The tensions of cyber-resilience: from sensemaking to practice

Benoît Dupont [a], Clifford Shearing [a, b, c], Marilyne Bernier [a], Rutger Leukfeldt [d, e]

[a] Université de Montréal, International Centre for Comparative Criminology, Montreal QC H3C 3J7, Canada
[b] University of Cape Town, Department of Public Law, Rondebosch 7701, South Africa
[c] University of Toronto, Centre for Criminology & Sociolegal Studies, Toronto ON M5S 3K9, Canada
[d] The Hague University of Applied Sciences, Centre of Expertise Cyber Security, Johanna Westerdijkplein 75, 2521 EN, The Hague, The Netherlands
[e] Netherlands Institute for the Study of Crime and Law Enforcement, De Boelelaan 1077, 1081 HV, Amsterdam, The Netherlands

Corresponding author: Benoît Dupont (benoit.dupont@umontreal.ca)

CRediT authorship contribution statement
Benoît Dupont: Conceptualization, Methodology, Formal analysis, Investigation, Writing – Original Draft, Supervision, Project administration, Funding acquisition. **Clifford Shearing**: Conceptualization, Writing – Review & Editing, Supervision. **Marilyne Bernier**: Conceptualization, Formal analysis, Investigation, Data Curation. **Rutger Leukfeldt**: Conceptualization, Investigation.

Funding: This work was supported by the Social Sciences and Humanities Research Council [grant number 435-2018-0615]; and the Global Risk Institute in Financial Services.

Declaration of competing interest: None

The tensions of cyber-resilience: from sensemaking to practice

Abstract: The growing sophistication, frequency and severity of cyberattacks targeting all sectors highlight their inevitability and the impossibility of completely protecting the integrity of critical computer systems. In this context, cyber-resilience offers an attractive alternative to the existing cybersecurity paradigm. We define cyber-resilience as the capacity to withstand, recover from and adapt to the external shocks caused by cyber risks. This article seeks to provide a broader organizational understanding of cyber-resilience and the tensions associated with its implementation, using financial institutions as a case study. We apply Weick's (1995) sensemaking framework to examine four foundational tensions of cyber-resilience: a definitional tension, an environmental tension, an internal tension, and a regulatory tension. We then document how these tensions are embedded in cyber-resilience practices at the preparatory, response and adaptive stages. We rely on qualitative data from a sample of 58 cybersecurity professionals in the financial sector – a particularly exposed field – to uncover these tensions and how they reverberate across cyber-resilience practices.

Keywords: cyber-resilience; risk management; cyber-risks; sensemaking; regulation; standardization

1. Introduction

Over the past 25 years, cyber-risks have morphed from mere annoyances into potentially catastrophic events threatening the survival of technology-dependent organizations. There has been a growing awareness that electrical grids, telecommunication networks, digital financial flows, and transport infrastructures, on which modern societies depend to function, are particularly exposed to cyberattacks (Greenberg, 2019). Despite significant investments in cybersecurity technologies, organizations remain exposed to a constant barrage of online harms that include ransomware, business email compromise (BEC), distributed denial-of-service attacks, data breaches, or the deployment of remote access malware to exploit international transfer systems and steal millions (Carnegie Endowment for International Peace, 2021). To respond to the proliferation of cyber-risks and the limited effectiveness of existing cybersecurity approaches, regulators, standard-setting bodies, and cybersecurity consultants are gradually promoting the concept of cyber-resilience as a new framework extending established risk management practices.

Despite a long history in the fields of materials science, ecology, psychology, and natural disaster management, the concept of resilience remains largely peripheral in the literature on cyber-risks. When used, it relates primarily to the technical concerns of computer scientists, whose primary research questions examine the engineering features that can make cyber systems more robust and the metrics that can be used to evaluate their capacity to endure (Bodeau and Graubart, 2011; Ross et al., 2021). It is only recently that a growing interest has resulted in the adoption of a more holistic approach to understanding what types of preparations, responses, recovery, and adaptation activities contribute to enhancing an organization's cyber-resilience to adverse events (Linkov et al., 2013; Sepulveda Estay et al., 2020).

If cyber-resilience is to become the new cyber-risk management paradigm promoted by cybersecurity consultants, standards-setting organizations and regulators, a better understanding of the organizational and social practices that influence the adoption of this more holistic mindset is needed. Most of the literature on cyber-resilience remains theoretical or normative, and this contribution aims to provide a broader organizational understanding of cyber-resilience. We are particularly interested in two questions: first, how do cybersecurity professionals make sense of this new concept, which could arguably be construed as one of the latest fads to afflict the field of cybersecurity, and how do they articulate it with more established cybersecurity frameworks? Second, what types of sensemaking challenges do they experience when translating cyber-resilience theory into action? Our use of the concept of sensemaking as an individual and social process is inspired by Weick's work on how people and organizations respond to surprises and address the unknown (Weick, 1995).

This article uses qualitative data from a sample of 58 cybersecurity professionals in the financial sector—a particularly exposed field that has reached a higher level of cybersecurity maturity. Our objective is to map the sensemaking constraints encountered by cybersecurity professionals when applying cyber-resilience measures and to elicit their insights on promising strategies they have used to overcome those hurdles. We start with a quick overview of the existing literature on cyber-resilient organizations and how it is translated into frameworks, standards, guidelines and regulations. We also introduce the notion of sensemaking. We then describe our qualitative methodology and the sample of financial sector cybersecurity professionals we interviewed. The following two sections detail the sensemaking tensions respondents experienced when trying to derive meaning from the cyber-resilience concept and how these tensions reverberated across the continuum of preparation, response and adaptation practices.

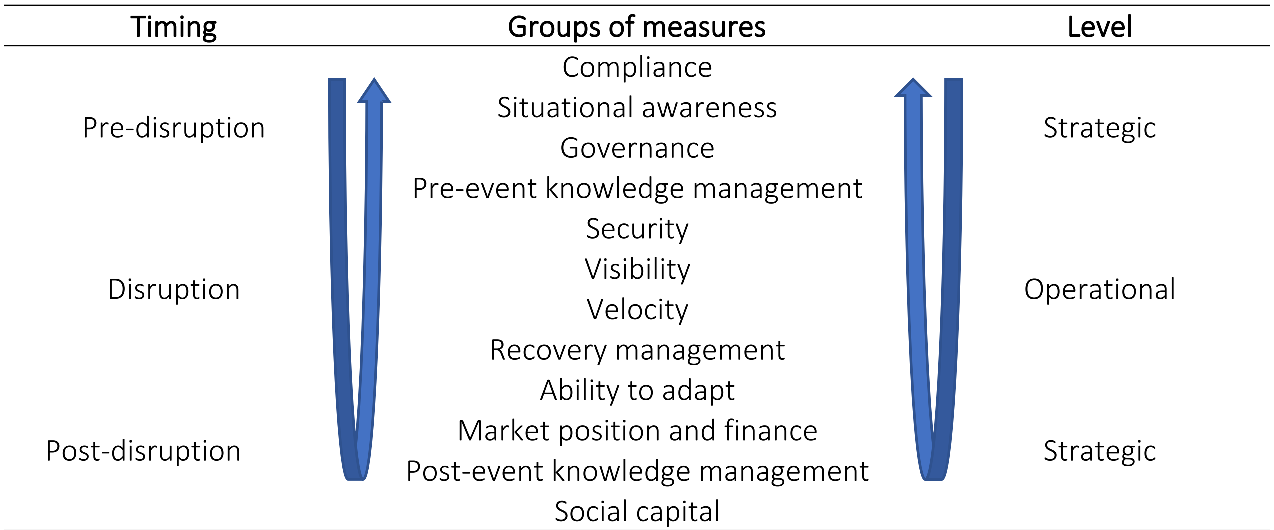
2. The rise of cyber-resilience

One of the main challenges associated with the general concept of resilience lies in its polysemic nature, derived from its use across multiple disciplines such as physics, materials science, ecology, psychology, and urban planning (Alexander, 2013; Dupont, 2019; Tiernan et al., 2019). For example, while engineering approaches favor a set of measurable parameters that can quickly bring a system back to its original state, ecological approaches place more emphasis on processes that foster persistence and often imply adaptation to new environmental extremes (Holling, 1996). It results that resilience is often used as a metaphor reflecting discrete disciplinary perspectives and that a scientific consensus on the core components, practices and metrics that should be used to define it has not emerged yet (Linkov and Kott, 2019). Practitioners face the same dilemmas due to a lack of standardization in the field of resilience (Linkov et al., 2016).

In the digital domain, cyber-resilience is defined as "the ability […] to prepare, absorb, recover, and adapt to adverse effects" caused by cyberattacks (Linkov and Kott, 2019: 2), with the ultimate aim for the organization to continuously deliver the intended functions or services (Björk et al., 2015: 312). In practical terms, it means that cyber-resilient organizations are able to contain and minimize the extent of disruptions caused by such events more effectively than their peers and that they can also resume satisfactory levels of performance faster and more efficiently. In that sense, cyber-resilience differs from cybersecurity, which describes the capacity of an organization to predict, prevent and avert the occurrence of cyber-risks. Where cybersecurity focuses on information technologies, cyber-resilience adopts a broader perspective to consider how cyber-risks that can threaten the survival of the entire organization impact a diverse range of business processes (Björk et al., 2015). This broader perspective also implies a more holistic approach, where security cannot be reduced to the sum of all the technical tools deployed within an organization but results from the constant interactions of humans, devices and algorithms enmeshed in a dense web of internal and external networks (Linkov et al., 2013; Dupont, 2019).

Disaster management researchers, who study how large-scale adverse events are handled by organizations (Manyena, 2006; Paton and Johnston, 2017), have generated two insights that are relevant to cyber-resilience. These findings are related to the different meanings the notion of resilience can take and the existence of various levels of resilience in constant interaction. First, resilience can be interpreted very differently by organizations with diverse levels of maturity in this area. Organizations starting their journey toward resilience define it as the ability to maintain the status quo and absorb the impact of disturbances. In contrast, more advanced organizations embrace an adaptive understanding of resilience that relies on self-organization and the adoption of new practices that do not compromise structure or functions. At the most mature end of the resilience continuum, a minority of organizations can leverage the transformative power of resilience to seize the new opportunities created by a changing environment and use adversity as a growth opportunity (Davidson et al., 2016). The second insight implies that studying resilience in complex systems—such as the financial sector that concerns us here or the operators of critical digital infrastructures—requires mapping the myriad of cross-scale interactions produced by geographical, temporal, organizational, social and technological factors enhancing or hindering resilience (Ansell et al., 2010; Linkov and Kott, 2019).

Several applied frameworks have been proposed to guide organizations on their cyber-resilience journey and to help them embed resilience practices at each stage of the risk lifecycle (Keys and Shapiro, 2019). In a systematic review, Sepúlveda Estay et al. (2020) identified more than 200 cyber-resilience frameworks published in peer-reviewed journals (mostly since 2013) and originating from 25 application areas (from power grids and manufacturing to healthcare and finance). These frameworks rely on a diverse set of quantitative and qualitative methodologies (from game theory and machine learning to systems architecture and regulatory approaches) to prescribe measures organized in twelve categories, thereby revealing the dynamic nature of resilience practices (what is done before, during and after a disruption) and the multiple levels at which they take place (operational vs. strategic), as shown in Figure 1. A quantitative analysis indicates that most frameworks focus on pre-event knowledge management (risk analysis and sensemaking activities) and operational measures (security, visibility of systems, velocity of response) (Sepúlveda Estay et al., 2020: 9).



Timing	Groups of measures	Level
	Compliance	
Pre-disruption	Situational awareness	Strategic
	Governance	
	Pre-event knowledge management	
	Security	
Disruption	Visibility	Operational
	Velocity	
	Recovery management	
	Ability to adapt	
Post-disruption	Market position and finance	Strategic
	Post-event knowledge management	
	Social capital	

Figure 1. Twelve categories of cyber-resilience measures (adapted from Sepúlveda Estay et al., 2020).

Risk consultancies have also embraced the concept of cyber-resilience in their marketing material, extolling its virtues and urging existing or potential customers to adopt what they claim is the "future of cybersecurity". In a review of eleven industry reports published by accounting, insurance, certification, software, and cybersecurity firms between 2013 and 2018 (the same period during which academic publications on cyber-resilience frameworks took off), Dupont (2019) identified twelve categories of measures associated with cyber-resilience outcomes. Although their terminology differs slightly, they follow the same risk lifecycle management framework as the one found in academic publications, which differentiates technological and organizational interventions at the pre-event, shock, and post-event stages of an adverse incident. Like their academic counterparts, these industry publications focused more on pre-event activities (such as risk-mapping, crisis scenarios, prevention, simulations, and insurance) and the operational capacities needed during an incident (such as detection, incident response, recovery, and forensics), than they do on post-incident measures (such as adaptation). Additionally, two cross-cutting activities (responsibility-sharing and networking) were frequently mentioned.

The cyber-resilience recommendations by consultancies are closely aligned with the frameworks developed by standards-setting organizations such as the International Organization for Standardization (ISO) and the US National Institute of Standards and Technologies (NIST). Both organizations have designed cybersecurity standards (the ISO 27000 family of information security standards and the NIST's Cybersecurity Framework) that include many measures aligned with the cyber-resilience approach. ISO's framework has, for example, been designed in liaison with ISO's resilience and risk management committees. At the same time, one of its more focused standards (ISO/IEC 27035) provides a set of guidelines to plan, prepare, and conduct cyber incident response activities (Disterer, 2013). The NIST Cybersecurity Framework is organized around a 'Core' of five functions (Identify, Protect, Detect, Respond, and Recover) that includes *de facto* cyber-resilience activities (such as the testing of response and recovery plans, the implementation of technical resilience mechanisms to face adverse situations, or the incorporation of lessons learned activities into recovery plans) (Shackelford et al., 2015). In December 2021, NIST released a new guidance document that provides a more detailed overview of how cyber-resilience translates into engineering approaches and lists eight technical objectives and fourteen techniques that contribute to this goal (Ross et al., 2021). More specialized standards have also been proposed concerning various domains of cyber-resilience, such as the CERT Resilience Management Model developed at Carnegie Mellon University (Caralli et al., 2016) or the work conducted at the European Union Agency for Network and Information Security, which supports expert groups developing sectoral cyber-resilience guidelines (ENISA, 2011).

This recent surge of interest in cyber-resilience and its enabling practices, combined with the increased frequency and severity of cyber-attacks targeting financial institutions, explains why regulators have also embraced the cyber-resilience terminology. As a result, they are developing a broad range of assessment, guidance and compliance tools to increase the capacity of the institutions they oversee to withstand cyber-shocks. International organizations such as the Bank for International Settlements, the Basel Committee on Banking Supervision and the European Central Bank have convened working groups and published documents to foster the adoption of harmonized cyber-resilience practices (CPMI-IOSCO, 2016; BCBS, 2018; ECB, 2018). National regulators and central banks in the US, Canada, Australia, New Zealand, Hong Kong, Singapore, the UK, the Netherlands, Denmark and many other G7 and G20 jurisdictions have responded with cyber-resilience activities ranging from awareness programs outlining what differentiates cyber-resilience from cybersecurity to aggressive simulation and penetration testing exercises (Maurer and Nelson, 2020).

3. Making sense of cyber-resilience

While academic, marketing and regulatory interests are converging toward cyber-resilience as an emerging cybersecurity paradigm, this growing body of knowledge remains predominantly normative. It tends to minimize the ambiguities and contradictions associated with the concept of resilience (Alexander, 2013). This problem is compounded by a minimal pool of empirical studies that examine how cybersecurity professionals and the organizations employing them make sense of these tensions and resolve them in practice (Fujs et al., 2019). This is problematic for two reasons. First, it prevents us from assessing to what extent cyber-resilience is effectively being understood, incorporated, ignored or even rejected by cybersecurity professionals, and how they translate its various concepts into practice. Second, it limits our understanding of how human factors (at both organizational and individual levels) practically enable, constrain or interfere with the core cyber-resilience activities usually prescribed by the most influential scholars, standards and frameworks, and how cybersecurity professionals handle this translation from theory to practice.

The concept of sensemaking was first delineated by Weick (1995) and referred to the range of processes through which people and organizations “structure the unknown so as to be able to act in it” (Ancona, 2012: 3). It seems particularly well-suited to analyze problematic situations where the cyber-resilience of organizations is tested. The notion of sensemaking has been used to explain how some organizations manage to maintain high levels of reliability in the face of complex environments and catastrophic risks (Weick & Sutcliffe, 2015). Specifically, Weick outlines some activities that contribute to sensemaking, such as “placement of items into frameworks, comprehending, redressing surprise, constructing meaning, interacting in pursuit of mutual understanding, and patterning” (Weick, 1995, 6). As such, sensemaking includes a much broader set of practices than simply interpreting events, as its name might suggest. Moreover, far from being limited to a contemplative state, sensemaking instead blends cognition and action (Steigenberger & Lübcke, 2022), “making the intractable actionable” (Ancona, 2012: 4). Ambiguous and uncertain contexts are particularly fertile grounds for sensemaking activities. This explains why a copious amount of research has studied how sensemaking unfolds during and after a crisis to help understand short-term responses and longer-term organizational learning (Maitlis & Sonensheim, 2010). Some authors have examined how sensemaking operates in IT environments during a crisis (Tapanainen, 2017). Still, so far, there have been very few applications of sensemaking to the work of cybersecurity incident response teams and cyber-resilience professionals (Lakshmi et al., 2021).

4. Data and methods

Our study blends three qualitative methodologies to capture the experience of cybersecurity professionals who deal routinely with cyber-attacks in the financial sector. We interviewed 58 respondents from 37 organizations. A purposeful sampling approach (Patton, 2015) was adopted to achieve a diversity of views and experiences across five specific dimensions (geography, institutional type, institutional size, interviewee role, and interviewee experience) and to ensure the networked aspect of cyber-resilience was adequately represented. The geographical diversity of the sample recognizes both the global nature of the cyber-resilience challenges faced by financial institutions and the local cultural or regulatory features that may foster different national practices. Respondents were interviewed in Canada, the US, the UK, the Netherlands, and France. Some organizations in each country had a vast international exposure, operating in dozens of markets, while others maintained a local footprint. The size of institutions for which the respondents worked also varied significantly–some of them have less than a billion USD$ in annual revenue, while others' profits can reach five to ten times that amount–leading to varying levels of resources and expertise available to implement cyber-resilience practices. The financial sector provides various services to retail and commercial customers. To take this into account, the sample included cybersecurity professionals who work for banks, insurance companies, pension funds, and stock exchanges. The consulting and incident-response firms that provide cybersecurity services to financial firms and the regulators who oversee their activities were also interviewed. The respondents' positions ranged from Chief Information Security Officers (CISOs) and Chief Risk Officers (CROs) to Directors of Security Operations Centres (SOCs), Incident Response Teams (CSIRTs), and business continuity units; leaders of penetration-testing teams and red teams; and IT governance and security advisors. Experience in a cyber-risk management or regulation role ranged from half a year to more than thirty years. Table 1 provides an overview of the respondents' features.

Country		
Canada	32	55%
United Kingdom	2	3.5%
United States	4	7%
France	14	24%
Netherlands	6	10.5 %
Total	58	100%
Organization		
Financial institution	36	62%
Regulator	8	14%
Incident response firm	9	16%
Government	5	8%
Total	58	100%
Gender		
Female	13	22%
Male	45	78%

Total	58	100%
Years of experience (in the current organization)		
Mean	11.4 years	
Median	11 years	
Range	0.5 – 31 years	

Table 1. Respondents' descriptive statistics

Interviews were conducted between August 2018 and November 2020 in person (36), by phone or videoconference call (21), or by email (1). Thirteen respondents (22%) were female, a higher representation than the 11% average for women in the cybersecurity workforce (Frost and Sullivan 2017). Interviews lasted for 57 minutes on average (range: 31 minutes to 1 ½ hour). They were recorded and transcribed for qualitative analysis, except for three interviews in public settings (café or restaurant) where the noise level was too high for recording, and handwritten notes were taken instead. The transcribed interviews were then imported into QSR International's NVivo 12, a qualitative analysis software package that facilitates the exploration, coding, and visualization of large quantities of unstructured data. The coding process was designed to pay particular attention to the tensions and challenges associated with cyber-resilience practices and the strategies respondents deployed to negotiate these hurdles.

All interviews followed a similar script: respondents were first asked to explain how they defined cyber-resilience and then to recall the most severe cyber-attack they had experienced. These questions were asked at the beginning of the interview to elicit specific and concrete recollections of disruptive adverse events unique to the participant's organization and how these events were managed. An indirect objective was to minimize participant reliance on generic statements or highly publicized cases, responses that are often used to deflect questions about a sensitive topic or one for which the organization has no response. The interview script then proceeded with questions about the technologies and procedures (including standards) used to foster cyber-resilience, the role played by public-private partnerships and external expertise, the organizational barriers to cyber-resilience, the impact of the human factor on cyber-resilience, and the regulatory aspects of cyber-resilience. A final open-ended question allowed respondents to identify any issues they thought had been overlooked.

While this study used interviews as its primary research material, we were also able to take notes and ask candid questions at a meeting in the summer of 2019, where the outcome of a large international cyber-resilience exercise was reported to a dozen representatives from large multinational financial institutions and national regulators. Finally, under strict confidentiality agreements, three organizations shared with us two complete cyber incident response plans, a series of ten post-incident reports, and a benchmarking report comparing the cyber crisis management models of ten multinational businesses from various sectors (including finance and insurance). These documents provided useful contextual information for the study.

5. The four foundational tensions of cyber-resilience

In this section, we expose the various ambiguities and uncertainties that inhibit the sensemaking processes of cybersecurity professionals and frame their ability to become resilient to stresses and shocks. Four major sources of sensemaking tension emerged from the interviews: a definitional tension that makes cyber-resilience still an elusive organizational objective, an environmental tension deriving from the manufactured and dynamic nature of cyber-risks, an internal tension arising from a collision with competing organizational rationalities, and a regulatory tension reflecting the disparity of national regulatory regimes for organizations whose activities span multiple jurisdictions.

5.1 A polysemic concept

While academics, consultants, standard-setting bodies, and regulators offer seemingly straightforward definitions of what cyber-resilience is (or ought to be), respondents expressed a lot more uncertainty and reflexivity about the meaning they assigned to the term. This is possibly the original sensemaking tension about a concept that can mean many things to many people and therefore be perceived as devoid of practical use. While this problem has been recorded in many other contexts where resilience is advocated (Davidson et al., 2016), one interviewee highlighted the direct negative impact it had on his ability to manage risk:

> We use different terms, people define cyber themselves, they'll define resilience themselves, and so when you put cyber resilience together, everyone you talk to is probably got a slightly different view of what that is… that's quite common, that we don't have common terms, a common lexicon, common relationships defined for us to understand, I heard someone say one time that if the people who engineered aeroplanes didn't have a common definition of velocity or mass, do you think it would ever get off the ground? Do you think anybody would get in one? No, but we manage operational risk that way, as an industry. (Canada 23)

This confusion is heightened by the hype surrounding cybersecurity, a market with such attractive growth prospects that vendors do not hesitate to use the most outrageous marketing language and the trendiest buzzwords to pitch their products and services. As a result, references to cyber-resilience proliferate in the marketing literature. These performative uses of cyber-resilience then find their way to the desks of directors and senior management, "making it very easy to get distracted," in the words of a respondent (Canada 25).

The sensemaking tensions generated by diverse meanings of cyber-resilience manifest themselves across multiple dimensions. The first one is the relationship to risk: while for some, cyber-resilience still implies a 'fortress mentality' where robustness to adverse events is the ultimate goal, for others, it implies a new acceptance of unknowable risks and the need for organizations to learn to live with them through agility. Attempts to blend those two approaches were mentioned, but their underlying rationales seemed incompatible to one of our respondents:

> These two properties are not compatible with each other. Robust means you cannot flex it, and agile means you can. How can you make something flexible and not flexible at the same time? You can't. Same with resilience. (UK 2)

The second dimension covers the functions explicitly associated with the cyber-resilience definition. Some respondents equated cyber-resilience with a comprehensive set of risk management functions, such as the design of safe-to-fail IT architectures, the prevention of attacks and the development of improved detection and response capacities. Others had a more restrictive approach that was limited to recovery capacities. The focused meaning of cyber-resilience reflects the heritage of established risk management practices such as disaster recovery (DR) and business continuity planning (BCP) and refers to a reassuring body of expertise. In contrast, the expansive meaning adopts a more integrative mindset that requires new coordination mechanisms between interdependent functions:

> We began talking about resilience when […] people began to realize that the various aspects of information risk are related to one another, that we are part of an ecosystem and focusing on just detection doesn't work, focusing on just protection doesn't work, and focusing on just response or recovery doesn't work, you have to have a capability across the spectrum and that capability, in total, […] gives us an ability to understand our ability to persist through damaging events, and that persistence capability is a measure of our overall resilience, it's a measure of our capability across that spectrum of you know, prevention, detection and response and recovery. (Canada 23)

The third dimension of relevance is the degree to which the meaning of cyber-resilience should be limited to technical considerations (resilience engineering) or should also incorporate social aspects. While many respondents initially framed their responses using technical terminology to define their understanding of cyber-resilience (password strength, use of encryption, extensiveness of backups, etc.), the most experienced in handling cyber-attacks emphasized the growing need to broaden this definition to include "the people side of it" (Canada 26). This has practical implications because it implies a more sustained dialogue with experts outside of the cybersecurity realm.

However, being able to define cyber-resilience and differentiate it from conventional cybersecurity approaches confidently was insufficient to resolve all sources of tension. The professionals we interviewed were also challenged by the turbulences that characterize the cyber-risk landscape in which their organization operates, which was another source of disruption to their sensemaking processes.

5.2 A turbulent cyber-risk landscape

A second sensemaking challenge cybersecurity professionals encountered in their attempts to design and implement cyber-resilience practices was the complexity of cyber-risks and the difficulty of making sense of them and understanding what was happening in a dynamic environment. With well-known risks such as natural disasters, established framings that make sense of events and identify response pathways can be quickly and easily deployed. With cyber-risks, where ‘newness’ abounds, frames need to be developed “on the fly” in a context of high uncertainty. Sensemaking processes are more challenging to implement because of the dynamic nature of cyber-risks, which are ‘manufactured’ by adversaries and for which there is often “very little previous experience” (Giddens, 1999: 4). Adversaries constantly innovate, developing attack strategies and tools that have never been encountered before and for which there are no known defences (Bilge and Dumitras, 2012; Ablon and Bogart, 2017). These so-called zero-day attacks introduce high levels of uncertainty that information-sharing arrangements between financial institutions, a form of distributed sensemaking, cannot alleviate.

> That approach only works against things that have already happened to others; the new things that are coming along, the zero-day threats, the brand-new virus that no one has seen yet, those are the things you have to watch for, that information sharing will never address because you have nothing to share because it hasn’t happened yet, and every day there are new things being invented. (Canada 22)

The same respondent added that these sudden and destabilizing shifts emerge from an ocean of noisy data. His organization, for example, had to deal with a trillion security alerts over the previous year, and the only way to handle such large numbers of events was to delegate sensemaking processes to artificial intelligence (AI) (Canada 22). Although AI is exceptionally effective at detecting unusual patterns in digital haystacks of data, it performs best after being trained extensively with accurately labelled data, which is resource-intensive and time-consuming. In other words, AI is best suited when operating in stable and familiar environments and becomes very fragile when confronted with constantly adapting thinking adversaries (Heaven, 2019).

The dynamic nature of cyber-risks can destabilize sensemaking processes at different stages of an adverse event. Respondents recalled many cases where what had initially been identified as a relatively minor incident quickly escalated into a much more complex crisis that unfolded over many months. In one example, infection of an employee’s laptop by malicious software, which would usually have been dealt with remotely in a few hours, led to the activation of a crisis team when forensic analysis indicated that troves of emails had been compromised. This particular employee was the point of contact with multiple industry regulators and organized the travel of the organization’s high-level management, so he had access to personal information such as passports, credit card numbers, etc. During a crisis, discoveries such as this can, and do, provoke sudden bifurcations in the sensemaking process, which in turn can increase the probability of errors. Mindful of this pattern, one organization in our study had introduced an informal deferred decision-making approach to enable more thorough sensemaking assessments of a situation and avoid implementing hasty measures that could prove counterproductive. Even when an incident has been resolved technically, its negative impact (such as the malicious use of stolen credentials or personal information) can linger for many months and require further sensemaking in a demanding and hostile environment.

Cyber-risks are often difficult to contain, generating risk cascades (van Eeten et al., 2011) that increase the dynamic properties of cyber-risks and amplify a crisis. The move to cloud infrastructures provided by third parties exemplifies this challenge. The concentration of the cloud industry around three dominant providers (Amazon, Google, and Microsoft), which are not regulated by the same organizations as their financial customers (except in the UK, where the financial regulator was granted new oversight powers over cloud services in June 2022), introduces new forms of uncertainty in case of failure. US insurers (AIR, 2018) and legislators (Schroeder, 2019) have expressed concern, and almost a quarter of participants mentioned that this shift to the cloud complicated their risk-management practices and even "made them blind" (Canada 16).

Another significant source of interference with the sensemaking process is the obfuscation of cyber-risks. The secrecy that frequently envelops the management of some incidents, the existence of 'Shadow IT' systems that are sometimes hidden from cybersecurity professionals (Hagenaars, 2019), and the loss of the expertise required to secure adequately multiple stacks of ageing legacy systems all contribute to this obfuscation.

> If you have this big sprawling mixture of technology and legacy architecture and infrastructures that you've acquired over twenty-five to fifty years, depending on how long you've been in business, it can be really hard to wrap that in something that looks resilient, because it's a leaky boat. (Canada 18)

These distinctive cyber-risk features can degrade sensemaking quality by making the severity of incidents harder to assess, their ramifications for the organization and its external partners harder to understand, and the level of response required harder to calibrate. These sensemaking blind spots are directly reflected in the quality of the response plans and 'playbooks,' which function as broad sensemaking tools that the financial industry has developed to manage adverse events.

5.3 Contested organizational rationalities

Not all sensemaking challenges can be attributed to the external pressures of a fast-changing risk landscape. The third source of sensemaking tension originated from the contested rationalities (or sensemaking frames) of business operational requirements and cyber-resilience. With digital technologies transforming financial institutions, the importance of using these new tools to optimize resources and maximize profits collides with a more cautious cyber-resilience approach in which innovation is delayed until proven safe. It also requires acknowledging that significant redundancy, diversity, and training investments are necessary, even if they may not show immediate benefits. The decision to deploy diversified and redundant technologies often involves a contest of rationalities:

> As a general rule, 'simple' is easy to interact with, but 'simple' is also potentially not as resilient as 'diverse' and 'complex,' but 'diverse' and 'complex' are more difficult to interact with, and so the questions become what your business goals are, what are the risks you face, and whether or not those pros and cons make sense in your business. (Canada 23)

To resolve this tension, cybersecurity professionals implementing cyber-resilience practices inside their organization place a strong emphasis on communication. They are mindful of their users' business needs, incorporate them into their risk management mandate, and are careful about communicating this mandate. Sometimes they even borrow sensemaking patterns from their business users to engage them more effectively in their cyber-resilience efforts.

> When you're a bank, you're making credit decisions all the time and there is a well-established model for measuring risk, how much risk are we accepting from a risk appetite. We're trying to bring those practices that have evolved in banks from a credit risk perspective to cyber-risk and operational risk and so that's where we're going in terms of trying to calculate our risk on what we're doing with our systems. (Canada 22)

The pre-eminence of a business rationality temporarily cedes ground to a cyber-resilience rationality when a major crisis erupts. As many participants noted, nothing focuses the mind of CEOs and board members and increases their interest in cyber-resilience like a highly publicized data breach or cyberattack. They recalled how an occurrence of these disruptive events in their organization or in competing financial institutions sparked a review of existing arrangements and unlocked significant investments that they had been unable to secure previously.

> My CEOO, so that's Chief Executive Operating Officer, he is actually responsible for the entire IT domain and operations, he says: it has become clear to me I can be fined for not being compliant, that can be a very high fine. And we have had that with [name of international financial scandal]. He said: I survive that, that hurts a lot, that is really something that hurts you, well, but you survive that. He says: but now I realize that we can have a cyberattack that you don't survive, that just actually wipes you off the map. (Netherlands 4)

5.4 Regulatory disparities

Finally, the fourth source of sensemaking tensions originated from interactions with regulators, whose oversight activities and cyber-resilience requirements varied greatly across geographic boundaries. Many respondents worked in financial institutions with branches in many countries (sometimes more than fifty) that operate under a broad range of regulatory regimes. Some countries have adopted a principles-based approach to the regulation of cyber-risks, while others, such as the UK or the Netherlands, have been more prescriptive and have developed proactive testing strategies (CBEST in the UK and TIBER in the Netherlands) in which external 'red teams' mimic the types of attacks carried out by sophisticated actors (Hielkema and Kleijmeer, 2019). Financial institutions must incorporate and consolidate these variations into their sensemaking processes to ensure they are compliant across the whole regulatory spectrum, introducing additional complexity. The time available for sensemaking can also be decreased by some regulators' requirement that the nature and scale of cyberattacks or data breaches be rapidly disclosed to the public, even though the dynamic nature of cyber-risks and the technical complexity of digital infrastructures mean that assessment of an incident's full impact may go through multiple iterations that alter how the crisis is understood. By forcing financial institutions to make their sensemaking processes transparent within a shorter timeframe, this regulatory strategy can lead to unexpected and detrimental outcomes.

> You know how in a lot of incidents that have gone public in the last number of years, you'll get someone from the communications department speaking, saying within two or three days of an incident being announced that they've got it contained. Well, the truth is, ninety percent of the time they have to come back in a few days or a week later and say "look, you know how we thought we had forty-thousand customer data records breached, oh shit, it's four-hundred-thousand." … Because the fog of war means that half the time, you're wrong, but don't go out and say to your regulator or the public or your constituency that you've got it fixed, right? If you do that more than a couple of times, your trust and brand get destroyed. (Canada 20)

The four sensemaking tensions outlined in this section (polysemic meaning, turbulent risk landscape, contested organizational rationalities and disparate regulatory requirements) reverberate across the plethora of decision-making processes activated by financial institutions' exposure to cyber-risks. They significantly complicate the job of cybersecurity professionals, who are usually selected for their technical expertise or business acumen but may be less comfortable dealing with unpredictability, uncertainty, ambiguity, and controversy. One respondent summed this up bluntly when he stated that these tensions provide fertile ground for "narrative fallacies that justify things that are not necessary" and allow "charlatans [to] proliferate to profit" (United Kingdom 2). In the next section, we explore how these sensemaking tensions are embedded in strategies and practices adopted in the name of cyber-resilience.

6. How sensemaking tensions reverberate through cyber-resilience practices

A famous quote by General Dwight D. Eisenhower (1958: 818) states that "plans are worthless, but planning is everything," highlighting the value of planning as a preparedness activity over the plans themselves. That general approach guided many participants, who often used the "muscle memory" analogy to convey the principles that informed their cyber-resilience practices. Mindful of the intrinsically unpredictable nature of cyber crises, they emphasized the development of general resources and practices that could be quickly adjusted to deal with unexpected events and would feel comfortable in doing so. At the core of this approach was the conviction that the human factor was a primary source of cyber-resilience. The most experienced respondents—most of them with a technical background—often reminded us that people trump systems and procedures in dealing with a severe cyberattack.

> People will save businesses in a time of crisis. If you train people, if you retain them, if you treat them well, you accumulate knowledge. And that knowledge in a time of crisis will be crucial. We did have several quite severe incidents. And again, it was people who were at the front end, at the edge, saving the business. Not technology. Technology was useless. (United Kingdom 2)

6.1 Preparing to improvise

Multiple strategies were advocated by respondents to better equip organizations with the resources to implement cyber-resilience practices that are compatible with ambiguities and tensions in the sensemaking process. The hiring of incident-response practitioners who displayed personal traits such as higher-than-average curiosity, creativity, and flexibility was frequently mentioned. This gave cybersecurity teams the ability to identify hidden patterns in large amounts of information, deviate from established procedures (or playbooks) when novel situations emerged, and quickly improvise previously unconsidered solutions. Without being reckless, these practitioners are comfortable with imperfect decision-making environments and are not prone to the "startle effect" that can lead to delay, panic, and even paralysis (Staal, 2004). They need to be good communicators who know how to translate technical approaches so they can be understood by all in the organization and can explain the reasons behind inconvenient or drastic measures, especially when they have never been taken before. They are also good listeners who can integrate multiple—and sometimes contradictory—perspectives into their own decisions. These results corroborate the findings of Chen et al. (2014), who conducted individual and team task analyses with three computer security incident response teams.

Beyond individual features, participants noted that diversity was becoming more valued in teams that manage cyber-crises (Canada 27, United Kingdom 2). Some organizations had built or were building multidisciplinary teams that drew on a wide array of backgrounds, perspectives, and expertise to ensure that their decisions did not overlook weak signals or discard unorthodox approaches because of groupthink (Janis, 1972). To a certain extent, the contours of effective cyber-resilience professionals drawn by our respondents have a lot in common with jazz musicians who create musical pieces from minimal structures in turbulent task environments where they must balance their individual skills and group coordination (Bastien and Hostager, 1988). They constantly update their sensemaking to incorporate their reading of the room and its atmosphere, the decisions made by other musicians in their ensemble and the ensemble leader, their knowledge of the main jazz forms and conventions, as well as their own inspiration to collectively improvise unique performances that feel very polished. This approach rests on a fluid practice of sensemaking that can accommodate errors and internal controversies (providing they remain constructive), in contrast with philharmonic orchestras, whose performance is dictated by strict adherence to the musical score of a composer (Kamoche and Pina e Cunha, 2001).

Respondents highlighted the importance of good communication as a cyber-resilience tool. Practically, effective communication is achieved through dense internal and external organizational networks that improve the speed and effectiveness of communication flows. Despite the natural tendency in many financial institutions to segment expertise and require secrecy when crises unfold—which hinders sensemaking, many respondents highlighted the benefits of having developed bridging capital and weak ties throughout the organization to deal with adverse events (Granovetter, 1973). For some, this meant embedding security workers inside business units to better understand their culture and technological constraints, but also attempting to "build fundamental security into the business processes" (Canada 18). Other participants establish 'fusion centres' of various security units (fraud, cyber, physical, business continuity) to consolidate sensemaking and decision-making capacities. Awareness campaigns and cybersecurity ‘ambassador programs’ can also create internal networks that can be activated in times of crisis. In another industry, Netflix has gone even further and launched a Reservist Program in which auxiliary crisis managers are trained across the organization to distribute and scale sensemaking and response expertise (Joshi, 2020).

External networks play a growing role in expanding the sensemaking capacities of an organization in support of cyber-resilience. Financial institutions are embedded in a dense web of business partnerships. Their sensemaking and incident response processes rely on the ability to quickly collect information from outside the organization and access ‘surge capacities’ while limiting bureaucratic or contractual frictions. Third parties, especially those providing IT services, need particular attention. Prompted by regulatory requirements, financial institutions are dedicating resources to assess the cyber-resilience of third parties and monitor how this impacts their own posture. A Dutch respondent provided such an example, where a company providing DDoS protection services to multiple key players became a concern for the local regulator

> So companies started to use certain professional service providers such as XYZ. They are good, the best, so Bank 1 wants to do business with XYZ, Bank 2 wants to do business with XYZ, Bank 3 wants to do business with XYZ. Hey, we have a concentration risk. So in the financial market XYZ is, well, becoming a critical point. (Netherlands 6)

However, as some respondents noted, these sensemaking processes can expand exponentially to unsustainable levels: third parties have their own third parties, not consistently recognized before an incident, and modelling these risk cascades across organizations can quickly become highly complex and unrealistic.

The primary function of external networks remains the sharing of intelligence, best practices, and best thinking. One participant used the medical analogy of inoculation to describe the utility of sharing information across financial institutions, while acknowledging that this approach offered protection only against known threats. Many respondents extolled information sharing as one of the most effective strategies to stop the contagion effect that can destabilize the financial system once attackers have found an industry-wide vulnerability.

> Networks of people who talk about what they’re experiencing, I think is very valuable, and in fact it’s sometimes more valuable than the consultants who come in and tell you stuff because—and I say this having been, given my prior history, essentially a consultant for a long period of time, the people who are out at the sharp end, sharing stories, are typically very open in the right setting and you learn more from that than you would do through a six-week consulting engagement and you’ll learn it faster. (Canada 25)

The external networks that share information effectively blend informal and formal structures that can extend from small peer groups to large industry consortiums. One respondent estimated that the not-for-profit information-sharing initiatives in which his bank participated gave him access to threat indicators three and a half weeks earlier than the notifications he received from commercial feeds (Canada 31), a considerable sensemaking asset. To fully benefit from these external resources, trust built over time through personal relationships is needed so that people have accumulated enough social capital to "call and ask for favours when they need to" (Canada 19).

6.2 Response capacities that can deviate from playbooks

Response playbooks are one of the main tools used by cybersecurity professionals to activate sensemaking processes during cyber-attacks. A playbook can be defined as "a linear style checklist of required steps and actions required to successfully respond to specific incident types and threats" (van der Kleij et al., 2022). Playbooks enable incident response teams to routinely and systematically apply formal procedures when faced with predictable adverse events so that they can focus their cognitive resources on strategic decisions. The playbook design process generally starts with a comprehensive mapping of the critical functions a financial institution must recover in case of an extreme adverse event and its regulatory requirements during such events. These mapping exercises are not new but, in the past, were more likely to focus on individual risks. This focus is changing in an environment where the complete loss of IT resources is a possibility (such as the one that affected 25% of Canada's internet users on July 8, 2022), and where different teams must be ready to coordinate their efforts quickly to restore access to markets and resume services to customers. Mapping is not limited to internal processes but must also extend to third parties, complicating matters when the latter are reluctant to share sensitive information (United States 1). The outcomes of these mappings are then combined with intelligence about the threat landscape to design scenarios of possible adverse events and create predefined response procedures.

The financial institution for which one of our participants worked maintained sixteen playbooks reviewed every quarter to assess whether new scenarios based on emerging modes of attacks were needed (Canada 22). Playbooks take time to develop because of the diversity of rationalities and resources they must incorporate into a single document. One participant explained that the creation of a playbook had involved several rounds of consultation and testing over almost a year to ensure that it captured the different perspectives, capacities, and methodologies of all the teams it was supposed to coordinate (Canada 4). Several respondents warned against an over-reliance on playbooks, which cannot possibly anticipate all the surprises encountered in real-life incidents or resolve all the sensemaking tensions described above. They highlighted that a cyber-resilient organization needs to be prepared to deviate from a playbook—sometimes radically—to adapt its response to unexpected conditions (Canada 1, Canada 32). This warning reflected the wariness of experienced practitioners who felt that playbooks could provide a false sense of security in extreme circumstances and paralyze the sensemaking process to exclude unusual but effective decisions.

6.3 Adaptation and the safe adoption of new sensemaking frameworks

The reports produced by the cybersecurity industry often describe cyber-resilience as a set of activities and processes undertaken to respond immediately to an incident (Dupont, 2019). However, the ultimate goal of resilience is not merely survival until the next crisis but adaptation to reach a new state of equilibrium. In that context, respondents reflected on what fostered or hindered the catalysis of new sensemaking frameworks.

The first form of adaptation is voluntary and reflects the learning that takes place after a significant unexpected incident or after a poorly handled routine incident. Highly publicized incidents such as the wave of Distributed Denial of Service Attacks against American banks in 2012, the Equifax breach in 2017, the Capital One hack in 2019, or the SolarWinds and Microsoft Exchange supply chain attacks in 2020 and 2021 sent shockwaves through the financial industry, highlighting the fragility of existing assumptions and leading to significant changes (Canada 5, Canada 16, Canada 17, United Kingdom 1, United States 2). Many more minor incidents that are never brought to the attention of the press and simulations that enact future-oriented scenarios also reveal the inadequacy of existing security measures and response procedures. The lessons learned during these events by those involved in their mitigation are usually captured in post-incident reviews.

The review documents we were granted access to summarized the causes of the incident, its impacts on the organization and its customers, how it was resolved, what lessons were learned, and what adaptations were required as a result. But it was difficult to assess how these insights had been incorporated into the organization's cyber-resilience practices. Echoing this impression, a respondent regretted that there was no technology available to tap into the accumulated organizational memory that these reports contained, including a track record of the good and bad decisions that had been made and their outcomes (Canada 3). To ensure that all the data needed to update established sensemaking frames are collected, especially the most sensitive and embarrassing, a few respondents insisted on the need to create a safe environment for the employees at the origin of an incident. This "no-fault learning" approach was reiterated publicly in one of the incidents described above.

> [name withheld], who is the Senior VP, even recorded a video to say that it is ok to make mistakes. We can make mistakes. What's not right is to keep making the same mistakes over and over again without correcting yourself, without thinking: Yes, I made a mistake, but what can I do to avoid it? And also, to realize, if I made a mistake in one system, in one way, can that mistake be reproduced elsewhere? So learn from our mistakes. (Canada 2)

Industry standards also perform an adaptive function. Sometimes defined as a "recipe for reality," standards have become ubiquitous in a complex world where technical and organizational infrastructures must be coordinated globally. They facilitate interactions between businesses by making explicit "the rules that others follow" (Busch, 2011: 28). Standards gradually incorporate lessons learned from past incidents and then help propagate best practices, raising the bar for everyone. But some respondents expressed doubts about the false sense of resilience that standards might introduce. Because of their complexity (often involving hundreds of criteria or controls), it is almost impossible for an organization to be fully compliant (Canada 19), and extremely difficult to embed standards into easily-communicable sensemaking frames. Standards are also very rigid by necessity and may therefore not be ideally suited to help deal with the unknown (Canada 3).

The third form of adaptation stems from the regulatory activity to which financial institutions are subjected. Respondents identified "a trend towards more regulation and more specific regulation" (Canada 23), with certain jurisdictions becoming much more directive about cyber-resilience. Although most participants preferred principle-based regulatory requirements out of concern that an excessively detailed and prescriptive approach would erode their flexibility, others explained how detailed regulations that mandated specific measures could accelerate collective adaptation. Even when financial institutions understand the value of technologies or processes that can enhance cyber-resilience, the costs associated with their deployment and the fear of being the only one to adopt them and losing customers to competitors that support customer experience rather than resilience act as powerful deterrents. Prescriptive regulations that force the whole industry to adopt the same sensemaking framework simultaneously can overcome this competitive barrier and lead to support for investments that would have been much more difficult to justify otherwise. Unsurprisingly, this more intrusive regulatory approach remains a sensitive issue. The importance of avoiding 'sensemaking capture' by lobbyists and vendors that try to embed their products into norms is a concern (France 1), as is the tendency for certain regulators to provide vague guidance that leads to interpretative uncertainty and accentuate sensemaking tensions instead of appeasing them (United States 1, Canada 28).

7. Conclusion

This article provides a detailed overview of the current sensemaking tensions that cyber-resilience practices generate for the cybersecurity professionals that implement them. Although we initially expected to identify different ways in which cyber-resilience sensemaking took place across countries, the limited size of our sample did not make this comparison possible. However, it became clear that even within the same jurisdiction or market (Canada, for example), it was impossible to identify a standardized sensemaking template around cyber-resilience. Cyber-resilience appears to be highly contextual, and the sensemaking processes surrounding it depend on various unique factors, such as the history, size, business culture, international footprint, IT priorities, regulatory environment, and leadership style of each organization.

By sharing some of their insights, cybersecurity professionals working in one of the sectors most exposed to cyber-risks have outlined the tensions inherent to implementing cyber-resilience practices, which are all too often shrouded in trendy buzzwords and shallow normative agendas. Our particular focus has been to describe in concrete terms how cyber-resilience is embedded in a complex web of interactions that link technical systems, organizational processes, and human behaviors and is constrained by tensions in framing processes that lead to the prioritization of particular choices by making some actions thinkable and others inconceivable (Smith, 1987; Simpson et al., 2019).

The web of interactions involved and the tensions inherent in it, along with the particular context of competing adversaries, help explain why cyber-resilience cannot be reduced to dealing with business continuity and disaster management. Conventional response models are designed to handle predictable and stable risks such as natural disasters, whereas cyber-risks are the result of actions by innovative and thinking adversaries who leverage their own sensemaking toolsets to identify vulnerabilities and weaknesses to exploit. Our research also illuminated the tensions that result from the contested rationalities of business performance and institutional security. Holling discussed this quintessential dilemma in his foundational work on ecological resilience, where he cautioned that conditions favourable to short-term economic productivity (such as reduced diversity and redundancy, which allow economies of scale and resource optimization) might be detrimental to resilience and ultimately increase vulnerability (Holling, 1996: 38).

A possible source of framing and sensemaking tension that we did not explore in our interviews arises from a set of individual and collective cognitive biases that can interfere with cyber-resilience. Heuristics that seem particularly relevant in this context include the myopia bias (the tendency to focus on present benefits rather than future harms), the amnesia bias (the tendency to quickly forget the lessons of past disasters), the optimism bias (the tendency to minimize the impact an adverse event can have on us even while acknowledging it will affect others), the inertia bias (the tendency to remain passive when confronted with high levels of uncertainty), the simplification bias (the tendency to consider only convenient factors when faced with complex risks), the herding bias (the tendency to align with the actions of others rather than rely on a more specific analysis of the situation), the familiarity bias (the tendency to rely on past actions as guides for behaviour), the consistency bias (the tendency to maintain an approach once an initial decision is made), the expert halo bias (the tendency to assess leaders' skills based on an overall positive impression rather than specific information), and the social facilitation bias (the tendency to take more risks when other people are involved) (McCammon, 2004; Meyer and Kunreuther, 2017). Future research on cyber-resilience should therefore investigate how significant these biases are in the sensemaking processes of cybersecurity professionals and what mitigating remedies may be available.

References

Ablon, L., & Bogart A. (2017). *Zero days, thousands of nights: The life and times of zero-day vulnerabilities and their exploits.* RAND Corporation. doi:10.7249/RR1751

AIR. (2018). *Cloud down: Impacts on the US economy*. Lloyd's.

Alexander, D. E. (2013). Resilience and disaster risk reduction: An etymological journey. *Natural Hazards and Earth System Sciences*, *13*(11), 2707-2713. doi: 10.5194/nhess-13-2707-2013

Ancona, D. (2012). Sensemaking: Framing and acting in the unknown, in Snook, S., Nohria, N., and Khurana, R. (eds.), *The handbook for teaching leadership: Knowing, doing and being*, SAGE, Los Angeles, pp. 3-19.

Ansell, C., Boin, A., & Keller, A. (2010). Managing transboundary crises: Identifying the building blocks of an effective response system. *Journal of Contingencies and Crisis Management*, *18*(4), 195-207. doi:10.1111/j.1468-5973.2010.00620.x

Bastien, D. T., & Hostager, T. J. (1988). Jazz as a process of organizational innovation. *Communication Research*, *15*(5), 582-602. doi: 10.1177/009365088015005005

BCBS (2018). *Cyber-resilience: Range of practices*. Bank for International Settlements.

Bilge, L., & Dumitras, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. In *CCS '12: Proceedings of the 2012 ACM conference on Computer and communications security*, 833-844. doi:10.1145/2382196.2382284

Björk, F., Henkel, M, Stirna, J., and Zdravkovic, J. (2015), "Cyber resilience – Fundamentals for a definition", in Rocha, A., Correia, A. M., Costanzo, S., and Reis, L. P. (eds.), *New contributions in information systems and technologies*, Springer, London, pp. 311-316. doi: 10.1007/978-3-319-16486-1_31

Bodeau, D., & Graubart, R. (2011). *Cyber resiliency engineering framework*. The MITRE Corporation.

Busch, L. (2011). *Standards: Recipes for reality*. The MIT Press.

Caralli, R., Allen, J., White, D., Young, L., Mehravari, N., & Curtis, P. (2016). *CERT Resilience Management Model, Version 1.2*. Carnegie Mellon University.

Carnegie Endowment for International Peace (2021), *Timeline of cyber incidents involving financial institutions*, retrieved from https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide.

Chen, T. R., Shore, D. B., Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., & Gorab, A. K. (2014). An organizational psychology perspective to examining computer security incident response teams. *IEEE Security & Privacy*, *12*(5), 61-67. doi: 10.1109/MSP.2014.85

CPMI-IOSCO (2016). *Guidance on cyber resilience for financial market infrastructures*. Bank for International Settlements.

Davidson, J. L., Jacobson, C., Lyth, A., Dedekorkut-Howes, A., Baldwin, C. L., Ellison, J. C., Holbrook, N. J., Howes, M. J., Serrao-Neumann, S., Singh-Peterson, L., & Smith, T. (2016). Interrogating resilience: Toward a typology to improve its operationalization. *Ecology and Society*, *21*(2), 1-15. doi:10.5751/ES-08450-210227.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(2), 92-100. doi:10.4236/jis.2013.42011

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity*, *5*(1), 1-17. doi:10.1093/cybsec/tyz013

ECB (2018). *Cyber resilience oversight expectations for financial market infrastructures*. European Central Bank.

Eisenhower, D. E. (1958), Remarks at the National Defense Executive Reserve Conference – November 14, 1957, in *1957: containing the public messages, speeches, and statements of the president, January 1 to December 31, 1957*, Office of the Federal Register, National Archives and Records Service, Washington DC, pp. 817-820.

ENISA (2011). *Resilience metrics and measurements: Technical report.* ENISA.

Flanagan, J. C. (1954). The critical incident technique. *Psychological Bulletin*, *51*(4), 327-358.

Frost & Sullivan (2017). *The 2017 global information security workforce study: Women in cybersecurity*. Frost & Sullivan.

Fujs, D., Mihelic, A., & Vhrovec, S. (2019, August 26–29). The power of interpretation: Qualitative methods in cybersecurity research. In *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019)*, Canterbury. doi:10.1145/3339252.3341479

Giddens, A. (1999). Risk and responsibility. *The Modern Law Review*, *62*(1), 1-10. doi:10.1111/1468-2230.00188

Granovetter, M. (1973). The strength of weak ties. *The American Journal of Sociology*, *78*(6), 1360-1380.

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Anchor Books.

Hagenaars, K. J. C. (2019). *An empirical study into how cyber security professionals deal with uncertainty in information security risks assessments*. Management of Technology, Technische Universiteit Delft.

Heaven, D. (2019). Why deep-learning Ais are so easy to fool. *Nature*, *574*, 163-166.

Hielkema, P., & Kleijmeer, R. (2019). *Lessons learned and evolving practices of the TIBER framework for resilience testing in the Netherlands.* Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/files/WP_Hielkema_Kleijmeer_TIBER1.pdf.

Holling, C. S. (1996). Engineering resilience versus ecological resilience. In P. Schulze (Ed.), *Engineering within ecological constraints* (pp. 31-44).

Janis, I. L. (1972). *Victims of groupthink: A psychological study of foreign-policy decisions and fiascoes.* Houghton Mifflin.

Joshi, S. (2020, January 29). Reservist model: Distributed approach to scaling incident response. *Enigma Conference*. Retrieved from https://www.usenix.org/conference/enigma2020/presentation/joshi.

Kamoche, K., & Pina e Cunha, M. (2001). Minimal structures : From jazz improvisation to product innovation. *Organization Studies*, *22*(5), 733-764. doi: 10.1177/0170840601225001

Keys, B., & Shapiro, S. (2019). Frameworks and best practices. In I. Linkov & A. Kott (Eds.), *Cyber resilience of systems and networks* (pp. 69-92). doi:10.1007/978-3-319-77492-3_4

Lakshmi, R., Naseer, H., Maynard, S., & Ahmad, A. (2021). Sensemaking in cybersecurity incident response: The interplay of organizations, technology, and individuals. *Twenty-Ninth European Conference on Information Systems*. Retrieved from https://arxiv.org/abs/2107.02941.

Linkov, I., Eisenberg, D., Plourde, K., Seager, T., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, *33*(4), 471-476. doi:10.1007/s10669-013-9485-y

Linkov, I., Trump, B., & Fox-Lent, C. (2016). Resilience: Approaches to risk analysis and governance. In M.-V. Florin & I. Linkov (Eds.), *IRGC resource guide on resilience* (pp. 3-14).

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In A. Kott & I. Linkov (Eds.), *Cyber resilience of systems and networks* (pp. 1-25).

Maitlis, S., & Sonensheim, S. (2010). Sensemaking in crisis and change: Inspiration and insights from Weick (1988). *Journal of Management Studies*, *47*(3), 551-580. doi: 10.1111/j.1467-6486.2010.00908.x.

Manyena, S. B. (2006). The concept of resilience revisited. *Disasters*, *30*(4), 433-450. doi:10.1111/j.0361-3666.2006.00331.x

Maurer, T., & Nelson, A. (2020). *International strategy to better protect the financial system against cyber threats*. Carnegie Endowment for International Peace.

McCammon, I. (2004). Heuristic traps in recreational avalanche accidents: Evidence and implications. *Avalanche News*, 68, 1-10.

Meyer, R., & Kunreuther, H. (2017). *The ostrich paradox: Why we underprepare for disasters*. Wharton Digital Press.

Paton, D., & Johnston, D. (2017). *Disaster resilience: An integrated approach*. Charles C. Thomas.

Patton, M. Q. (2015). Sampling, qualitative (purposeful). in G. Ritzer (Ed.), *The Blackwell encyclopedia of sociology*. John Wiley & Sons. doi:10.1002/9781405165518.wbeoss012.pub2

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach*. National Institute of Standards and Technology.

Shackelford, S., Proia, A., Martell, B., & Craig, A. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST Cybersecurity Framework on shaping reasonable national and international cybersecurity practices. *Texas International Law Journal*, *50*: 305-355.

Schroeder, P. (2019). U.S. House lawmakers ask regulators to scrutinize bank cloud providers. *Reuters*, 23 August. Retrieved from https://www.reuters.com/article/us-usa-congress-cloud/u-s-house-lawmakers-ask-regulators-to-scrutinize-bank-cloud-providers-idUSKCN1VD0Y4.

Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security*, *97*, 1-15. doi:10.1016/j.cose.2020.101996

Simpson, N., Shearing, C. D., & Dupont, B. (2019). Climate gating: A case study of emerging responses to Anthropocene risks. *Climate Risk Management*, *26*, 1-10. doi:10.1016/j.crm.2019.100196

Smith, D. E. (1987). *The everyday world as problematic: A feminist sociology*. Northeastern University Press.

Staal, M. (2004). *Stress, cognition and human performance: A literature review and conceptual framework*. NASA Ames Research Center. Retrieved from https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20060017835.pdf.

Steigenberger, N., & Lübcke, T. (2022). Space and sensemaking in high-reliability task contexts: Insights from a maritime mass rescue exercise. *Organization Studies*, *43*(5), 699-724. doi: 10.1177/01708406211035511.

Tapanainen, T. (2017). Sense-making in cyber security – Examining responder behaviors in cyber-attacks. *Twenty-third Americas Conference on Information Systems*. Retrieved from https://core.ac.uk/download/pdf/301372538.pdf.

Tiernan, A., Drennan, L., Nalau, J., Onyango, E., Morrissey, L., & Mackey, B. (2019). A review of themes in disaster resilience literature and international practice since 2012. *Policy Design and Practice, 2*(1), 53-74. doi: 10.1080/25741292.2018.1507240

van der Kleij, R., Schraagen, J. M., Cadet, B., & Young, H. (2022). Developing decision support for cybersecurity threat and incident managers. *Computers & Security*, *113*, 1-15. doi: 10.1016/j.cose.2021.102535.

Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, M., & Cruz, E. (2011). The state and the threat of cascading failures across critical infrastructures: The implications of empirical evidence from media incident reports. *Public Administration*, *89*(2), 381-400.

Weick, K. E. (1995). *Sensemaking in organizations*. SAGE Publications.

Weick, K. E., & Sutcliffe, K. M. (2015), *Managing the unexpected: Sustained performance in a complex world – Third edition*. John Wiley & Sons.