity anticipate adverse events. It will focus on how cybersecurity managers engage in meaningful activities, preparing for opportunities and problems that may arise in the future, and construct a meaningful reality based on their interpretations and the social context of their work. Social constructionism is adopted as the epistemology for this research, as Crotty (1998, p. 43) notes, "constructionism claims is that meanings are constructed by human beings as they engage with the world they are interpreting. Before there were consciousnesses on earth capable of interpreting the world, the world held no meaning at all."

For this research, interpretivism is adopted as a theoretical perspective. The research methodology is aligned with ethnography; however, the direct observation aspect of ethnography is not suitable for studying the cyber security domain, where practitioners often work remotely and are distributed around the world. Obtaining corporate cybersecurity documentation related to an organisation's risk management – its predictions and preparations – is nearly impossible; therefore, interviews with practitioners were employed as the main data source for the project.

The research is aimed to be naturalistic, providing a specific context, settings, and participants, and aimed at resonating with the experiences of the reader, highlighting similarities between the analysis and other research (Braun & Clarke, 2022, p. 144).

3.2 Method and Data Collection

Qualitative studies are well-positioned to examine how meaning is constructed, a qualitative data analysis method aligned with reflexive thematic analysis (Braun & Clarke, 2006, Braun & Clarke, 2022) will be used to analyse the data for patterns of shared meaning.

Several ways of collecting data have been considered. Organisational documents that often reflect human anticipatory practices in cybersecurity are difficult to obtain. Even if obtained, such documents would likely be sanitised, making them of limited utility for the research. Direct ethnographic observation of anticipatory practices are also problematic, as a significant proportion of practitioners work remotely. Therefore, semi-structured video interviews with cybersecurity managers were chosen as the primary means of engagement with practitioners in the field of study.

Nine semi-structured interviews were conducted with participants who agreed to take part in the research. Interviews ranged from forty-five minutes to more than two hours, depending on interviewees' availability.

Participants were recruited through LinkedIn and other professional connections. Practitioners who agreed to be interviewed were former colleagues of the author. All interviewees were men. Attempts were made to recruit three female CISOs; however, none responded. Interviewees are based in Australia, the EU, Singapore, the UK, and the US. Participants have held the following roles: CSO, CISOs, country cybersecurity manager within a multinational corporation, and senior managers in information security departments.

Table 1 Participants roles and their industries.

Interviewee	Role	Industries
CSM1	CSO	Software and digital services
CSM2	CISO	Software and digital services
CSM3	Country cybersecurity manager	Insurance, Consulting
CSM4	Senior cybersecurity manager	Digital services, banking
CSM5	CISO	Software and digital services
CSM6	CISO, Senior cybersecurity manager	Banking, utilities
CSM7	Senior cybersecurity manager	Software and digital services
CSM8	CISO	Banking, Consulting
CSM9		Had withdrawn
CSM10	Senior cybersecurity manager	Banking, software, and digital services

All interviews were conducted in English, which is not the first language for some practitioners, careful manual verification of the transcripts was performed. The dataset offers a variety of perspectives, as the informants are located in various parts of the world, embedded in diverse cultures, and operate across different industries. Industries range from lightly regulated to heavily regulated – finance being one example – thereby the dataset has the potential to provide a broader perspective. It was anticipated that industry context would influence participants' views; this forms part of the analytic interest.

All interviews were conducted via Zoom and then transcribed using Microsoft Word 365 transcription feature. Interviews were directed by open-ended questions around anticipation, sensemaking, and practical ramifications. Obtaining data on practitioners' lived experiences was a key focus of the interviews. The following prompts were used:

- What is your time horizon for foresight and preparations?
- What or who helps you look ahead? Who or what is helpful and what is not?
- What makes it easy and what makes it hard?
- How do you know you "see" the big picture?
    - What do you do in that case?
- What scares you in the development of threats?
- Who or what helps you think about the future and prepare for it today?

- What percentage of your work is forward-looking as opposed to managing daily activities?
- What do you pay attention to, so that you learn something about the future?
- What narratives about the future make sense to you?
- What role do emotions play in your understanding of the future?

3.3 Researcher Reflexivity

As a researcher-practitioner, I engaged throughout the research in ongoing critical self-evaluation, aimed at separating my practitioner view from the researcher's view. I have worked in various roles in information security since 2007; this experience proved valuable for the research; and I drew on it during certain parts of the research while attempting to suspend it in others.

My professional experience and knowledge of recent incidents proved valuable for the interviews, I was able to "speak the same language" as the interviewees and to probe for deeper issues in matters discussed. My knowledge of the domain, and the fact that the interviewees were all connected to my previous work experience in one way or another, helped to establish good rapport during the interviews. At times I was surprised by the information provided by the participants, and I actively suppressed expressing my own views during the interviews.

As a practitioner-researcher, I sometimes noticed a tendency to pull myself back when I found myself "arguing with the data". As data gathering and analysis progressed, I, however, became more comfortable accepting the data as it was. I used my domain experience in the coding and the theme development phases. In line with Braun and Clarke's reflexive thematic analysis (2022, p.13), researcher subjectivity is treated as a resource.

This research project brought in two surprises. First, despite cybersecurity being a rather secretive affair, I was repeatedly struck during the interviews by the transparency and openness of the interviewees, who were willing to share their lived experiences. One factor contributing to that may have been the fact that I had worked with all participants at one point in time; I was not an unfamiliar researcher with no prior relationship to them. Second, my initial expectations and the focus were on the adversarial interplay and how practitioners might imagine future attacks and prepare for them. To my surprise, however, they focused at least as much, if not more, on their own organisations – their history, context, relations with stakeholders, business direction and technology.

3.4 Data Analysis

Qualitative thematic analysis, aligned with the six steps of reflexive thematic analysis (Braun & Clarke 2006, p. 87) was used to identify patterns and themes. An inductive, data-driven approach was chosen for the data analysis rather than a theory-driven framework, in part due to the scarcity of prior research in this area.

Interview transcripts were uploaded into NVivo 14, and all subsequent transcript verification, correction and data analysis were performed using this software. Table 2 below provides further information on the data analysis steps, including how the software was used in the analysis.

Table 2 Six steps of qualitative data analysis.

Step	Description of activities
1. Familiarisation with the data	All transcripts were read once; researcher notes were made in NVivo and in a separate document noting relevance of existing literature and prior research. These notes highlighted initial impressions, thoughts, and researcher reflexivity.
2. Generation of initial codes	Transcripts were coded inductively in NVivo; overall, close to five hundred (500) codes were generated. Line-by-line coding was not used; codes were assigned to varying sizes of data.
3. Searching for themes	Code grouping was performed at this stage, looking for potential affinities. Code groups were further clustered into initial themes. All steps were performed in NVivo.
4. Reviewing themes	Initial themes were checked against data extracts and initial impressions. Four themes answering the research question were identified through an iterative process of going back and forth to data and codes to see how the themes fit the research question; thematic map was generated (Figure 1). NVivo was used to trace the codes back to the interview transcript excerpts. The thematic map was hand drawn.
5. Defining and naming themes	Several names were identified as candidates. Names were checked against the idea of identifying the essence of the theme (Braun and Clarke, 2006, p. 22), telling what the theme is about. Data from previous phases was reviewed to identify which name would work best.
6. Producing the report	Report on themes was produced, aiming to "tell the complicated story of your data in a way which convinces the reader of the merit and validity of your analysis" Braun & Clarke, 2006, p. 23)

Final thematic map is shown below:

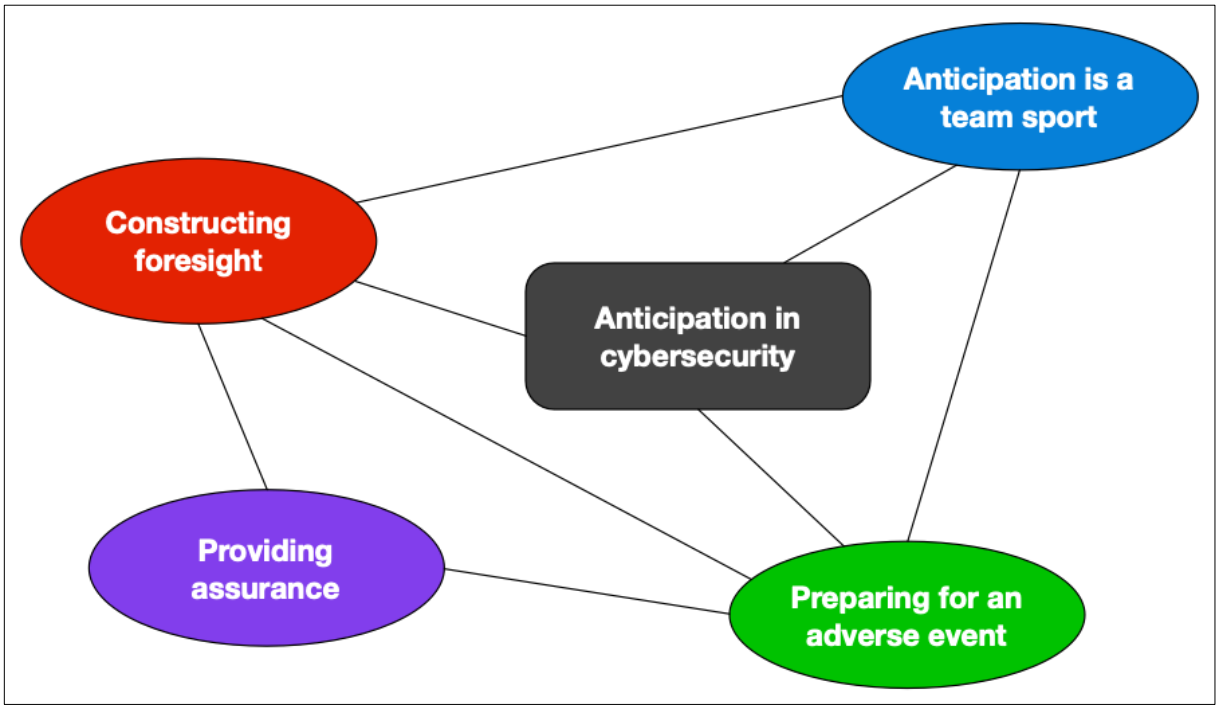

Figure 1 *Final thematic map.*

4. Results and Analysis

Four themes related to the development of anticipation in cybersecurity have been constructed: "Constructing foresight", "Preparing for adverse events", "Anticipation is a "team sport", and "Rituals of assurance: "We're OK here."

In keeping with Braun and Clarke (2022, p. 132), this section provides an interpretive account of the themes. Further interpretation, implications and the location of the analysis in a broader theoretical context are provided in the Discussion section.

Interview extracts were lightly edited, mostly by removing repeated words and by omitting parts unrelated to the point illustrated.

4.1 Theme 1. Constructing Foresight

It is unsurprising that the interviewees provided a substantial amount of data on how they try to "see" the future and make sense of it. A rich and diverse set of codes was created around foresight development. The definition of an adverse event was left to practitioners, as part of their practices of foresight construction.

Adverse events in cybersecurity are typically understood as disruptions of cybersecurity goals: confidentiality, integrity, and availability of information (Ham, 2021, p.18). In practice, interviewees defined adverse events based on their perception and framing of risk, their own definition of goals, professional identity and negotiated areas of responsibility. Furthermore, what counted as an adverse event was also shaped by the organisational dynamic, power relations and risk appetite, making it socially defined. One of the CSM shared an example of how during the COVID19 pandemic lockdown printing of loan documents was done on home printers, it was prohibited after an audit but later revised:

> ... some auditor went through was like hey, people are printing to their personal printers. We got to stop this. They could print out sensitive information and we would never know. And so, they locked all that down. ... And so, because this was an audit finding and because people were worried and they shut all this down, ended up shutting down our auto loan business for like a week and a half.
>
> Because nobody could process the paperwork and submit it to other banks and other loan institutions because they all wanted physical hard copies. Right, and it took a while before we're like, no guys this is not an insider threat issue. I mean it is an insider threat issue but like where do you want to draw that line? Right. Like these people need this to do their job. (CSM10).

This extract shows that interpreting something as an adverse event is both negotiated and socially defined: possible exposure of sensitive information through home printing resulted in a decision to get it blocked, thus pursuing the goal of preserving confidentiality. However, that also had negative economic

consequences for the bank and had to be revised. While some audits possess the authority to declare something as an adverse event or as a risky activity, once the evidence of economic harm accumulated, stakeholders redefined home printing of loan documents as a normal work practice under the circumstances (Muller, 2024, p. 3).

What is an adverse event for CSMs is also defined by the goal statement and the division of labour in the organisation: "I care much less about if a server goes down, we have a backup team. I am primarily focused on ... what can a human adversary do to mess with our data." (CSM10). The goal statement reveals one of the key factors that shape the construction of foresight (Fuller & Loogma, 2009, p. 73) – perceived malicious intent. CSM5 reflecting on the CrowdStrike incident (CrowdStrike, 2024) portrayed it as not an adverse cybersecurity event, even though information availability was affected:

> If you look at the canon of security, the security practice, we can look at it and see it as an as an availability as a security problem because it touches on availability. Now that does not mean that in 99% of organisations out there that it should be treated as a security incident. I don't think it should, even though it affects the CIA triad. ... Security folks are not good at availability. (CSM5)

The same CSM in the interview discussed events like a distributed attack (DDoS) on a web application making it unavailable, or a ransomware attack as an adverse cyber event. Even though the effects of the CrowdStrike incident (CrowdStrike, 2024) closely resembled those of a ransomware attack – for example, computing resources became unavailable, data on disks was encrypted, and the adverse effects were caused by security controls such as anti-malware software and disk encryption – the incident was not considered as a cybersecurity event because it was perceived that no adversary was involved. The malicious intent of an actor, as perceived by the CSM to be responsible for an adverse event, emerges as one of the strongest defining factors shaping the scope of anticipatory practices. If no malicious intent is perceived or attributed as a cause, an event may not be considered as a cyber incident.

To "see" how the future may play out, participants engage in building a story that makes sense or mental simulation. During the coding phase, codes like "story building" or "mental simulation" were used to mark those utterances. For example, practitioners imagine how a particular known attack might or might not be stopped by existing defences in the future: "if the threat actor will execute the same kill chain, will they be successful in my situation?" (CSM4). CSMs interpret signals and cues into a meaningful narrative (Wright, 2005, p. 86), try to make sense of the future (Tapinos & Pyper, 2018, p. 295, Klein et al., 2011, p. 237) by assembling stories or narratives of what might happen:

> So, you list these factors which may be the subjective which may be objective, but overall, also you're going through the story that this is what's going on in the world. This is what's going on in in these sectors. This is the factors which are internal to our company which we believe which are relevant. This is the statistics, if we have it right. And then we're saying, OK, what will happen? (CSM4)

This process of building a forward-looking narrative (Tapinos & Pyper 2018, p. 293, Klein et al., 2011, p. 235) can be framed as a process of prospective sensemaking (Tapinos & Pyper, 2018, Wright, 2005, Rosness et al., 2016). Wright (2005, p. 91) notes that while sense is made individually, sensemaking is inherently a social process. Sense is never fixed, it is continuously constructed, deconstructed, and reconstructed (Wright, 2005, p. 86). This ongoing nature of the process is evident in how CSMs characterise the breakdown of old meanings and the creation of new ones:

> We got popped because somebody we didn't have multi factor auth on a cloud service. We have shifted gears dramatically and now we have multi factor authentication on almost all of those services. So suddenly my threat landscape, my worries about OK what are we doing with stolen credentials on the cloud, has now changed dramatically and has changed dramatically since June, right within two months. (CMS10)

The threat landscape here is a mental creation that is constructed, deconstructed, and reconstructed by this individual CSM. One cannot take a photograph of this landscape; it is a metaphor for the meaning and perception about one's system vulnerabilities and the possible and plausible actions of attackers. The threat landscape as a created meaning shapes what is anticipated in this environment, guiding the practitioner's sense of what they should worry about. The quote above also highlights that the way the interviewee defines the threat landscape is actively shaped by organisational choices as well as adversarial capabilities.

Discussing past incidents and lessons learned is one of the main ways CSMs construct possible futures:

> So basically, we had an incident, we closed it. And then as a part of the root cause discussion and report, since then discussion, we decided those are those are the things that we need to implement to be able to respond to that ... kind of incident next time better. (CSM2)

Anticipation here is based on and triggered by reactions to an adverse event that has occurred. The future here is seen as a repetition of the past, which implies a reactive approach. Furthermore, CSMs reported that their cybersecurity program is reactive in nature: "the whole cyber security programme as a reaction to external events overall" (CSM2). This "reaction" means that CSMs must monitor the external events, decide which ones are applicable to their organisation, assess how likely they are to occur, and then decide how to prepare. Tapinos and Pyper (2018, p. 295) referred to this process as "predictive hindsight".

While, as expected, much of foresight focus was on the "other side" – the adversaries – the CSMs also reported explicitly engaging in understanding their own organisations and their histories, which provided a crucial source for their anticipatory practices:

> It tells a lot about the type of activities that business is involved in and the types of events that have impacted it, guide you on where your vulnerabilities and weaknesses may be that are relevant to how you operate as a business. ... it gives you a gut feel, some instinct, some insights into what can go wrong in this organisation. What does tend to go wrong. (CSM6)

The history of the organisation is not just found "out there"; it is actively constructed, remembered, and interpreted. In this excerpt, the CSM constructs meaning about a possible future based on his "reading" of the organisation's history. Rather than appealing to data as a source of supposedly objective truth – an approach that is only too common in cybersecurity – the CSM implicitly acknowledges that data by itself neither creates meaning nor tells a story. Furthermore, the CSM highlights the role of intuition as a source of insight about the future.

In another example, a focus on the organisation enables the CSMs to develop foresight regarding how it will respond under pressure to quickly remediate vulnerabilities in its software:

> So, what is helpful is to understand what people and organisation's pain points are. And what they're willing to tolerate. ... when I realise that ... every year there is a critical vulnerability in a library you depend on OpenSSL Lib, PNG Lib, XML or any of the 10 critical libraries that accept user input. So, I know that once a year I'm going to destroy one of your four [software] releases because ... I'm going to say ... you need to fix OpenSSL right now. ... if you only get four a year and I take one of them, I have just eliminated 25% of your ability to release new products. If I understand that pain point, that lets me to predict things. (CSM1)

Here, the CSM predicts that production pressures to release software features might hinder the ability to remediate a dangerous vulnerability drawing on his prior experience. This extract also shows that the CSM grounds his view of the future in his experience. On this basis, he makes a prediction of how frequently the organisation will encounter a vulnerability in its core software system. The CSM envisages an adverse future event and then backtracks to today, which can be characterised as the future-perfect prospective sensemaking (Tapinos & Pyper, 2018, p. 299).

CSMs actively probe the system – for example, through red team exercises – to find system weaknesses and vulnerabilities and to model how a potential adverse event might unfold in the future:

> We ordered a red team exercise against the organisations ... we said that we don't have a particular target ... we asked them to get the domain domination. The idea is that on average a threat actor would prefer to get the domain domination and then to act upon their objectives. The result that we got back ... set our backlog for the next 18 months. (CSM2)

Knowledge of prior incidents and how they transpired shaped the red team's task. In this case, it was an assumption that an adversary might gain control of the organisation's Active Directory server. The red team therefore investigated how susceptible the organisation was to this kind of attack.

While in most cases the CSMs described constructing the future on the basis of organisational history, experience, and interpretation of past incidents, there was also evidence that they attempted to synthesise the future from observed trends:

> Let's say legal companies because companies are juicy targets right now for the data exfiltration and then ransomware. Hackers love lawyers because they have a lot of sensitive information of

> their customers. And they don't have good defences most of the time, or at least for now. Probably this is going to evolve quickly, but for now this is like this. So, the hackers are specifically trying to target legal. (CSM4)

CSM4 went on to say that this hypothesis was not derived from his knowledge of prior incidents. Instead, constructing the future in this manner can be seen as the convergence of different streams of observation (Klein et al., 2011, p. 237). This activity required "adversarial thinking", that is, imagining the actions that an attacker might plausibly take to achieve their goals:

> The piece of adversarial thinking, right? What are the bad guys thinking about? And ... trying to put yourself in their place and say, what could I do or what might I do tomorrow in order to meet my own goals? And you know, we say their goals are more money. ... But we also have to be careful because it's very easy to fall into your own biases. (CSM10)

This construction of the foresight can be seen as an extension of macro trends over longer-term time horizons. Macro trends such as artificial intelligence (AI) or quantum computing, while salient and potentially harmful for organisations, are associated with a high degree of uncertainty. Possible contours of the future, and adversarial use of AI are considered by the CSMs; however, such possibilities might not readily compel practitioners to take concrete actions. Instead, their focus is directed towards more known and salient issues. Moreover, given the constrained resources, CSMs must balance their attention between the long-term and short-term time horizons:

> So, I would try to pick out well what is the macro theme here, who's going to benefit from AI that will seek to attack us, and cyber criminals are using AI. They'll be using AI to pick more social engineering weaknesses to mine data and to come up with different ways of doing things and to evaluate. ... Those macro level views of how it is going to be misused against an industry against the world against you as an organisation. I think that's about as far as I go with those long horizon views. Because there is just so much to deal with on a daily basis, the things that we know can go wrong today, they're far from fixed. (CSM6)

The extract gives the impression that CSMs tend to focus on known, concrete "things". While CSMs try to construct foresight on how their organisation might be attacked in the future using cutting-edge technology; this, however, remains largely a theoretical exercise. In practice, CSMs appear to be overwhelmed by unresolved known issues. Their anticipatory practice is predominantly about determining the likelihood that a known issue is applicable to the organisation and, if so, how urgently it must be addressed – that is, how quickly the window of opportunity for attackers should be closed (Branlat, 2011, p. 106). CSMs imagine that a known issue might cause an adverse event in the future and then work backwards estimating how such an event could unfold and what must be done to prevent it – a process described as "predictive hindsight" (Tapinos & Pyper, 2018, p. 295)

4.2 Theme 2. Preparing for Adverse Events

Practitioners spoke frequently in the interviews about what they do to prevent incidents. In the analysis a well-defined cluster of codes was formed, which is unsurprising for a study focused on anticipatory practices, and the cluster provided the foundation for a theme on preparation for an adverse event.

The "roadmap" (or backlog, as one CSM referred to it) was one of the most used organisational vehicles for implementing preparations mitigating an adverse event. A roadmap refers to a way of planning and implementing preparations to either prevent an adverse event or better manage it if it still occurs. When asked about anticipatory time horizon, CSMs typically responded in terms of their roadmap planning, some plan for 1 year, some for 3 years, while one reported a 5-year long roadmap within their organisation: "I usually look between one and three years ahead in terms of what I'm looking in terms of strategy structure in terms of capabilities" (CSM5).

When asked about the time horizon of their anticipation CSMs typically referred to the planning horizon of their organisation's roadmap. This highlights how the term "anticipation" is understood by the CSMs: it is seen as a reaction to what might happen to the organisation and preparations made to address them: "I usually look between one and three years ahead in terms of what I'm looking in terms of strategy structure in terms of capabilities" (CSM5). The roadmap is typically comprised of specific, actionable projects, including the implementation of a particular security control or remediation if an identified weakness or issue:

> You use a cyber simulation, you use certain you know pen tests, you use certain internal audit findings, red teams, all of these things going back to our three-year vision and that 6 to 12 month review of what we need to be focusing on. (CSM8)

In this example, penetration testing might uncover a security issue or a vulnerability that can be exploited by a malicious attacker. That possible issue is assessed for likelihood and severity and a project aimed at preventing an incident is then scheduled on the roadmap, including sub-projects, milestones and budgets required to achieve the desired end-state.

The roadmap is used to plan and deliver projects that advance an organisation toward a particular level of security maturity – for example, in accordance with the NIST Cyber Security Framework (National Institute of Standards and Technology, 2024). A level of maturity here represents a desired target state (Alexander, 2024, p. 30), and the roadmap is the path that leads to it: "We're at NIST 3.88 at the moment. ... I'm really gonna have to lift my game over the next 6 to 12 months. Putting in tooling that can give me an advance notice of events." (CSM2). The chosen framework not only guides what is included on the roadmap, but also serves as a legitimising factor for the preparations to be implemented:

> …we basically look at NIST and we based everything off NIST, and we go "how can we increase our score?" And so, we look through that framework and say if we do this doesn't lift our maturity up, yes or no. (CSM2)

The target state is not static; it is assessed and reassessed on a regular basis: "there was a maturity level we wanted to gain ... a couple of jumps above that maturity level. We'd expect this level of investment, but we put that three-year horizon. ... A caveat in there that we review annually" (CSM8), the plans remain provisional and re-prioritisation can and does occur as new developments challenge them.

CSMs and their departments rarely execute roadman projects on their own; they are dependent on other parts of the organisation and on other business units. A recurring theme I the interviews was the goal conflicts within the organisations: limited resources, conflicting priorities and incentives of different business units, all of which had to be overcome for projects to be implemented:

> You've got application owners, you've got infrastructure owners, you've got IT, service management, you've got security operations, you've got IT operations. All those have different objectives, different lenses that they apply to that project or issue, and you have to work amongst all of those, not just functional roles, but the individuals in those functional roles. (CSM6)

Nothing in this extract is about technology or technical difficulties; rather, it reveals that CSMs must engage in a process of competition for resources and negotiation of goals and priorities – processes that are inherently social. CSMs advocate, influence, and gain support for their construct of reality, engaging and communicating with various stakeholders – a process described as sensegiving (Wright, 2005, p. 90). It is inherently a social activity, and CSMs need to be effective and skilled language users to achieve their strategic goals (Logemann et al., 2019, p. 1). The following extract below illustrates how a CSM used particular language and framing to align other parts of the organisation with the CSM's goals. The CSM leveraged a recent incident and their interpretation of it to frame their sensegiving (Logemann et al., 2019, p. 1) and emphasise the urgency of the preparations they considered necessary:

> The [telco] outage affected some of our second factor SMS. Second factor capabilities for our clients. ... Programmes of work were already in place to remove the reliance on a second factor SMS as a security control. ... An incident like [telco] did allow us to go back and say, well, look, here is a risk that we have again out of our control that potentially compromises our security or compromises a user experience for our clients. ... Can we bring forward our year three pass key implementation programme for a couple of key applications that we had destined for 2027? Can we throw that into the back part of 2024? And then we'd then we'd have to sort of, you know, review things. What's the risk to the business, and you sort of calculate all of these sorts of things and then the organisation could actually make a decision. So, some of them would trigger further conversations around parts of the business, not willing to invest in newer technology that provides a stronger security outcome. Now, when they see "Ohh well, if we take away our archaic SMS second factor. And replace it with something that's more contemporary, far more secure, and more customer ready." That sort of shows a modern view on the way that we're treating our clients' security and our clients' data. It then could offer a different conversation to the business

> owners and go "Oh well, actually, yeah, I hear what you're saying now. Happy to, you know, invest X amount of dollars to get this done." (CSM8)

Moving application users to another authentication technology is viewed as a measure to prevent the recurrence of an adverse event in the future caused by a telco outage. The CSM used such an outage as a source of influence to advance their world view, namely that the reliance on a third party for their business-critical operations is risky, appealing to the organisational anxiety triggered by the recent event. The CSM does not estimate the likelihood of another telco outage based on past performance, nor do they appeal to historical evidence; instead, they use a specific vocabulary, describing the SMS authentication status quo as "archaic". This is contrasted with a "contemporary", "more secure, and more customer ready" technology which is framed as a way to build customer trust and demonstrate the organisation's commitment to customer data protection, thereby making CSM's values explicit (Slovic, 2001). Through framing and narrative, CSM8 presents the risk and the need to prioritise the work in business rather than technical terms, framing security goals as business goals and guiding the sensemaking of other organisational stakeholders (Logemann et al., 2019, p. 3). As a result, instead of a goal conflict, there is an organisational alignment on objectives.

Work prioritisation was identified as one of the key features of preparation and scheduling of roadmap projects designed to forestall an adverse event. Work prioritisation can be understood, in part, as determining how quickly the CSMs and their organisations must close the "window of opportunity" (Branlat, 2011, p. 106) for attackers before they exploit it. This means that CSMs themselves also have a window of opportunity to act on signals and implement remediations before the adversaries use those windows of opportunity to achieve their goals (Branlat, 2011, p. 106). One interviewee shared his lived experience in a bank, recounting a story about prioritising work to prevent money from being stolen from ATMs. The initial decision about the urgency of preventative work was based on the received threat intelligence about ATM attacks, However, such threat intelligence about a malicious actor stealing money from ATMs does not come with an "urgency" tag or a specific date indicating when the bank's own ATMs might be targeted. These signals must be interpreted, and urgency determined, by the practitioners defending the systems. Prior decisions might need to be revised as new evidence arises. Yet, even after an ATM breach occurred in a sister bank, the priority of preventative measures within the holding company remained unchanged (Woods et al., 2021, p. 13):

> For some reason we were treating that as a normal priority programme, we were looking at it as just another project in the whole road map, we were not looking at it as the example is something that this is priority zero. ... If everything [of high priority] then something will be deprioritized.
>
> ... I've got a clear signal from a business that we want our ATMs to work flawlessly, don't want any problems with them. (CSM4)

The implementation of ATM remediations was delayed because they caused business disruptions. Only when the holding bank itself experienced a breach of their ATMs was the project implemented

immediately – a signal as strong as one's own ATM breach was required to trigger a revision of the priorities.

As in the SMS authentication story, it was only after experiencing an ATM breach directly that the CSM could overcome the business pressure and prioritise the implementation of mitigations. CSMs must continuously consider and reconsider project priorities on the roadmap as the new information becomes available. With limited resources, prioritisation becomes an act of trade-off: CSMs interpret signals, make sense of them, and shift project priorities to close the window of opportunity and prevent adverse events.

Not only do the CSMs have to navigate through goal conflicts with other business units, balancing the goals and making trade-offs are also ever-present within their own departments. With a limited budget, a CSM must choose how they allocate funds, prepare for adverse events, and determine what capabilities they develop:

> Right now, I know that I get to review about 30% of all of the indications and warnings that come into my [SIEM]. So, from my point of view, it does not make sense at all to have [incident responding] resources that are not productive 80% of the time because something may happen right? I much rather have that a smaller team because they do things that are important, potentially get that complemented with the incident response retainer from one of the big companies and then use that saved budget to actually hire more people [into] security operations to do some other work. ... It would be unacceptable for me to kind of miss something that actually was an actual incident because I'm putting money into resources that 80% of the time are not productive, right? I can't live with that trade off. (CSM5)

In this extract, the CSM anticipates that, with the current capabilities, an adverse event might be missed by the monitoring function and therefore applies his judgement to strengthen the detection and monitoring capabilities, potentially at the expense of the response function. In this case, preparation takes the form of an organisational change driven by the CSM's mental simulation, in which different scenarios are played out. While the incident response team is recognised as important, it is hard to justify the cost of keeping it when incidents are rare, as there is minimal feedback to support such investment.

Economic pressure can also affect the CSMs through personal KPIs, which shape their decision-making as they evaluate vendor capabilities and costs. In doing so, they perform a balancing act between meeting economic objectives and ensuring broader control coverage of identified risks:

> For the same amount of money you're spending on a competitive product, we can give you the same capability, actually, probably better, but we can also add 1, 2, 3, 4 and we can give you a discounted rate of return over a couple of years which, as a security leader or as a technology leader is one of my KPIs, make me meet my end of year performance targets might allow me to get a bonus internally because I'm saving money and really ultimately reducing complexity (CSM8)

The way CSMs prepare for an adverse event is shaped not only by their understanding of adversaries – their motivations and capabilities – but also by broader organisational and individual economic pressures. The personal economic pressures influence procurement decisions, which in turn shape how the organisation prepares for an adverse event.

There was an explicit recognition by the CSMs that complete prevention of adverse events is not possible; therefore, incident response capability is seen as essential. One aspect of such a preparation is the creation of runbooks – scripts invoked in response to signals of danger that direct actions and decision-making of responders. Such preparations are often the result of "baptism of fire and learning from that" (CSM2); often, runbooks are written after mitigating an incident. The use of runbooks illustrates the socio-technical nature of anticipatory work: cognitive artefacts like runbooks are used not only to capture knowledge but also to provide authority for performing potentially disruptive actions (Johnansen et al., 2015, p. 346).

Outside of projects on the roadmap, hiring was viewed as anticipatory practice, not only for incident response purposes but to cope with long-term anticipation and macro trends. This long-term capability – hiring to address the ambiguity of macro trends – can be interpreted as building adaptive capacities and developing the system's requisite variety (Flach, 2015, p. 96):

> Right now, I do think strategically about things like manpower and some of that feeds into a longer term. Like, OK, if I'm hiring somebody today, what do I want them to be able to do in three or five years, right? That shifts right. So, like right now, for example, it's like, OK, like I'm not necessarily worried about AI based attacks in the next year. We're not there yet, right? But if I'm going to hire somebody, I want somebody who has some of that background or at least some interest and someplace that's going to give me the ability in the future to play that game right and to say, yeah, we have some expertise on board that can talk about AI threats. (CSM10)

A common feature in CSMs' accounts of anticipating adverse events was a sense of being overwhelmed and experiencing operational overload: "overload of the of the operational tasks" (CSM4), "you're simply just overwhelmed by too much of it" (CSM7). The greatest anticipatory challenge concerning preparation to prevent an adverse event were resource constraints: "You know the biggest blocker is internal competition for resourcing to get things done. So that's sort of like no one's going to stop you from understanding the importance of a potential incident coming your way" (CSM8). When balancing long-term and short-term horizon, CSMs reported being more focused on present, known threats that had the potential to cause harm to their organisations: "I think I'm more scared about the present than I am about the future if that makes sense because I know of things I need to do now, and I'm trying to push to get those things in place." (CMS7). This can be interpreted as closing a known "window of opportunity" that attackers can use to achieve their goals.

One CSM expressed the view that organisations often fall behind the curve, failing to adapt quickly enough to changes driven by adversaries:

> The pace of change is increasing and that gives the attackers a much bigger advantage. Organisations are getting larger, and they become slower as a result. And if the attacker's speed is speeding up, if their ability to adapt to whatever defences we have and bypass them, continue to increase and our speed of countering that isn't increasing as well, that's an equation we're never going to win. (CSM10)

This also communicates a mismatch between the dynamics of organisational change and those of adversaries, creating the impression that preparations lag behind the actions of adversaries; defenders mostly play catch-up. The challenge is not only resource constraints, as other interviewees noted, but also the organisation's complexity, which becomes a major hindrance.

4.3 Theme 3. Anticipation is a "Team Sport"

This study aimed to understand the anticipatory practices of CSMs. While, on one level, such practices can be viewed as individual cognitive activities – stemming from expertise, intelligence, or intuition – CSMs' accounts, however, explicitly included collaboration and other interpersonal factors, such as trust. Their anticipatory practices were embedded in teamwork, invoking the metaphor that anticipation in cybersecurity is a team sport.

Throughout the interviews, it became apparent that the development of anticipation of an adverse event is inherently collaborative – a social process (Wright, 2005, p. 91). CSMs reported relying on their teams to collectively construct images of possible future and discuss their implications – an intersubjective process (Wright, 2005, p. 91):

> We call it internally as internal wisdom, and so that is much harder to quantify. I think this is the team's opinion, and I think ... it is anticipation of what is going to be the largest risk in the next period, and this is not necessarily built upon the past incidents, although there's definitely an influence of that. (CSM2)

In addition, in the interviews CSMs consistently described engagement with other organisational stakeholders as vital to their anticipatory practice; such engagement helped ensure that their anticipatory work remained aligned with broader business objectives.

CSMs equally valued engagement with parties outside their organisation, particularly those who could help update their mental models and guide their anticipation. This highlights that anticipatory practice is a dynamic and social process of meaning-making, situated within networks of internal and external peers, and trusted supporting organisations – in effect, a team sport. This sense of collectivity was inherent in both envisaging a future adverse event and preparing for it. Some practitioners even suggested that peer networks were the primary source of industry updates: "I personally do not rely much on industry analytics or magazines or anything like that. ... I instead would prefer, or I rely more on my network of my peers, whose opinion I trust." (CSM2). Here, trust is recognised as a central condition of possibility enabling such networking.

CSMs recognised that peers outside of their organisation can provide valuable perspectives on threats and security issues related to dominant technological trends, helping CSMs bootstrap their own thinking about possible incidents in their companies:

> AWS is a huge, complicated monster. So, talking to other people and saying so, what are you guys worried about? What are the threats that you're anticipating? Oftentimes it's not a one-to-one right? Nobody's going to hand me a road map that says here's how you're likely to get breached. But what that does is that gives me some starting points where I can start following those threads and saying OK, if this is true, then what does that mean for me? Could this lead to some sort of loss in the future, and if so, what do I need to do to be prepared for it, either to detect it or ideally to block? And so that comes from both people who have more experience with the technologies, but also people who have done a bunch of the thought work already and maybe in different ways than we have, right? (CSM10)

Collaboration with peers outside the organisation was consistently reported as valuable and highly desirable by most interviewees, as it helped them to make sense of technological trends. CSMs looked for and valued peers who spoke "the same language" – individuals who were perceived not only as experts but also as those able to contextualise the information and explain its relevance for meaning-making. This suggests that CSMs and their peers mutually construct a shared framework for interpretation and meaning-making that helps understand potential futures:

> People that are talking and I want to say the same language as me because it's not necessarily accurate, but people can kind of describe why something might matter. ... lot of times people say ... ransomware is big, AI is upcoming. ... But what does that mean? Right? What does "AI upcoming" mean? How does that make me worried? (CSM10)

CSMs noted that, in addition to peer networks, threat information dissemination agencies such as FS-ISAC or FIRST were also valued. These organisations facilitate anonymised information exchange between their members, which may include recent threat intelligence and incident reports. One CSM, however, highlighted a clear limitation: while often very useful, such information sharing is a sanitised monologue:

> That becomes much less of a dialogue, and much more of a monologue from the entity creating that information. ... It's anonymized, so you can't go back to the source easily and say, hey, let's grab coffee or a drink and talk me through what happened, right, completely off the record ...
>
> [Researcher] Is it something you'd prefer to be available to you? Is that it's valuable?
>
> Yeah, I would very much if information security information and intel sharing ran much more on the Chatham House rule ... (CSM10)

The extract shows CSMs desire to engage directly in a dialogue with a peer, who can share their lived experience of incidents or attacks. A possible contributing factor is that ISAC members are not individual

cybersecurity managers but organisations. This means that the information about an incident or attack necessarily goes through various organisational filters – such as legal review – before it is further anonymised and converted into a controlled narrative for dissemination. For CSMs, this does not seem to be sufficient: a direct dialogue with a peer, with the opportunity to probe for messy details, appears to be much more valuable rather than an anonymised narrative. Such peer engagements are not considered one-off but are ongoing: "you're constantly in that network. So, it's not just the people you know, but also the groups you know, and kind of really making sure you're plugged into what's happening in industry" (CSM7), the word "plugged" indicates that it is an ongoing process of learning and interpretation that supports anticipatory practices.

Relying on external peers, information sharing agencies, and being "plugged into" the network invokes an image of decentralisation and self-organisation rather than top-down governance – "decentralized anticipation" (Wildavsky, 1988, p. 9).

CSMs also relied on peer networks to learn what similar companies do to manage similar risks and prepare for adverse events. CSMs engaged in benchmarking to assess what preparations had been made in similar companies in the industry and whether these were on par with their own company. This practice allowed CSMs to identify solutions used by peers to address risks while simultaneously learning about possible implementation challenges and the "real-world" effectiveness of technical solutions:

> We started surveying a lot at companies like ourselves that we realised we are a little bit behind .... We want to determine the value of doing it, how it could be effective to implement, particularly in large technology company. So, we looked at kind of peer like companies we met with [Company], we met with [Company], we've talked to a number of those types of companies about how they implemented, had they implemented the thing we were looking to do, how did they do it, how effective was it? (CSM7)

CSMs looked for and especially valued lived experiences of their peers – "war stories" of suffering from an incident or successfully mitigating an attack. Such experiences were perceived as trustworthy, signalling that the problem was "real" and marking the information as a valid signal rather than noise. Trust within the community of practice was a pervasive theme in CSMs' accounts, enabling networking and information sharing:

> You know, it's that kind of thing where it's like, hey, I really want to share information. I want to talk about this. I want to hear about it. ... You know, it really comes down to finding the right groups and the right people that are willing to do that, even if it means ignoring something from legal to really get at the meat of what the problems are and if you can find that, great. (CSM10)

Cybersecurity as a domain of practice has a substantial reliance on vendors supplying services, software and hardware, and trust, or rather the lack of, was one the themes too. Unlike with peers, however, CSMs expressed caution about information received from a vendor, noting potential conflict of interest:

> I have kind of a love-hate relationship with vendors primarily because they like to vendor things and so it becomes much more challenging, I find .... I worry more about the types of information that they're pushing because I don't know if there is a profit motive behind it. You go to, you know somebody like, you know, like [vendor] or you go to, you know, [vendor] is another. ... So, what are you trying to get out of me? What are you trying to get me to pay for when you're giving me this and are you giving me a clear, unbiased view or only giving me part of the picture? So, you can try to use that to say, oh, and if you want more information, cut me a PO. (CSM10)

For CSMs, perceived intent or motivation was a key factor shaping how they viewed and interpreted the world. Perceived profit motivation of a vendor marked information as questionable – possibly distorted – in contrast with the shared lived experience of a peer, who had no intention to directly profit from it. Cybersecurity work is inherently socio-technical, and various technical artefacts can be viewed as team players too – for example, scanners providing information about system vulnerabilities (Woods, 2017, Rosness et al., 2016, p. 63):

> 2017 in February ... the Shadow Brokers, they have released a big dump of the hacking tools and exploit tools from the NSA. ...in the beginning of March, it became evident that all these tools, they work. ... So that's when we started preparing, that's when we've started to check our systems, whether they're vulnerable. In mid-April, we have discovered that our current vulnerability management solution, which is a primary source of such information assessing your posture, it doesn't identify that particular issue, so we're basically blind. Well, first of all, of course, we call the vendor and ask like what the heck? And then it was a lengthy back and forth discussion on is it working, is it not working, so the Vendor initially wasn't ready to take the responsibility and the time was gone. (CSM4)

Trust in the capabilities of the vendor and its technical artefact, initially present, was lost when the vendor failed to adapt its technology to capture new knowledge. As a result, the vendor's vulnerability scanner was no longer able to provide the necessary system representations (Woods, 2017) for CSM's anticipatory practices and was eventually disused.

Vendors are not mere suppliers of technology; CSMs also depend on their anticipation work – for example, on updating capabilities that are then used in CSMs' own anticipatory practices. This dependency is especially critical in the fast-moving world of cybersecurity, where well-known vulnerabilities can allow adversaries to act quickly to fulfil their goals.

4.4 Theme 4. Rituals of Assurance: "We're OK here"

A distinct cluster of codes shaped around CSMs providing assurance (Spencer, 2022, p. 793) to the organisation and its senior management that expected adverse events are prepared for and can be prevented. Assurance is provided not only to internal stakeholders within the organisation but also to wider audiences, such as regulators and customers. Within the organisation, assurance is typically provided

for two reasons: firstly, to ease organisational anxiety by convincing that adverse events are well anticipated and preparations are sufficient; and secondly, to demonstrate that money allocated to the cybersecurity function of the organisation is well spent. In regulated industries, such assurance is provided to regulators to legitimise the organisation's operations, convincing the regulators that the organisation can operate safely. Providing assurance can also extend to large audiences, including customers:

> So, we're supporting business in two ways if you will. So, one is by assessing risk and adequately responding to them and preparing to that and all that. And the second one is by proving our partners and customers that we actually can do that. (CSM2)

Providing assurance to the customers is about demonstrating that the company manages its cyber risk effectively and can be trusted.

Within the organisation, CSMs need to give senior executives and the board comfort, easing their anxiety by assuring them that the cyber risks are under control, as their careers and wellbeing can be at risk in the event of a cyber incident. Providing assurance to senior stakeholders can be seen as part of CSMs' sensegiving practice (Klein & Eckhaus, 2017, p. 225), as it involves gathering and assimilating the information from various sources and providing clear and convincing judgements in terms that these stakeholders can understand (Da Silva & Jensen, 2022, p. 1). Providing assurance can also take the form of repeated rituals, such as regular risk mitigation and control assurance meetings with management, which demonstrate that the current architecture and preparations are effective in preventing adverse events:

> …inspecting, inspecting, inspecting your architectures, your controls how sure you are they're working to the to the effectiveness that you think that they should be, because ultimately that's what you stand behind when you go to the board or your executive sponsors and say we're OK here. (CSM6)

The language used in the extract – "We're OK here" (CSM6) – captures the performative nature of assurance provision (Krahmann, 2017, p. 547), creating a shared sense of control and order and transforming the uncertainty of cybersecurity into a sense of certainty. Such performative acts are directed towards the audience seeking to control the anxiety and requiring certainty and comfort. Because executives do not speak the technical language, CSMs must generate a narrative that aligns with pre-existing ideas and norms (Krahmann, 2017, p. 547) accepted and recognised by stakeholders: "I need to translate that warm and fuzzy back to my board" (CMS8). Senior executives in the organisation need to have that comfort that risks are under control, as their careers may depend on it:

> And I think the process of doing that should also include and has often not, how you pass that assurance all the way through to your people that are signing the check or the people that are gonna lose their jobs or end up in the firing line of the public inquiry if something goes wrong and I think I think it's a security risk manager that's your job is to make sure that that assurance is available and is as efficiently as possible, pass through as it in in as near real time as possible. (CSM6)

Certain events can trigger an acute need to provide assurance to executives that an adverse event will not occur in their organisation. Widely publicised external cyber incidents, especially those with visible ramifications beyond the cyber domain, can heighten organisational anxiety, often captured in the question "Could this happen to us?" (CSM8)":

> When Colonial Pipeline was hit a few years back, we immediately reacted and looked at, OK, exactly how that happened, could that have been pulled off in our environment? ... I did a full ransomware walkthrough for the board a few years back ... when the Colonial Pipeline thing hit. The types of controls we have in place to ensure that that scenario wouldn't play out for us (CSM7).

In this case, the CSM must assemble a convincing narrative involving the "use of capabilities as 'props' to lend persuasiveness and legitimacy to a performance" (Krahmann, 2017, p. 547), ultimately communicating that "we're OK here"; we're anticipating an event like that and have prepared for it:

> How can they comprehend the answer that I give them? I've got to give it in such a way that it goes "ohh now quickly spoke to [name]. He gave me the confidence that we're good and you know we're not going to be affected in this way." (CSM8)

Providing assurance for a CSM is a sensegiving practice aimed at tuning and shaping the sensemaking of the executives. CSMs act "akin to that of a modern-day soothsayer for senior management" (Da Silva & Jensen, 2022, p. 1), translating a complex issue into simple terms – such as *affected / not affected* – which helps reduce organisational anxiety and project a sense of control in the face of a threat that could affect the organisation. The Colonial Pipeline incident described in this extract indeed could produce a strong sense of anxiety among executives, threatening to place them – as it occurred with the executives of Colonial Pipeline – in "the firing line of public inquiry" (CSM6).

In regulated organisations, regulators also need to be convinced that the organisation manages the risks effectively:

> It also brings a bunch of attention from regulators, which can be very challenging. I'm in banking. It's a regulated industry, so the Federal Reserve banks and the US Federal Reserve are very, very interested in what we do and how we do it. (CSM10)

The attention of regulators, especially after an incident, provides abundant legitimacy to the cybersecurity function, as it often results in additional funding and resources to address problems, thereby enabling the provision of assurance to executives and regulators:

> It helps that I have regulators looking at these things and saying make sure that you're doing it right, which is helpful. On the downside, it means I'm doing a lot more paperwork, right? And demonstrating that we're doing these things as well. And soothing a lot of executive worry. (CSM10)

Paperwork, dashboards, and other artefacts of data-driven assurance are used as props in the rituals of assurance (Krahmann, 2017, p. 547), making the process convincing and "real": "I'm trying to build the Power BI's so that I have a good local view of Australia. So, I will understand where we potentially have issues, where are things trending?" (CSM3). However, the data by itself does not carry inherent meaning; it needs to be contextualised and interpreted:

> Like any human I form I form that assurance on a number of things. I would love for it to all be automated and data driven. I know that that's never going to happen. And I strive to get as much of it to that level as I can easily, but I think the rest of it is about talking to people and understanding. You know, understanding their views on it (CSM6)

The data-driven assurance appears to be the superior option, as it seems to be generally trusted and preferred over a narrative. Data conveys a sense of certainty and objectivity, as opposed to narratives, which may appear fuzzy and lead to an increase of the sense of uncertainty about how risks are controlled. In this data extract, the CSM admits the limitations of the data-driven approach, resorting to interviewing stakeholders and understanding their views on risk in the organisation.

CSMs provide visibility into how the funds allocated by executives to the cybersecurity department are spent and what capabilities are being developed:

> And I think it then putting all of these controls and initiatives within those four buckets [of security programme] makes it really easy for me to articulate to particularly to my peers and my executives and my board what I'm doing with their money in a way that is very, very simple for them to understand. (CSM5)

The "four buckets" here refer to the four streams of work within the cybersecurity program – a breakdown that is easy for the audience to understand and helps convince them that funds are being well spent.

In providing assurance that risks are controlled and preparations for adverse events are in place, CSMs also defend their budgets, as there is ongoing pressure to demonstrate efficiency. This budget defence becomes especially acute when no incidents happen and the cybersecurity department risks losing its legitimacy in the eyes of executives:

> and usually your CFO is your security guys nightmare because he's like,
>
> - Well, why do we need to pay [name], you know, 500 grand a year?
>
> - Because he's a superstar.
>
> - Oh, well, no, I'm not paying anybody else that much in my business. Nothing has happened, should we get rid of him? Because that will save me money… ...
>
> so, it's just elevating their [CFO's] awareness of cyber people that aren't cheap, cyber products aren't cheap, the integration isn't… (CSM8)

For a CSM, anticipating an adverse event means not only predicting what adversaries may do and how to defend against them but ensuring that powerful stakeholders continue to see cybersecurity needs as legitimate and therefore allocate budgets and resources. An adverse event can even be redefined as a loss of legitimacy in the eyes of executives, resulting in reduced budgets and resources. The absence of incidents may be interpreted by executives as evidence that threat is absent or sufficiently low so as not to warrant additional resources for its control (Dekker, 2011, p. 106). In this case, to keep the budget, the CSM is required to present a different picture. Providing assurance therefore can help restore the balance of such feedback asymmetry: the cybersecurity expenditure is immediately visible, whereas the actual work of cybersecurity might not be.

5. Discussion

The goal of this research was to study the anticipatory practices of people in management roles in cybersecurity, focusing on how they develop foresight and prepare for possible negative scenarios to defend their organisations. The starting point for this research project was a quote from Branlat's (2011, p. 120) thesis: "anticipation means understanding and making projections regarding what the other side is targeting". The analysis of the interviews enriched and extended that notion, four themes were created using qualitative thematic analysis to answer the research question, namely:

- Construction of foresight
- Preparing for adverse events
- Anticipation is a "team sport"
- Rituals of assurance "We're OK here"

It is not surprising that, in answering the research question about anticipation, themes of foresight and preparation in advance for an adverse event fit well within the definition of anticipation – using a forward-looking stance in today's decision making and activities (Poli, 2019, p. v). Two additional themes that were created as part of the analysis extend and enrich the answer to the research question, providing additional dimensions to CSMs' anticipatory practice.

Literature on anticipation in complex socio-technical systems – particularly the works of Klein et al. (2011), Tapinos and Pyper (2018), and Rosness et al. (2016) – has been most helpful in providing a theoretical and explanatory framework for the analysis of the data. I repeatedly coded interview extracts as "story building", implying that the practitioners provided an account of their meaning-making through a narrative about the possible futures. Klein and co-authors note that "seeing" the future through a narrative and making sense of it are fundamental aspects of anticipatory thinking:

> By paying attention to the experiences of others, generally expressed through stories, we build additional patterns that we can use to govern our response to future events. Narrative is a fundamental mechanism for meaning making (Kurtz & Snowden, 2003) and is of particular use in trajectory tracking to understand the possible moves of other actors in the decision space. (Klein et al., 2011, p. 237).

Narratives about the future that CSMs construct are not value neutral – they carry values, assumptions, and political choices that shape anticipation practices. These values influence which futures are imagined, which risks are made salient, and mobilise certain organisational responses. The definition of risk and the anticipation of an adverse event are shaped by social processes and values – playing a "risk game", as noted by Slovic (2001).

The literature on senior and mid managers' sensemaking and sensegiving has proved useful in providing an explanatory lens for data analysis. In contrast, the literature focused on anticipation in cybersecurity has proved less useful for forming a theoretical and explanatory foundation. The reason for this, in my view, is that it is tends to focus on technology and adversarial interplay while avoiding human factors, organisation dynamics, managerial decision-making, collaboration, and sensemaking – as Beznosov and Beznosova (2007) and Ceric and Holland (2019) point out. This body of literature covers more technical aspects of the cybersecurity practice, such as security engineering, threat analysis, and security operations; however, it has proved to be insufficient and misaligned with the anticipatory work of cybersecurity managers. As anticipated by Beznosov and Beznosova (2007), CSMs anticipation of adverse events is social and collaborative in nature and can be characterised as prospective sensemaking (Tapinos & Pyper, 2018, Wright, 2005, Rosness et al., 2016).

5.1 Future-perfect Anticipation

There seems to be a contradiction: while the domain of cybersecurity is typically viewed as ambiguous and uncertain (van den Berg, 2024), CSMs often characterised their work as reactive, which suggests certainty. One CSM, when asked to elaborate on his attitude towards uncertainty, replied: "I'm not sure I'm qualified to anticipate that, I'm more practical person and maybe like someone can say I'm more like reactive." (CSM4). Another CSM went further and characterised the whole cybersecurity program as reactive: "I think of that of the whole cyber security programme as a reaction to external events overall" (CSM2).

The choice of words – "reactive" and "external events" – suggests that the CSMs are talking about something concrete and certain, rather than ambiguous or blurred in contour. Data analysis indicates that CSMs often imagine a future event and then work backwards to the present, exploring how an incident could happen and how it might be prevented. This corresponds to the *future-perfect* modality of prospective sensemaking (Tapinos & Pyper, 2018. p. 299).

Correspondingly, the preparations for an adverse event also fit into the logic of "predictive hindsight" (Tapinos & Pyper, 2018, p. 295): CSMs worked toward a defined maturity score, remediated found vulnerabilities, and established concrete projects on the roadmap with specific milestones and allocated resources. The idea of a linear attack progression, embodied in the "kill-chain" model (Hutchins et al., 2011), with layers of defences to prevent an adverse event, also aligns well with this dominant future-perfect modality of sensemaking (Tapinos & Pyper, 2018. p. 299).

How can these incompatible positions be explained – that cyberspace is ambiguous and unpredictable, yet CSMs behave as if it were predictable and well-modelled?

Firstly, cybersecurity is a broad domain and cybersecurity managers operate in a particular role – managing a cybersecurity program (or part of one) within an organisation. Their role requires a more pragmatic view of the world: obtaining resources, developing capabilities, demonstrating that these capabilities work, and providing assurance that the organisation is safe.

Organisations require accountability, metrics, and risk controls that can be tested. It is much easier to obtain resources to improve the NIST maturity score (Alexander, 2024, p. 30), plan projects on a roadmap and provide progress reports to the management than to obtain resources to defend against potential future social engineering attacks powered by AI. This future-perfect way of preparing for the future aligns with the definition of anticipation as a centralised control (Wildavsky, 1988, p. 35). Operating this manner – as if the domain were ordered and rational – allows CSMs to reduce organisational anxiety by demonstrating that things are under control or can be if further investments are made. Thus, for CSMs, grounding anticipatory practices in the future-perfect modality of prospective sensemaking is rational.

The future-perfect modality is also reinforced by feedback. When organisations act on a predicted future as though it has already occurred and later observe that anticipated event did occur but was prepared for and prevented, the choice of modality is reinforced: "And that you had losses before and now you don't have losses, right? So, then you have a good monetary affirmation." (CSM4). This kind of confirmation – this feedback about investments – makes the approach feel real, justifiable, and actionable. In contrast, feedback about future-oriented anticipatory practices that build capacities to deal with a variety of possible futures may be less readily available, delayed, or even unrecognised by the organisation (e.g. narrative vs financial data).

Secondly, while ambiguous and uncertain, the domain of cybersecurity is not entirely unpredictable. Adversaries can and do employ stabilised attack patterns, acting as "copycats" (CSM7). Copycat attacks exist because organisations often build their IT systems using the same technologies and similar design patterns, resembling monocultures. If existing attacks work and organisations are slow to adapt and change, there may be no need for adversaries to invest in developing new attack tactics and techniques. Expecting copycat attacks functions as a form of heuristic – a practical way to deal with uncertainties and ambiguities of the domain by relying on patterns.

Thirdly, Poli (2017, p. 2) notes that predictive models explain the anticipatory practices of organisations and people. CSM10 provided an excellent example of how repeated past experiences forms a stabilised model that guides the expectations:

> up until the day before Mirai [a DDoS botnet] hit, we were sitting around saying, "Yep, biggest attack we've ever seen was about 160 Gigabits a second ..., right, and the next day, suddenly we're seeing things that are indicating 320. And our initial thought was: "Oh, crap, who's double counting attack packets. This doesn't make any sense." We, you know, we expect an incremental increase in attack capacity from bad actors, right? We don't expect to see a sudden doubling overnight. And we did the research, and we figured it out. We realised, oh, shit, no, there's a new [DDoS] botnet out. (CSM10)

This extract shows that, for a time, DDoS attacks developed in a linear fashion, forming a stable pattern of expectations. Relying on this pattern worked for practitioners most of the time, functioning as a heuristic, however, did not guarantee complete predictability. The remark "This doesn't make any sense"

(CSM10) demonstrates a fundamental surprise (Lanir, 1986) and a breakdown in sensemaking when adversaries were able to mount an unpredictable DDoS attack.

5.2 Bad Actors and Bad Apples: Constructing Anticipation

From a broader perspective, the very essence of the cybersecurity professional's identity is that of a defender against a motivated human adversary. Consequently, an adverse event most often anticipated by CSMs is harm caused by deliberate targeted actions – whether by a financially motivated attacker, a nation-state actor conducting an espionage operation, or a disgruntled employee. Rochlin (1998, p. 10) highlights the idea that threat and security are socially constructed, defining threat "to be an expression of intentionality, and secure to be a perceptual frame, in which case both are inherently and irrevocably intersubjective". The notion of malicious intent plays a key role in how CSMs anticipate threats; understanding motivations can be considered a crucial analytical filter that helps determine who is – and is not – an adversary, making it an inherently intersubjective process.

Adverse events interpreted as the result of malicious intent are classified as cybersecurity incidents. If malicious intent is not perceived – even when the incident involves cybersecurity technical controls (CrowdStrike, 2024) – it may instead be framed as an infrastructure issue, located outside the scope of cybersecurity. Within an organisation, the perceived intent of workers is also a defining factor for CSMs in determining whether a particular situation should be labelled as insider threat or considered normal work. Perceived adversarial motivation is used as a classification factor, shaping stereotypes of different attacker types and enabling CSMs to project their likely actions into the future, as portrayed by CSM10: "North Koreans want, you know, they want money. The Chinese, they want business intelligence." Such categorisations simplify a complex reality, thereby enabling action on defenders' side.

Suffering from an adverse event is often attributed to someone's deliberate actions that exploit gaps or weaknesses in organisational defences. With this reasoning, bad things often happen because of bad actors: "They're not nice people. They're not trying to break through my firewall to, you know, give me a cookie recipe or something like that. They're bad." (CSM10). This depiction of a malicious actor disrupting the security goals of system owners closely resembles the "bad apple theory" (Dekker, 2014, p. 1). Insider threats are often framed through the "bad apple" perspective – as employees with a bad attitude toward cybersecurity, who are believed to "undermine the organized and engineered systems that other people have put in place" (Dekker, 2014, p. 1). Such issues are framed as "personal problem, a motivational one, an issue of individual choice" (Dekker, 2014, p. 2). Focusing on the malicious intent or bad attitude of an actor as a cause of suffering offers a sense of closure and reinforces a linear cause-effect narrative:

> The Western world tends to locate both the meaning and cause of suffering in the realm of human moral choice, which typically condenses accounts of failure down to single acts and actors.

> This competes with increasingly complex epistemological narratives of accidents that have neither obvious causes nor clear, linear cause-effect relationships. (Dekker, 2015, p. 202)

Using malicious intent as an epistemological explanation of an adverse event (Dekker, 2015, p. 203) implies that CSMs focus on identifying certain users of the system as malicious and excluding them from system interactions, thereby preventing them from achieving their goals before harm is caused. This reductionist logic is equally applied to the organisation's employees – the "weakest link" – who might be deemed at fault for a successful attack – for example, by clicking on the wrong link or opening the wrong attachment. The "weakest link" metaphor arises from the idea of a chain under stress: technological defences and the people who together form this imaginary chain can break at its weakest link – the people. Linear accident causality models like the "kill-chain" (Hutchinson, 2011) call for more layers of defence and improved reliability, while the "weakest links" are retrained or automated out.

Anticipating an adverse event within the logic of a linear causation model is akin to viewing anticipation through the lens of the "first story" (Cook et al., 1998, p. 3). Therefore, installing additional barriers will control the threat: "We got popped [breached] because somebody, we didn't have multi factor auth on a cloud service. We have shifted gears dramatically and now we have multi factor auth" (CSM10). This simplification – singling out a particular failed authentication technology exploited by a bad actor – enables blame allocation. Josephine Wolff, writing about the aftermath of the TJX breach, suggests that different stakeholders have strong reasons to focus on malicious actors and blame allocation:

> Various parties had strong motivations to identify a specific, single locus of blame in the aftermath of the TJX breach. Reporters wanted to offer a satisfying explanation of what had happened to curious readers. The individuals, banks, and payment card networks suing TJX to recoup the fraud losses resulting from the breach wanted to make clear that it was solely the retailer's fault this had happened, not anyone else's. Even TJX itself may have been relieved to be able to pinpoint a specific technical problem so that it could then reassure customers the wireless encryption had been fixed and its systems were now secure. (2018, pp. 20-21)

Blaming external parties for the harm caused by cyberattacks – while understandable and even useful for many stakeholders – as Wolff (2018, pp. 20-21) shows, allows organisations to maintain a moral order: attackers are bad, the organisation is good. This framing diffuses harmful consequences in an organisationally safe way (Cook and Nemeth, 2010, p. 91). It obscures the "second story" of an incident (Cook et al., 1998, p. 3). This also illustrates that defining the story of an incident – what counts, how the story is told, and who is to blame – is inherently a social and political process shaped by powerful actors.

5.3 Drifting to the Boundary

Rasmussen's bounded risk model (1997, p. 190), depicted in Figure 2, offers an interpretive lens for understanding how the interviewed CSMs defined an adverse event. In terms of the model, an adverse event can be conceptualised as the crossing of the security boundary. CSM10's story in Theme 1 about

printing loan documents at home illustrates this: exposing sensitive information through home printing – and thus breaching confidentiality – represents an irreversible crossing of the system's acceptable performance boundary (the "security boundary" in Figure 2). Allowing home printing under economic pressures due to the car loan business lost by the bank can be seen as a systemic migration of the operating point toward this boundary (Figure 2). The security margin, expressed as the rules set by the auditor that define home printing as risky and prohibited, was crossed as the operating point moved under production pressures in a competitive environment. Both the security boundary and the margin are neither static nor predefined; rather, they are socially constructed and negotiated through "an intersubjective social act" (Rochlin, 1998, p. 8). What information counts as sensitive -and what constitutes harm if it is exposed to unauthorised parties – is inherently socially and politically defined.

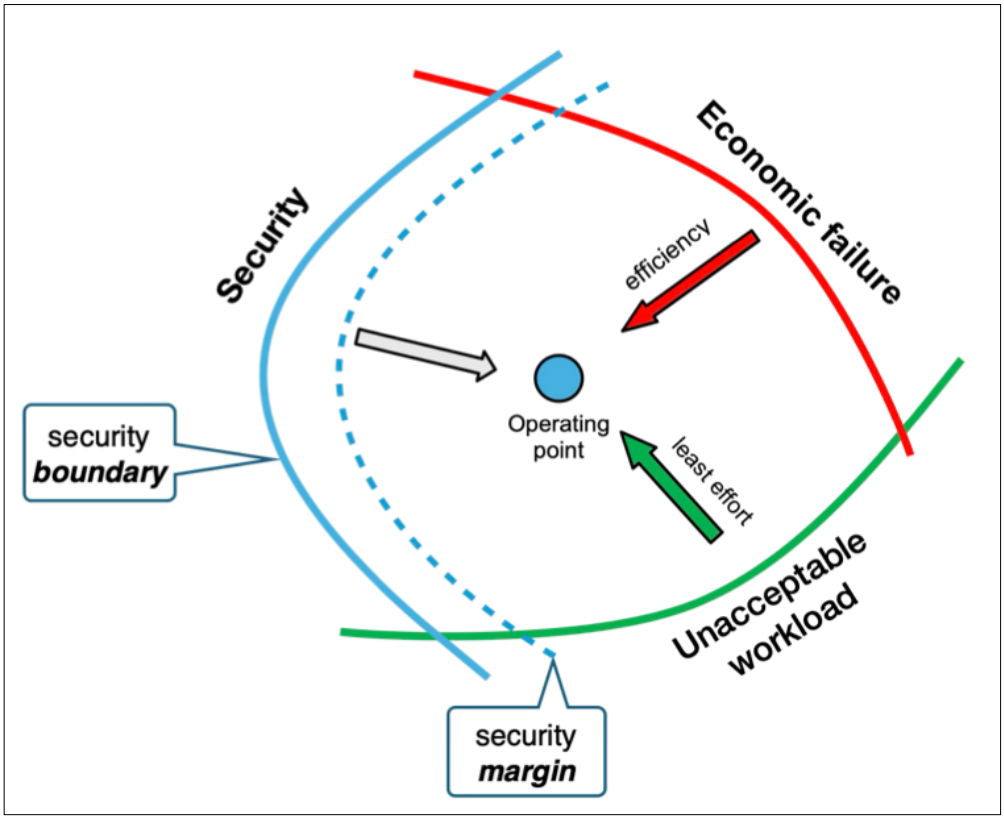

Figure 2 *Rasmussen's bounded risk model.*

One of the features of Rasmussen's model (1997, p. 190) is the idea that, under the economic and workload pressures, the operating point can drift toward the boundary of the system's functional performance – in this case, the security boundary. Dekker, however, warns that this drift is a retrospective construct, a product of hindsight: "it may only be possible in hindsight to see how decisions and trade-offs accumulated and reverberated to create a particular trajectory toward an accident" (2011, p. 19).

CSM4's story about the ATM breach in Theme 2 illustrates this drift: how business pressure to keep ATMs online affected the execution of mitigations intended to prevent the theft of money from the

ATMs. Despite the identification of a significant threat to ATM security, the bank's business leaders were unhappy with the ATM outages caused by deploying these mitigations. Under this pressure, the ATM hardening project was assigned a lower priority, leaving the ATMs vulnerable and keeping the "window of opportunity" for attackers open (Branlat, 2011, p. 117). Dekker warns that this process of "borrowing more and more from safety may go well for a while, but we never know when we are going to hit." (2011, p. 39).

Remarkably, this ATM story also shows that even a similar ATM breach in a newly acquired bank was not seen as a strong enough signal calling to review the priority of the ATM remediation project; stakeholders did not interpret it as an indication that the security margin had been exhausted. Only when the bank's own ATMs were breached was the remediation project promptly completed. The story shows that the CSM and the business leaders held different understandings about the location of the operating point, its movements, and organisational priorities. Finally, the breach of the bank's own ATMs – a direct, lived experience – was treated as a strong and unambiguous signal that clarified the boundary's location and aligned the views and priorities of the CSM and the business stakeholder.

Situating the CSMs' stories from the interviews within Rasmussen's model (1997) reveals another important aspect of anticipatory practices: power relations. Who defines where the operating point is and how far it is from the boundaries? How pressures to move away from the boundaries are negotiated and what constitutes feedback about the operating point's location depend on the power relations within and outside of the organisation. Answering the question of how cybersecurity managers anticipate an adverse event, therefore, requires acknowledging that power relations are one of the defining factors shaping anticipation. Both stories – about home printing and about the ATM breaches – highlight the power dynamics between various stakeholders: auditors, cybersecurity professionals, and business leaders.

Rasmussen noted that the most promising approach to maintaining the operating point within the boundaries is to make those boundaries explicit and allow actors to learn to cope with them (1997, p. 192). If the boundary of secure performance is socially and politically defined, making it explicit means making the "risk game" explicit – exposing the multidimensional, subjective, value-laden, and frame-sensitive nature of risk decisions (Slovic, 2001, p. 21). Allowing actors to learn how to cope at the boundaries involves learning to operate near or even at the edge of failure, where existing tools, procedures, and runbooks might be insufficient – that is, developing adaptive capacities. Adaptive capacities in this case are not just available technologies to forestall an attack but also human expertise and tacit knowledge of the system, both of which must be recognised and actively maintained: "Unattended, loss or degradation of this expertise may not be noticed until the organization experiences significant and costly impacts" (Wettick, 2024, p. 45).

5.4 Trust as Enabler of Anticipation

Weick and Sutcliffe (2007, p. 44), writing about nuclear power station operations, noted that the production of electricity is a secondary goal; establishing trust in the station's operations is the primary one: "Profitable production of electricity is secondary to establishing and sustaining trust. Without trust, there is no production." Trust emerged as a major factor shaping anticipatory practices of CSMs. It functions as an enabler of anticipatory collaboration, facilitating the sharing of information and the distinction between signal noise. Zinn (2008, p. 442) noted that trust is one of the "in-between" strategies of decision-makers managing uncertainty, helping reduce the complexity of decision-making. Relying on trust is a viable strategy to overcome the constraints of the cybersecurity domain, where decisions often must be made "without enough time or knowledge available. Such decision-making requires increased trust, e.g. in the experts with appropriate knowledge and skills" (Zinn, 2008, p. 442).

Trust in CSMs' anticipatory practices is also socio-technical (Johansen et al., 2015); it extends beyond interpersonal relationships to include technical tools. CSM4 shared a story about how their vulnerability scanner could no longer be trusted to identify vulnerabilities. When this trust collapsed, the tool fell into disuse, disrupting the CSM's anticipatory practice.

CSMs must build trust with stakeholders for whom they perform rituals of assurance. Without trust, their performance of "We're OK here" (CSM6) does not produce a sense of comfort and reassurance in stakeholders whose careers depend on CSMs' anticipation. Without trust, these powerful stakeholders will not provide resources to support CSMs' practices, making trust an existential requirement – as in the nuclear power station example above. The lived experience of CSMs' peers was actively sought out and trusted as a source of valuable information. Lived experience also fits well into the future-perfect modality: it has already happened; someone has already experienced it, making it a strong and credible signal.

5.5 Research Limitations

While this research offers a view into how people in management positions in cybersecurity anticipate, there are several limitations to it. First, the industries represented by the interviewees are limited -for example, manufacturing, retail, transportation, and healthcare are not included. Practitioners working in the public sector, law enforcement and military were not interviewed as well. Second, all interviewees are male and came from the Western tradition (Dekker, 2015, p. 202); no practitioners of Asian background participated in the research, potentially creating an imbalanced view. Expanding the research to include a wider range of industries, female practitioners, and professionals from diverse cultural and regional backgrounds could provide a richer perspective and offer a more nuanced and balanced answer to the research question.

5.6 Directions for Future Research

This research was set up to answer a broad research question, and one fruitful direction for future research could be to zoom in on specific aspects of CSMs' anticipatory practices. The following directions could be pursued:

- As noted above, gaining expertise about a system's behaviour at the boundary of acceptable performance can be a viable strategy to prevent an adverse event. An enquiry into how such expertise is developed, maintained, and eroded could be especially fruitful.
- As the research indicates, anticipation in cybersecurity is mainly oriented towards preventing harm from malicious actors. While it is undeniable that motivated attackers cause security breaches, this view can obscure organisational factors. Future research into how organisational factors – such as power relations and hierarchies – shape anticipatory practices.
- It is evident from the interviews that economic pressure on organisations translates into efficiency pressures on cybersecurity departments in general and into CSMs' personal KPIs. Further research could explore how CSMs personally balance the need to save money with the need to procure well-functioning but expensive preventative technologies.
- The interviewees revealed that adverse events can also take different shapes for practitioners – for example, limited future employment opportunities if the organisation experiences a significant cyber breach. Research into how cybersecurity managers anticipate an adverse event that might affect their personal well-being was not pursued here but could be another valuable direction for future study.
- The research indicates that cybersecurity managers operate in an environment that requires multidisciplinary education. Future research could explore which disciplines might be most useful in augmenting the dominant STEM education of cybersecurity professionals.

6. Implications

Cybersecurity is often perceived as primarily a technical discipline – one that is focused on commanding an assemblage of tools, reacting to indicators of compromise, and building defence in depth based on popular frameworks. The research, however, paints a different picture: anticipatory practices of cybersecurity managers are shaped not only by technology and formal risk analysis but also by narrative construction, interpretation of history, and socio-political interactions and negotiations. This section will first focus on theoretical implications of the research followed by broader implications for the cybersecurity domain, and finally outline specific implications informing future policy and practice.

6.1 Theoretical implications

The research links a range of existing theoretical perspectives – including cybersecurity and risk management, anticipation, sensemaking, cognitive science, the theory of performativity, safety science, and sociology – in novel ways. It offers a critique of the dominating linear adversary-centric model of anticipation, arguing that this perspective is too narrow and neglects the complexity of organisational factors in anticipatory practices. Instead, the phenomenon of anticipation is framed as a wide social process rather than a narrow exercise in technical risk management.

6.2 Broader Implication for Cybersecurity

Shifting the view of anticipation from a technology-centric adversarial interplay to a broader social process implies that "doing" cybersecurity within an organisation means engaging in a social and political process. From this perspective, cybersecurity work is not limited to deploying and managing technical defences; it is also about a process of meaning-making, building trust, and navigating organisational goal conflicts.

Consequently, cybersecurity managers require more than technical expertise – they must also develop the capacity to navigate the organisational political landscape.

6.3 Constructed Foresight

The future in cybersecurity is not an objective reality "out there" waiting to be uncovered, it is actively produced through social processes. What is seen as a "real" and "plausible" threat is shaped by internal negotiations among stakeholders who hold power and political capital. As a result of such negotiations, certain threats can be ignored or downplayed, resulting in defences against them being. Conversely, other threats can gain priority because they are positioned as resonating with dominating organisational narratives – such as being "customer-ready" and "contemporary". A narrow focus on malicious actors and linear risk models fails to capture this complex organisational dynamic, often obscuring socio-political processes through which priorities are formed.

Anticipation in cybersecurity thus becomes an inherently political process, in which different actors advocate for competing constructions and interpretations of meaning, each leading to distinct organisational actions. Surprise or failure to anticipate can therefore be seen as not just a failure of prediction but as a result of the internal organisational dynamic.

Consequently, improving anticipatory practices and the construction of foresight is not merely about getting better threat intelligence, tools, and dashboards. Rather, it involves improving the social processes of anticipation in an organisation. This may include making stakeholders' assumptions and values explicit, changing organisational hierarchies and power structures, and creating space for reflexive practices – ultimately positioning anticipation as a broader organisational improvement.

6.4 Demands of Cybersecurity Manager's Role

Viewing anticipation of adverse events as a social and political process – rather than as mostly a technological race between attackers and defenders – exposes the often-hidden demands placed upon a cybersecurity manager's role. Not only do they need to be technically skilled, but their effective anticipatory work requires a repertoire of social, political, and organisational competences. Yet, contemporary cybersecurity education and regulatory perspective remain explicitly grounded in the STEM curriculum, reducing the socio-technical nature of the profession to mainly technical concerns. Meaningful progress in cybersecurity may depend on overcoming the dominance of the technical epistemology, and explicitly recognising the social processes within which technologies are situated.

6.5 Enabling Trust

The theme Anticipation as a team sport highlights the importance of trust between cybersecurity managers and their peers outside the organisation, positioning such trust as an enabler of anticipatory practices. Supporting these practices for cybersecurity managers would mean lowering legal and regulatory barriers to information sharing. One of the participants (CSM10) directly called for the adoption of Chatham House-style rules of information sharing to govern dialogue between cybersecurity practitioners across organisations, thereby enabling vital information exchange.

7. Conclusion

This research set out to understand how cybersecurity managers anticipate adverse events through semi-structured interviews and qualitative thematic analysis. Focusing on the lived experiences of cybersecurity practitioners in management positions, the study generated four themes: the construction of foresight, preparations for adverse events, collectivity of anticipation, and assurance-giving. Together, these themes provide a rich description of how anticipation is practiced in naturalistic settings.

The analysis suggests that prevailing understanding of anticipation in cybersecurity as focusing on software vulnerabilities, modelling capabilities of adversaries, and building defences against breaches is simplified and superficial. Cybersecurity managers engage in anticipation by constructing narratives of the future and engaging in the process of prospective sensemaking, while navigating the web of competing priorities within the organisation. An adverse event here is not a fixed reality awaiting to be found "out there"; rather, it is socially negotiated and constructed through organisational meaning-making processes. The analysis shows that anticipation of adverse events in cybersecurity is a socio-political process – one that produces meaning, negotiates appropriate responses, and performs confidence that helps manage organisational anxiety. This way, the future is cast as tamed, and the environment is framed as predictable and stable.

The research contributes theoretically by integrating insights from cybersecurity, study of anticipation, organisational studies, and the "new view" of safety science. First, it conceptually reframes anticipation of adverse events in cybersecurity as a social and collaborative process situated within organisational context, rather than a predominantly technical affair. Second, it exposes the hidden demands of cybersecurity managers' role, highlighting the need for competences in storytelling, political negotiation, and trust building. Third, it demonstrates the limits of current anticipatory practices, which are mostly narrowly focused on malicious actors and overlook broader organisational and system dynamics.

The practical contribution is in the suggestion to shifting the focus of education policy in cybersecurity by explicitly balancing the STEM curriculum with social sciences, preparing new generations of professionals for the demands of their roles.

In closing, the research reveals the anticipation of adverse events in cybersecurity as an ongoing collective process of meaning-making, shaped by organisational politics and power relations, and performing confidence and control in the face of ambiguity.

References

Ahrend, J. M. & Jirotka, M. (2019). Anticipation in Cyber-security. In Roberto Poli (Ed.), *Handbook of Anticipation: Theoretical and Applied Aspects of the Use of Future in Decision Making*. Springer Verlag. pp. 1559-1585.

Alexander, C. (2024) *Risky Business: Quantitative Risk Assessments as Enabling Devices in Cybersecurity*. Lund University

Allspaw, J. (2016). Human factors and ergonomics practice in web engineering and operations: navigating a critical yet opaque sea of automation. *Human Factors and Ergonomics in Practice*, 313-322.

Australian Broadcast Corporation. (2021). *Colonial Pipeline CEO confirms company paid $5.6 million ransom to 'DarkSide' hackers*. https://www.abc.net.au/news/2021-05-20/colonial-pipeline-ceo-confirms-company-paid-ransom-darkside/100151094

British Broadcast Corporation. (2017). *NHS 'could have prevented' WannaCry ransomware attack*. https://www.bbc.com/news/technology-41753022

Beznosov, K.and Beznosova, O. (2007), "On the imbalance of the security problem space and its expected consequences", *Information Management & Computer Security*, 15(5), 420-431. https://doi.org/10.1108/09685220710831152

Branlat, M. (2011). Challenges to Adversarial Interplay Under High Uncertainty: Staged-World Study of a Cyber Security Event [Doctoral dissertation, Ohio State University]. OhioLINK Electronic Theses and Dissertations Center. http://rave.ohiolink.edu/etdc/view?acc_num=osu1316462733

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101.

Braun, V., & Clarke, V. (2022). *Thematic Analysis: A Practical Guide*. SAGE Publications Limited

Ceric, A. and Holland, P. (2019), "The role of cognitive biases in anticipating and responding to cyberattacks", *Information Technology & People*, 32(1), 171-188. https://doi.org/10.1108/ITP-11-2017-0390

Cook, R. I., & Nemeth, C. P. (2010). "Those found responsible have been sacked": some observations on the usefulness of error. *Cognition, Technology & Work*, *12*, 87-93.

Cook, R.I., Woods, D.D., & Miller, C. (1998). A tale of two stories: contrasting views of patient safety. US National Patient Safety Foundation.

CrowdStrike. (2024, August 6). *External technical root cause analysis—Channel File 291*. https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf

Da Silva, J., & Jensen, R. B. (2022). " Cyber security is a dark art": The CISO as Soothsayer. *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW2), 1-31.

Dekker, S. (2011). *Drift into Failure: From Hunting Broken Components to Understanding Complex Systems (1st ed.)*. CRC Press. https://doi.org/10.1201/9781315257396

Dekker, S. (2014). *The Field Guide to Understanding 'Human Error' (3rd ed.)*. CRC Press. https://doi.org/10.1201/9781317031833

Dekker, S. W. (2015). The psychology of accident investigation: epistemological, preventive, moral and existential meaning-making. *Theoretical Issues in Ergonomics Science*, *16*(3), 202-213.

Flach, J. M. (2015). Supporting self-designing organizations. *Journal of Design, Economics and Innovation*, *1*(2), 95-99.

Fuller, T., & Loogma, K. (2009). Constructing futures: A social constructionist perspective on foresight methodology. *Futures*, 41(2), 71-79.

Greenberg, A. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. WIRED. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Ham, J. V. D. (2021). Toward a better understanding of "cybersecurity". *Digital Threats: Research and Practice*, 2(3), 1-3.

Hutchins E. (1995) *Cognition in the wild*. MIT Press.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, *1*(1), 80.

Klein, G., Snowden, D., Pin, C. L. (2011). Anticipatory Thinking. Informed by Knowledge Expert Performance in Complex Situations. In K.L Mosier, U. M. Fischer, (Eds.). *Informed by Knowledge: Expert Performance in Complex Situations (1st ed.)*. Psychology Press. https://doi.org/10.4324/9780203847985.

Johansen, J.P., Almklov, P.G. & Mohammad, A.B. What can possibly go wrong? Anticipatory work in space operations. *Cognition, Technology, and Work* 18, 333–350 (2016). https://doi.org/10.1007/s10111-015-0357-8

Krahmann, E. (2017). From performance to performativity: The legitimization of US security contracting and its consequences. *Security dialogue*, *48*(6), 541-559.

Kurtz, C. F., & Snowden, D. J. (2003). The new dynamics of strategy: Sense-making in a complex and complicated world. *IBM systems journal*, *42*(3), 462-483.

Lanir, Z. (1986). Fundamental surprise. *Eugene, OR: Decision Research*, *424*.

Logemann, M., Piekkari, R., & Cornelissen, J. (2019). The sense of it all: Framing and narratives in sensegiving about a strategic change. *Long Range Planning*, *52*(5), 101852.

Lund University. (n.d.). Research ethics and animal testing ethics [Accessed: 2024-5-30].

Muller, L. P. (2024). Cybersecurity in practice: The vigilant logic of kill chains and threat construction. *European Journal of International Security*, 1-21.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper No. 29).

Pitsis, T. S., Clegg, S. R., Marosszeky, M., & Rura-Polley, T. (2003). Constructing the Olympic dream: A future perfect strategy of project management. *Organization science*, *14*(5), 574-590.

Poli, R. (2017). *Introduction to Anticipation Studies*. Springer Cham

Poli, R. (2019). Introducing Anticipation. In Roberto Poli (Ed.), *Handbook of Anticipation: Theoretical and Applied Aspects of the Use of Future in Decision Making*. Springer Verlag. 3-16.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety science*, *27*(2-3), 183-213.

Rochlin, G. I. (1998). The social construction of safety. In *Nuclear Safety* (pp. 4-25). CRC Press.

Rosness R, Evjemo TE, Haavik T and Wærø I (2016) Prospective sensemaking in the operating theatre. *Cognition, Technology & Work* 18(1): 53–69.

Shostack, A. (2014). *Threat modeling: designing for security*. John Wiley & Sons.

Slovic, P. (2001). The risk game. *Journal of hazardous materials*, *86*(1-3), 17-24.

Spencer, M. (2022). Characterising assurance: scepticism and mistrust in cyber security. *Journal of Cultural Economy*, *17*(6), 793–808. https://doi-org.ludwig.lub.lu.se/10.1080/17530350.2022.2098515

Tapinos, E., & Pyper, N. (2018). Forward looking analysis: Investigating how individuals 'do' foresight and make sense of the future. *Technological Forecasting and Social Change*, 126, 292-302.

van den Berg, B. (2024). Dealing with uncertainty in cyberspace. *Computers & Security*, *144*, 103939.

Weick K. (1995) *Sensemaking in organizations*. SAGE, Thousand Oaks

Weick, K. (2011). Organizing for Transient Reliability: The Production of Dynamic Non-Events. *Journal of Contingencies and Crisis Management*. 19. 10.1111/j.1468-5973.2010.00627. x.

Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the unexpected: Resilient performance in the age of uncertainty* (2nd ed.). Jossey-Bass.

Wettick, M. (2024) *Adaptive tactics in software operations: How people manage complexity by asking for help*. Lund University

Wildavsky, A. (1988). *Searching for Safety (1st ed.)*. Routledge. https://doi.org/10.4324/9781351316248

Woods, D. D. (2017). STELLA: Report from the SNAFUcatchers Workshop on Coping With Complexity. Columbus, OH: The Ohio State University.

Woods, D.D. (2018). The theory of graceful extensibility: basic rules that govern adaptive systems. *Environment Systems and Decisions*, 38, 433-457.

Woods, D.D., Branlat, M. (2010) Hollnagel's test: being 'in control' of highly interdependent multi-layered networked systems. *Cognition, Technology, and Work*, 12, 95–101. https://doi.org/10.1007/s10111-010-0144-5

Woods, D., Licu, T., Leonhardt, J., Rayo, M., Balkin, E., & Ciponea, R. (2021). Patterns in how people think and work: importance of patterns discovery for understanding complex adaptive systems. In *EUROCONTROL*.

Wright, A. (2005). The role of scenarios as prospective sensemaking devices. *Management Decision*, *43*(1), 86-101.

Zinn, J. O. (2008). Heading into the unknown: Everyday strategies for managing risk and uncertainty. *Health, risk & society*, *10*(5), 439-450.

Appendices

Appendix 1. Research Ethics

Interview participants have been asked to sign an informed consent form, in accordance with Lund university's requirements. As per Lund University's ethic research guidelines (n.d.), ethic approval is not needed for such research and was not obtained.

Appendix 2. Compliance with Personal Data Protection Laws

All data collection and processing will be done in accordance with the EU's GDPR. Interviewees are not identified in the thesis and all interview recordings and raw transcripts have been deleted.