Computers & Security 132 (2023) 103372

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

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

ARTICLE INFO

Article history:
Received 4 February 2023
Revised 23 May 2023
Accepted 26 June 2023
Available online 29 June 2023

Keywords:
Cyber-resilience
Risk management
Cyber-risks
Sensemaking
Regulation
Standardization

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. 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 to uncover these tensions and how they reverberate across cyber-resilience practices.

© 2023 The Author(s). Published by Elsevier Ltd.
This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/)

1. Introduction

Over the past 25 years, cyber-risks have morphed from mere annoyances into potentially catastrophic events. 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 ballooning investments in cybersecurity technologies that reached USD 173.5 billion in 2022 and keep on growing (ResearchAndMarkets, 2022), 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. In their study on the costs of cybercrime, Anderson et al. (2019) estimate that these various online harms generate billions of dollars in financial losses annually for victims and society, including direct losses, indirect losses and defence costs. Although catastrophic scenarios remain hypothetical, recent research published by the International Monetary Fund found that aggregate losses generated by cyberattacks at 7,947 banks worldwide amounted to $97 billion yearly in 2018 (9% of net income), with value-at-risk (VaR) oscillating between $147 and $201 billion (14% to 19% of net income). The most pessimistic models returned annual losses of up to 51% under maximum adverse circumstances (Bouveret, 2018). To respond to the proliferation of cyber-risks and to overcome the limited effectiveness of existing cybersecurity approaches to mitigate inevitable attacks, regulators, standard-setting bodies, and cybersecurity consultants are increasingly 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

* Corresponding author.
E-mail address: benoit.dupont@umontreal.ca (B. Dupont).

https://doi.org/10.1016/j.cose.2023.103372
0167-4048/© 2023 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/)

(Linkov et al., 2013; Sepúlveda Estay et al., 2020). Google's NGram Viewer shows that the term 'cyber-resilience' appeared in the literature around 2010, accounting for 11.9 $\times$ 10^{-9}% of all the words used in the English language that year and that the number of occurrences increased sharply around 2015 with 428.4 $\times$ 10^{-9}%, reaching a high of 4074.9 $\times$ 10^{-9}% in 2019, the last year for which statistics are available.[1] Since then, interest has remained strong, as Google Scholar indicates that more than 6,500 scientific publications have analyzed this concept, 30.5% of them in 2022 alone.[2]

If cyber-resilience is to become the new cyber-risk management paradigm promoted by cybersecurity consultants, standards-setting organizations, regulators and researchers, a better understanding of the organizational and social practices that influence the adoption of this more holistic mindset is needed. Most of the scientific literature on cyber-resilience remains technical, theoretical or normative, and our contribution aims to provide a broader organizational and empirical understanding of cyber-resilience. We are particularly interested in sensemaking, understood as the subset of individual and social processes by which people and organizations frame the unknown and respond to it (Weick, 1995). In the field of cybersecurity, sensemaking plays a central and multifaceted role: it directly informs decisions made by organizations to optimize their investments in specialized technologies and human resources (Fedele and Roner, 2022), enables the emergence of a robust cybersecurity culture that promotes desirable values, attitudes and behaviours (da Veiga & Martins, 2017; Uchendu et al., 2021), supports the operational effectiveness of threat intelligence and incident response teams (Naseer et al., 2021; van der Kleij et al., 2022), and facilitates the learning processes required for adaptation to a constantly shifting threat landscape (Steinke et al., 2015). Hence, this article focuses on two dimensions of sensemaking: first, we want to examine how cybersecurity professionals make sense of cyber-resilience—a recently-introduced concept that could arguably be construed as one of the latest fads to afflict the field of cybersecurity—and how they articulate it with more established cybersecurity frameworks. A more applied line of enquiry complements this conceptual question: what types of sensemaking challenges do they experience when translating cyber-resilience principles into action?

This article uses qualitative data from a sample of 58 cybersecurity professionals. 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. We also introduce the notion of sensemaking and demonstrate why it plays a central role in cyber-resilience. We then describe our qualitative methodology and the sample of cybersecurity professionals we interviewed. The following two sections present and discuss 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 emphasize processes that foster persistence and often imply adaptation to new environmental extremes (Holling, 1996). In the field of systems engineering, of great relevance to cybersecurity, Woods' typology identifies four different meanings for resilience: rebound, robustness, graceful extensibility, and sustained adaptability (Woods, 2015). 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. For some authors, it implies that cyber-resilience differs from cybersecurity, which focuses on the capacity of an organization to predict, prevent and avert the occurrence of cyber-risks. They also claim that whereas cybersecurity focuses on information technologies, cyber-resilience reflects 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 invokes 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; Bellini et al., 2021).

To capture how cyber-resilience translates into practice, Connelly et al. (2017) suggest that four universal features need to be examined: the critical functions that should be preserved in priority, the thresholds above which adverse events exceed the organization's capacity to absorb them, the temporal implications of recovery activities, and the memory enabling or impeding adaptation. One of the major challenges associated with the study of cyber-resilience lies in its meaningful quantification, which must cover a large number of dimensions: domains of reference (technical, organizational, social, economic), the effectiveness of risk management processes, the various steps that make up the cyber-resilience cycle (prepare, prevent, protect, respond, recover, adapt), the organizational capabilities needed to deliver cyber-resilience, and the cognitive skills cyber-resilience professionals require to support cyber-resilience activities (Häring et al., 2016). Linkov and Kott (2019) outline two main families of cyber-resilience quantifications: metric-based approaches focusing on individual properties of systems and trying to assess how far they are from an ideal state of cyber-resilience, and a model-based approach seeking to evaluate the interdependent dynamics of complex systems, resorting for example to digital twins (Salvi et al., 2022). Economists have been more interested in measuring the costs of producing cyber-resilience, trying to identify the optimal equilibrium between investments and effectiveness and looking for low-cost but still effective practices (Rose and Miller, 2021).

Disaster management researchers, who study how large-scale adverse events are handled by organizations (Manyena, 2006; Paton and Johnston, 2017), have generated two insights relevant to cyber-resilience. First, as mentioned above, organizations with diverse maturity levels in this area can interpret resilience very differently. 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 com-

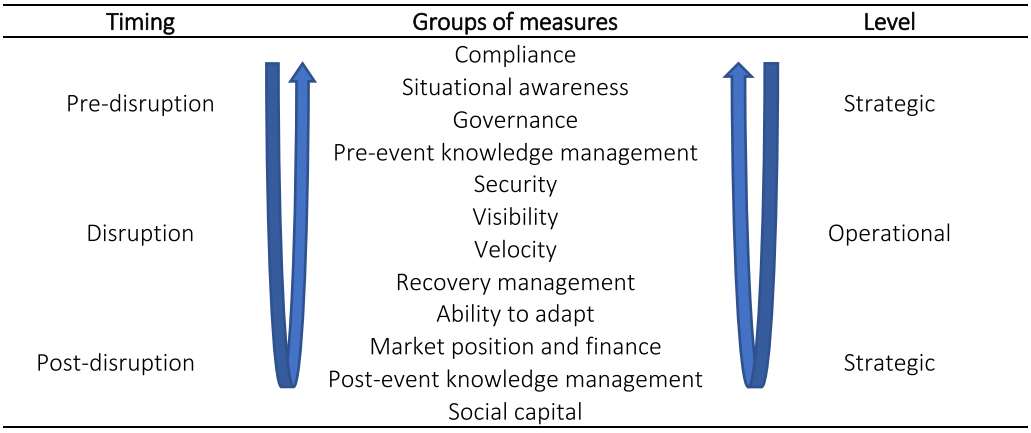

Fig. 1. Twelve categories of cyber-resilience measures (adapted from Sepúlveda Estay et al., 2020).

promise 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 or 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 into 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 Fig. 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).

These frameworks highlight that the scientific literature relevant to cyber-resilience is much broader than the papers making explicit use of the terminology and its afferent concepts. Cyber-resilience can be described as an umbrella term covering research areas that do not self-identify as cyber-resilience research but still produce empirical knowledge central to our understanding of how organizations prepare for, absorb, respond to, and recover from cyber-shocks (Grøtan et al., 2022). Research on incident response is a good illustration. A growing number of empirical studies have examined how "diverse teams of organizational stakeholders […] develop situation awareness, adapt to the rapidly evolving situation, raise the necessary resources, and respond to threats" (Ahmad et al., 2022). For example, Thangavelu et al. (2022) have shown that increasing the metacognitive awareness (the process of being aware of one's learning processes) and self-efficacy of incident responders could significantly improve their threat management performance. Combined with the development of evidence-based practical cognitive tools such as the critical-thinking memory aid proposed by van der Kleij et al. (2022), this line of work enhances the capacity of teams to deal with the unpredictability and uncertainty of cyberattacks and strengthens organizational security and resilience (Ahmad et al., 2020). Beyond incident response studies, other fields of research, such as cybersecurity training, awareness and compliance (Kirova and Baumoel, 2018; Hu et al., 2022), or information sharing (Skopik et al., 2016; Pala and Zhuang, 2019; Pomerleau and Lowery, 2020), to name a few, contribute to an emerging cyber-resilience body of knowledge. However, the insights generated by these discrete research areas remain fragmented, where cyber-resilience calls for an integrative approach that can blend the social and technical dimensions and strategic and operational considerations in frameworks that can formalize knowledge and practices while remaining flexible enough to thrive in uncertain environments.

3. Sensemaking and 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 and 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 and 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 and Sonensheim, 2010).

Cybersecurity researchers have used the sensemaking framework to understand how organizations and individuals perceive the techno-social risks they face and how they share information to update their decision-making models when new threats emerge (Tapanainen, 2017). Shreeve et al. (2022) have, for example, found that managers with limited cybersecurity knowledge can still use logic and conventional risk-management thinking to make sound cybersecurity decisions. Lakshmi et al. (2021) have examined how sensemaking activities unfold in specific settings, such as incident response, and developed a framework outlining the interplay of organizational, technological and individual factors. They extended the work done by van der Kleij et al. (2017), who identified the need for cybersecurity incident response teams to adopt collective sensemaking methods more broadly. Others, such as Dykstra and Orr (2016), have argued that existing sensemaking frameworks used in other fields such as public health and aviation should be transferred to cybersecurity to enhance decision-making. Sensemaking has also been leveraged in a more general context. Pawlowski and Jung (2015) have used sensemaking to study how IT users, such as students, perceive cybersecurity threats and use their frames of reference as levers to improve engagement in training and awareness activities. Østgaard Skotnes (2019) applied the sensemaking framework to cybersecurity standards, showing that the professionals tasked with their implementation translate formal prescriptions into local practices that differ from one organization to another. Hence, sensemaking has demonstrated its potential to illuminate several essential cybersecurity practices but has not yet been used to analyze cyber-resilience.

4. Data and methods

Our study blends three qualitative methodologies to capture the experience of cybersecurity professionals who routinely deal with cyber-attacks. We interviewed 58 respondents from 37 organizations. A purposeful maximum variation sampling approach (Patton, 2015) was adopted to achieve a diversity of views and experiences across five dimensions (geography, institutional type, institutional size, interviewee role, and interviewee experience). These dimensions were chosen to ensure that the rich and varied national, organizational and personal contexts influencing how respondents incorporate cyber-resilience into their practices were accounted for. While other dimensions, such as internal culture, the competitive environment, or specific types of cyber-attacks repelled, could also have been added for a more comprehensive analysis, the five core dimensions used here still allow us to avoid distortions due to limited breadth in sampling and to identify potential temporal changes and trends (Poulis et al., 2013). The geographical diversity of the sample recognizes both the global nature of the cyber-resilience challenges faced by organizations 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 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. Most of our respondents originated from the financial sector, understood in its broadest sense (banks, insurance companies, pension funds, and stock exchanges). Still, their insights apply well beyond the world of finance. The consulting and incident-response firms that provide cybersecurity services to organizations and the regulators who oversee their activities were also interviewed to understand how cyber-resilience was understood and adopted across the service delivery and regulatory divides. The respondents' positions ranged from Chief Information Security Officers (CISOs) (11 respondents) and Chief Risk Officers (CROs) (3 respondents) to Directors of Security Operations Centres (SOCs) (2 respondents), Incident Response Teams (CSIRTs) (4 respondents), threat intelligence teams (4 respondents), and business continuity units (4 respondents); leaders of penetration-testing teams and red teams (2 respondents); IT governance and security advisors (13 respondents); consultants providing incident-response services (9 respondents); and industry regulators (6 respondents). This diversity of roles and responsibilities generated interesting variations related to sensemaking and the perceived usefulness of cyber-resilience. Experience in a cyber-risk management or regulation role ranged from half a year to more than thirty years, providing historical perspectives on the various risk management trends that preceded cyber-resilience. Table 1 provides an overview of the respondents' features.

Table 1
Respondents' descriptive statistics.

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	

Potential interviewees were identified and contacted through four main strategies: in Canada, a think tank (the Global Risk Institute) and a cross-sectoral information-sharing hub (the Canadian Cyber Threat Exchange) supported the research project and helped connect the research team with their membership. The first author also leveraged the database of the Smart Cybersecurity Network (SERENE-RISC), an academic-public-private partnership which he led between 2014 and 2022, to identify respondents. In the UK, France and the Netherlands, key academic informants with well-established connections in the cybersecurity industry were contacted to identify and introduce us to respondents. Finally, US respondents were identified through personal networks and LinkedIn searches using keywords such as cyber-resilience, CISO, CRO, CSIRT, SOC, and business continuity units. They were contacted via the social media platform and invited to participate in the study. Interviews were conducted between Au-

gust 2018 and November 2020 in person (36), by phone or video-conference call (21), or by email (1). Thirteen respondents (22%) were female, reflecting the current under-representation of women in the cybersecurity workforce, which is estimated to be 22-25% women ((ISC)2, 2018; Hoteit, 2022; Risse et al., 2022). Interviews lasted for 57 minutes on average (range: 31 minutes to 1 ½ hours). 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 NVivo 12 (QSR International, 2018), a qualitative analysis software package that facilitates the exploration, coding, and visualization of large quantities of unstructured data.

All interviews used a semistructured approach, well-suited to exploratory projects such as this research (Billups, 2022). All interviews followed a similar script, found in Appendix A: 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. A benefit of semistructured interviews is that the sequence of questions and topics to be covered can be adjusted based on opportunities identified by the interviewer to uncover novel information or to expand on a specific line of enquiry (Billups, 2022).

The Thematic Analysis method was used to translate the collected data into valid meanings and insights about the cyber-resilience practices and experiences of cybersecurity professionals (Braun and Clarke, 2006). Thematic Analysis has become widely recognized in qualitative research because of its systematic nature allowing the clear reporting of coding, analytical and interpretative processes (Miles and Huberman, 1984), and its flexibility to blend inductive and deductive approaches. The six phases of Thematic Analysis outlined by Braun and Clarke (2012) were followed thoroughly. After having immersed ourselves in the data by reading all transcripts and notes at least once (1), we started the systematic analysis by generating the initial codes (2) using NVivo12. The codes were a mix of descriptive and interpretative, some of them corresponding to the concepts that guided our questions (incident response, redundancy, leadership, regulation, etc.) while others mirrored respondents' own experiences and mental models (red-teaming, information sharing downsides, luck in incident response, etc.). The coding process uncovered new codes and subcodes as it unfolded, and the recoding of earlier material proved necessary (Braun and Clarke, 2012: 63). The complete codebook containing the main codes, subcodes, definitions and examples is provided in Appendix B. Once the coding was done, themes that reflected patterns in the data and were connected to the research questions were extracted (3). This shift from codes to themes resulted from collapsing or clustering codes into two larger units of meaning: tensions and practices. The theme of sensemaking tensions describes the uncertainties and ambiguities that interfere with the adoption of a cyber-resilience mindset and is composed of four subthemes associated with the meaning(s) of cyber-resilience, the turbulences of the risk landscape, the contest with other organizational rationalities, and regulatory incoherence. The theme of cyber-resilience practices includes five subthemes that illustrate how tensions are absorbed and reduced on the ground through activities such as workforce development, communication, networking, preparation through playbooks and adaptation. In phase 4, the themes were reviewed in relation to the entire dataset. A potential information-sharing subtheme was considered for example for the practices' theme but was instead found to duplicate the communication and networking subthemes and abandoned as a theme to remain a code. Phase 5 involved defining and naming the themes, the outcome of this process being presented in sections 5 and 6. Finally, phase 6 consisted of producing the report from this analysis (this article), with an effort to summarize our findings through a simple but informative diagram illustrating the relationships between themes and subthemes, a strategy encouraged by Miles and Huberman (1984).

Although qualitative research is well-suited to uncover the extreme complexity and nuances of human experiences, the intertwined issues of rigor, validity and bias raise significant and legitimate concerns that prevent claims of generalizability (Golafshani, 2003). In cases where purposeful sampling is used, for example, errors can be made by the researcher in selecting respondents, which can introduce low levels of reliability and a higher probability of bias. As Norris (1997) reminds us, "there is no paradigm solution to the elimination of error and bias. Different forms of research may be prone to different sources of error." However, mitigating strategies can be adopted to reduce the likelihood that such errors and bias taint qualitative research findings (Krefting, 1991; Sandelowski, 1993): the ones used in this research include member checking (through presentation and discussion of results at professional conferences attended by respondents), triangulation (through the use of internal documents and a sampling of respondents across the regulatory and service provision divides), and a prolonged and varied field data collection strategy (in time and space). Despite these precautions, it is impossible to generalize the results presented here. Only a more experimental design enabling the systematic collection of pre- and post-incident data across a larger sample could improve the validity of the data. Using the Critical Incident Technique on a randomly selected group of organizations would undoubtedly increase the reliability of what is known about their cyber-resilience practices and their impact (Butterfield et al., 2005).

5. Results

In this section, we expose the four major sources of sensemaking tension that 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. These four sensemaking tensions reverberate across a plethora of decision-making processes that 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" (CISO, United Kingdom 2). In the second half of this section, we describe how these sensemaking tensions are embedded in strategies and practices adopted in the name of cyber-resilience.

5.1. The tension of polysemy

While academics, consultants, standard-setting bodies, and regulators offer seemingly straightforward definitions of what cyber-resilience ought to be, respondents expressed a lot more uncertainty and reflexivity about the meaning they assigned to the term. 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. (CRO, 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 (CRO, 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. (CISO, 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 reflects 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. (CRO, 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" (CRO, Canada 26). This understanding was not restricted to respondents with a social science background; technically-minded professionals also embraced this approach.

5.2. The tension of turbulent cyber-risk landscapes

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.

> That approach [information sharing as a sensemaking activity] 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. (CISO, 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) (CISO, Canada 22).

The dynamic nature of cyber-risks can destabilize sensemaking processes at different stages of an adverse event. Respondents recalled many cases where what was initially identified as a relatively minor incident quickly escalated into a much more complex crisis that unfolded over many months. In one example, the 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 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.

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 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. (Consultant, Canada 18)

5.3. The tension of 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 operational business requirements and cyber-resilience. With digital technologies transforming organizations, 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. (CRO, Canada 23)

To resolve this tension, cybersecurity professionals implementing cyber-resilience practices inside their organizations place a strong emphasis on communication. They are mindful of their users' business needs, incorporate them into their risk management mandate, and carefully communicate 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. (CISO, 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 these events that disrupted their organization or competitors 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. (Red Team Leader, Netherlands 4)

5.4. The tension of 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 organizations with branches in many countries (sometimes more than fifty) that operate under a broad range of regulatory regimes. Organizations must incorporate and consolidate these variations into their sensemaking processes to ensure compliance 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 organizations 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. (CISO, Canada 19)

5.5. How sensemaking tensions reverberate through cyber-resilience practices: preparing to improvise

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 doing so. Respondents advocated multiple strategies compatible with ambiguities and tensions in the sensemaking process. 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. (CISO, United Kingdom 2)

Human resources: The hiring of incident-response practitioners who displayed personal traits such as higher-than-average curiosity, creativity, and flexibility was frequently mentioned. This allowed cybersecurity teams 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. Beyond individual features, participants noted that diversity was becoming more valued in teams that manage cyber-crises (Threat Intelligence Team Director, Canada 27; CISO, United Kingdom 2). Some organizations had built or were building multidisciplinary teams that drew on a wide array of backgrounds, perspectives, and expertise.

Communication: 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 organizations to segment expertise and require secrecy when crises unfold—which hinders sensemaking, many respondents highlighted the benefits of having developed a dense web of ties throughout the organization to deal with adverse events. For some, this meant embedding security workers inside business units to understand their culture and technological constraints better and attempting to "build fundamental security into the business processes" (Consultant, 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.

Engaging with third parties and information sharing: External networks play a growing role in expanding the sensemaking capacities of an organization in support of cyber-resilience. Organizations 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. In the financial sector for example, and prompted by regulatory requirements, organizations 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 vital 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. (SOC Director, 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 with external partners 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 critical systems 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. (CRO, 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 (CISO, 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" (CISO, Canada 19).

Playbooks: Response playbooks are one of the main tools used by cybersecurity professionals to activate sensemaking processes during cyber-attacks. 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 an organization must recover in case of an extreme adverse event and its regulatory requirements during such events. 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 (Business Continuity Unit Director, 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 (CISO, 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 creating a playbook 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 (Security Advisor, 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 (Threat Intelligence Team Director, Canada 1; CISO, Canada 32).

Adaptation: 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 global financial industry, highlighting the fragility of existing assumptions and leading to significant changes (Security Advisor, Canada 5; Security Advisor, Canada 16; Incident Response Team Director, Canada 17; CISO, United Kingdom 1; Business Continuity

Unit Director, United States 2). Many more minor incidents 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.

These review documents summarize 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. But it is difficult to assess how these insights are incorporated into cyber-resilience practices. 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 (Security Advisor, 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. (Business Continuity Unit Director, Canada 2)

Industry standards also perform an adaptive function. Standards gradually incorporate lessons learned from past incidents and 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 (CISO, 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 (Security Advisor, Canada 3).

The third form of adaptation stems from the regulatory activity to which organizations are subjected. Respondents identified "a trend towards more regulation and more specific regulation" (CRO, 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 organizations 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 whole industries 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 (Regulator, 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 (Business Continuity Unit Director, United States 1; CISO, Canada 28).

6. Discussion

6.1. The four foundational tensions of cyber-resilience

Our research identified four central ambiguities and uncertainties that inhibit the sensemaking processes of cybersecurity professionals and frame their ability to become resilient to stresses and shocks. The polysemy tension 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), this is, to our knowledge, the first time this challenge has been empirically documented in the field of cybersecurity. It is clear that many cybersecurity professionals feel cyber-resilience remains a fuzzy concept that is hard to distinguish from well-established cybersecurity approaches and that this confusion is interfering with the emergence of new sensemaking processes. The problem of defining what cyber-resilience is and what practical measures are associated with this definition is not only a theoretical puzzle to solve. It also has practical implications, for example, when the technical and social dimensions of cyber-resilience are considered. A definition of cyber-resilience that is more inclusive than a pure engineering perspective and incorporates social and organizational features implies a more sustained dialogue with practitioners outside of the cybersecurity realm, such as lawyers, psychologists, and management experts, and an effort to disseminate sensemaking frames to a broader group of professionals in a format that is compatible with their own sensemaking habits.

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. 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 organizations, a form of distributed sensemaking, cannot alleviate. It has been demonstrated that AI technologies can prove helpful in helping cybersecurity professionals cut through the endless noise of incidents, alerts and risks to which their detection systems expose them, enabling them to handle more incidents more efficiently and to address weak signals before they transform into full-fledged crises (Bridges et al., 2023; Zoppi et al., 2023). But 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 fragile when confronted with constantly adapting thinking adversaries (Heaven, 2019).

Once cyber-risks have materialized into actual incidents, they often prove difficult to contain, generating risk cascades (van Eeten et al., 2011) that increase their dynamic properties 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 cus-

tomers (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. Almost a quarter of participants in our study mentioned that this shift to the cloud complicated their risk-management practices and even "made them blind" (Security Advisor, Canada 16). The existence of 'Shadow IT' systems (Hagenaars, 2019), often hidden from cybersecurity professionals, is another source of turbulence that can destabilize sensemaking processes. 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.

The tension of contested organizational rationalities captures the resistance that cyber-resilience practitioners encounter within their organizations, from revenue-generating colleagues who see any cost to prepare for a hypothetical risk as a waste of resources that could be allocated more productively. If cybersecurity professionals are familiar with this posture and are encouraged to adopt budgeting tools that focus as much on processes as on outcomes (Moore et al., 2015), the challenge of demonstrating return on investment (ROI) for cyber-resilience measures that attempt to address the unknown is significantly more demanding. In our sample, respondents tried to overcome this tension by using various communication strategies to persuade their C-suite counterparts that investing in redundancy, diversity, and surge capacities can help the organization avoid some public embarrassment. They can rely on a constant stream of very public cybersecurity debacles to support their argument. More recently, Linkov et al. (2023) have proposed a novel approach to counter the dominant narrative of the structural inefficiency of cyber-resilience, introducing a distinction between short-term and long-term efficiency. By expanding the timeline over which efficiency is measured, they flip the argument of necessary trade-offs between efficiency and resilience to suggest that resilience might hamper short-term efficiency but strengthen long-term efficiency through limited degradation and speedier recovery of systems. Although challenges persist in how best to optimize long-term efficiency through resilience, this approach can potentially reconcile competing organizational rationalities.

The fourth and final tension reflects how regulatory disparities between jurisdictions might undermine the coherence of cyber-resilience practices for organizations that operate internationally. Some countries have adopted a principles-based approach to the regulation of cyber-risks, while others, such as the UK, Denmark or the Netherlands, have been more prescriptive and have developed proactive testing strategies (CBEST in the UK and TIBER in Denmark and the Netherlands) in which external 'red teams' mimic the types of attacks carried out by sophisticated actors (Hielkema and Kleijmeer, 2019). Jurisdictions such as Australia, Hong Kong or Singapore are explicitly adding cyber-resilience as one of the outcomes mandated by regulatory authorities, while others are adhering to more familiar cybersecurity frameworks. These variations indicate an encouraging capacity for innovation and adaptation but also force regulated entities operating across multiple jurisdictions to track an extensive array of regulatory regimes and tweak their cyber-resilience measures accordingly. This results in the artificial fragmentation of cyber-resilience practices, where consolidation would be a more desirable outcome. The European Union has acknowledged this tension and introduced in late 2022 the Digital Operational Resilience Act (DORA), which will come into effect in January 2025 (European Council, 2022). This set of uniform requirements seeks to harmonize the cyber-resilience capacities of financial institutions and their critical third parties (such as cloud providers) across 27 countries (Clausmeier, 2022). How well this approach can scale globally and across sectors remains an open question.

6.2. Cyber-resilience in practice

The four sensemaking tensions outlined in our data (polysemic meaning, turbulent risk landscape, contested organizational rationalities and disparate regulatory requirements) reverberate across five types of activities triggered by organizations' exposure to cyber-risks. Diagram 1 represents how sensemaking tensions intricately shape cyber-resilience practices, which in turn attempt to ease these tensions to improve the quality and reduce the uncertainty of decision-making.

We found that the processes and technologies needed to enhance cyber-resilience apply to socio-technical systems defined by the entanglement of humans and machines. It implies that to deliver cyber-resilience, one must engineer robust systems but also promote social practices and support human choices that let people adapt systems to unpredictable attacks (Dunn Cavelty et al., 2023). This means that cyber-resilience programs within organizations must pay particular attention to the selection, training, and retention of cyber-resilience practitioners. Without being reckless, these practitioners need to be 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 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.

Collectively, cyber-resilience units need to be assembled with diversity in mind to ensure that their decisions do not overlook weak signals or discard unorthodox approaches because of groupthink (Janis, 1972). Their diversity should, in turn, be leveraged to enhance their networking capacities, helping them activate bridging capital and weak ties within and outside the organization (Granovetter, 1973). The curation and maintenance of such network ties act as a resource multiplier that can deliver surge capacity in adverse situations. Under this approach, Netflix has for example launched a Reservist Program in which auxiliary crisis managers are trained across the organization to distribute and scale sensemaking and response expertise (Joshi, 2020).

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). The analogy seems fitting since the playbooks that are developed to guide cybersecurity teams through incidents can sometimes be as detailed and rigid as musical scores, with their "linear style checklist of required steps and actions required to successfully respond to specific incident types

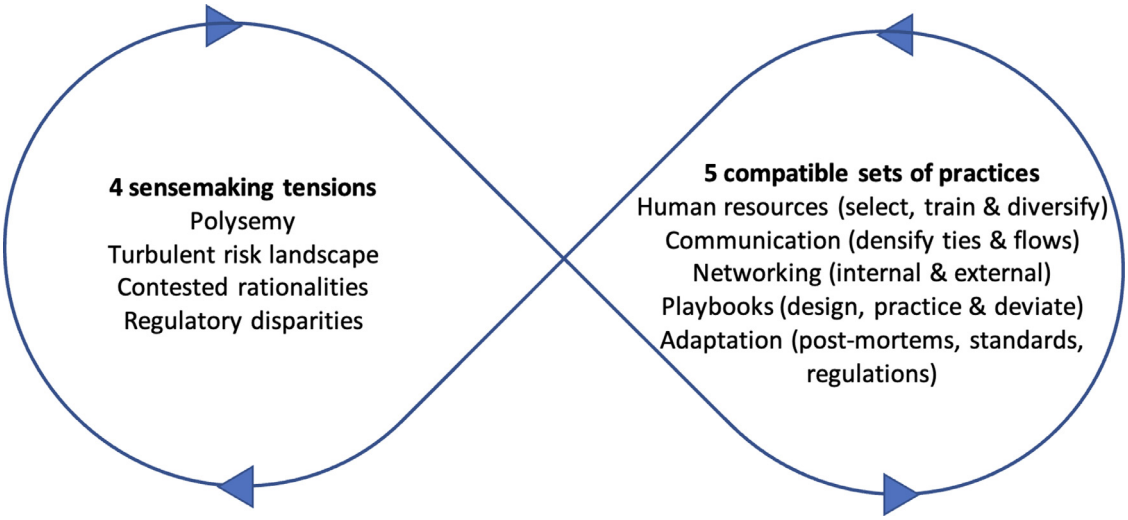

Diagram 1. The cyber-resilience cycle.

and threats" (van der Kleij et al., 2022). As our respondents indicated, playbooks are valuable assets that can provide a false sense of security in extreme circumstances and paralyze the sensemaking process to exclude unusual but effective decisions. Playbooks become traps when teams face unexpected or unknown attack configurations and cling to obsolete and counterproductive procedures instead of improvising an adequate response.

6.3. Limitations

The analysis of the empirical data reflects the fact that all interviewees did not share the definition of cyber-resilience that we had, which was derived from the burgeoning scientific literature. Hence, there are significant distinctions between the theory and practice definitions that we did not anticipate but have important implications for future research. Researchers should be aware of this gap when they collect data, making sure that they find ways to clarify how practitioners make sense of cyber-resilience when they answer surveys or questionnaires, to avoid misinterpreting their responses. Their theoretical models should be able to account for the diversity of cyber-resilience approaches and framings and avoid seeking a unique explanation of how cyber-resilience is delivered.

Although we initially expected to identify different ways in which cyber-resilience sensemaking took place across countries, the size of our sample was insufficient to make this comparison possible. Even within the same jurisdiction or market (Canada, for example), it became clear that 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. Future research should seek to capture this information at a much higher level of granularity than we were able to, to understand better how these sources of variation impact levels of cyber-resilience.

Finally, our interviews relied on respondents' capacity to recall accurately their organizations' responses to the most disruptive cyber-shocks they had experienced. In that respect, we could not control for a set of individual and collective cognitive biases that can interfere with sensemaking and 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). These biases likely influenced the data we collected, leading respondents to underestimate the negative impact of disruptions and overestimate organizational cyber-resilience skills and capacities. Future research on cyber-resilience should therefore try to investigate how significant these biases are in the sensemaking processes of cybersecurity professionals and design methodologies that limit their impact.

6.4. Practical implications

We see four practical implications deriving from this research. The first one is that a cyber-resilience program that aims to be effective should not only rest on technologies and procedures that enhance an organization's ability to absorb, withstand, respond to, and recover from a cyber shock. It should also assess the organization's exposure to the four tensions exposed here and strive to ease them through strategies that foster the emergence of an internal shared meaning for cyber-resilience, the provision of tools and methodologies to managers that enable them to forecast and navigate risk turbulences more confidently, the creation of an internal consensus to align various organizational rationalities, and the optimization of responses to regulatory obligations.

At the individual level, hiring and training strategies that value and develop the specific analytical, decision-making and communication skills supporting cyber-resilience practices should also be designed and implemented more systematically. Obviously, technical skills should still play a central role when making HR decisions. Still, cybersecurity teams should also consider how to balance them with the cognitive and social abilities that seem pivotal

in resolving adverse events. Diversity in teams can also become a tool for cyber-resilience, as was mentioned by several respondents, not to conform to the current trend toward more equitable, diverse, and inclusive organizations but because it reduces groupthink and expands the range of available operational options.

The third practical implication is that organizations will need access to more integrated cyber-resilience knowledge to design and implement measures that embrace the technical and social aspects described in this research. Cyber-resilience knowledge is multidisciplinary by nature (Linkov and Kott, 2019; Dunn Cavelty et al., 2023), and various disciplines are needed to support organizations in their journey. These disciplines must overcome their current fragmentation to start a more productive dialogue on cyber-resilience. Even within cybersecurity, more linkages are required between research areas that are frequently considered separately to fit with a reductionist scientific model but whose interdependencies can positively contribute to cyber-resilience. Research topics such as risk modelling, information sharing, situation awareness, incident response, business continuity, education, training and awareness, cyber-hygiene, and organizational learning, to name a few, form a web of knowledge and expertise from which cyber-resilience can emerge, providing they are considered as discrete parts of a larger whole.

Finally, regulations and standards can become powerful governance tools to broaden and accelerate the adoption of cyber-resilience practices and overcome the barriers that market forces impose on cyber-resilience. Standards are sometimes defined as a "recipe for reality," they 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). Government regulations are more constraining and contain elements of coerciveness and control that voluntary standards lack. Our research suggests an increased interest in translating cyber-resilience practices into formal standards and compulsory regulations, particularly in the financial sector and other critical infrastructures (Maurer and Nelson, 2020). However, there is a risk that the uncoordinated proliferation of such tools could become counterproductive by fuelling sensemaking tensions instead of clarifying expectations. Policymakers, legislators, standard-setting bodies and industry associations should work collaboratively to ensure that emerging cyber-resilience standards and regulations reduce sensemaking tensions.

7. Conclusions

This article provides a detailed overview of the current sensemaking tensions that cyber-resilience practices generate for the cybersecurity professionals who attempt to implement them. By sharing some of their insights, these professionals have outlined the tensions inherent in implementing cyber-resilience practices, 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 links technical systems, organizational processes, and human behaviors and is constrained by four central 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). These sensemaking tensions are caused by the polysemic meaning of cyber-resilience, the turbulences of the cyber-risk landscape, the contested rationalities of business performance and innovation that hinder cyber-resilience practices, and the regulatory disparities that face organizations trying to deploy cyber-resilience programs across jurisdictions. To overcome these tensions, cybersecurity professionals also rely on a set of resilience metaphors that help them live through the messiness of risks that can never be wholly predicted or prevented. In that respect, cyber-resilience is a complex sensemaking activity whose enactment enables the maintenance of critical flows.

Organizations and cybersecurity professionals partly resolve these tensions through five sets of practices that enhance their capacities to withstand and recover from cyber shocks: the selection, training and retention of individual operators who display and acquire crisis management and handling skills, a focus on communication strategies to align organizational rationalities, the buildup and maintenance of internal and external networks to quickly access and mobilize surge capacity, the design and rehearsal of playbooks to exercise organizational muscle memory, and the development of adaptation strategies to learn from past experiences and formalize the insights gained. Beyond lessons for individual organizations aiming to enhance their cyber-resilience, this research also identified some theoretical implications, calling for a more interdisciplinary approach. Its main policy implication for regulatory and standards-setting organizations is to ensure they promote clear expectations and coordinate their actions to increase coherence and robustness instead of fuelling sensemaking tensions that interfere with cyber-resilience.

Declaration of Competing Interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Benoit Dupont reports financial support was provided by Social Sciences and Humanities Research Council of Canada. Benoit Dupont reports financial support was provided by Global Risk Institute

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. **Marilyne Bernier:** Conceptualization, Formal analysis, Investigation, Data curation. **Rutger Leukfeldt:** Conceptualization, Investigation.

Data availability

The data that has been used is confidential.

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.

Appendix A. Interview Script

1. Can you tell me more about your role and your responsibilities at your current organization?
2. How do you define resilience and how has your understanding of the concept/practice evolved since you first began working in the field of cybersecurity/information security?
3. Can you describe what you believe has been the most severe cyberattack or hack you've experienced?
4. What were the short and long-term impacts on your operations?
5. How have you responded to it?
6. How have you kept the organization operating during the crisis?

7. Can you provide examples of conflicts, struggles, clashes of interests and sensitivities (internally or externally to the organization), hindering mitigation efforts and preventing the implementation of more resilient technologies/policies/practices?
8. Do public-private partnerships (in the information-sharing space, for example) that are systematically advocated as a way to improve the state of cybersecurity actually improve the resilience of your organization? How does it contribute to or erode your cyber-resilience?
9. What kind of technology decisions and practices enhance your organization's cyber-resilience? Do you purchase for example overlapping security technologies to increase redundancy and diversity?
10. What is the role of external security service providers in achieving resilience objectives? Do they hinder or facilitate resilience?
11. Can legislation and regulation play a positive role in fostering cyber-resilience?
12. Does your cybersecurity workforce contribute to your organization's cyber-resilience, or on the contrary proves to be a liability in that domain (because of a lack of skills—quantitative or qualitative—for example)? What kind of stress did it experience as the result of a shock? Did it lead to departures or a decrease in morale?
13. What are the personal features of people who thrive in crisis situations and contribute the most to building resilience within an organization? What personal traits have helped you most work toward the resilience of your organization?
14. How do you train for resilience? (readiness, simulations, exercises, reviews of existing arrangements and emerging threats)
15. What is the hardest thing that prevents an organization from becoming cyber-resilient? (what makes cyber-resilience hard to achieve for your organization?)
16. Is there a question you think I should have asked you but did not?

Appendix B. Codebook

Code: parent	Code: child	Definition	Example
Role		Describes the current role of the respondent.	And then I became Security Lead for the entire IT domain within [name of financial institution]. For your image, that's just under 9,000 people. So I took the responsibility there to figure out about all departments and units, to bring all security disciplines together and to ensure that we spoke with one voice there. [Red Team Leader, Netherlands 4]
Experience	General	Describes the professional experience of the respondent.	So I'm a chartered accountant or a CPA by background, by essentially for my career, I've been either in internal audit or risk management, so I've been about 20 years, or maybe a little more than 20 year now, doing that, so I work with insurance organizations, my first seven years I was with Price Waterhouse Coopers and then after than with a financial institution. [CRO, Canada 26]
Experience	Law enforcement & intelligence	Describes previous experience in law enforcement and intelligence.	I worked in investigation for many years before that... I was one of the project leaders for setting up the electronic crimes task force. [Threat Intelligence Team Director, Netherlands 5]
Definition		Describes the definition that respondents assign to the term 'cyber-resilience' and the nuances they include in this definition.	We do not explicitly differentiate between operational resilience and cyber resilience. "Operational resilience" is defined as the implementation of techniques to absorb the shock of an event in order to minimize the impact to the firm, its customers, and the sector during an incident. Cyber security has long been a critical aspect of resiliency efforts, and the continuing evolution of both our cyber security and business continuity and disaster recovery (BC/DR) finds them increasingly integrated and complementary in the current technology and threat environment. [Business Continuity Unit Director, United States 2]
Cybersecurity organization		Describes the organizational arrangements that support cyber-resilience roles and measures.	We have a group, it is called IT-Continuity Services, ITCSS, Continuity and Security Services, that is the group where we..., which we call the bridge. So it ensures that the internal systems continue to run. So let's say the control room, in the classic form, that ensures that all infrastructure is in place. Attached to that is a small team that does network security, and there is another team attached, which is our cyber defense center, the CBC. They are also physically close to each other, so that when the control room signals that what is not going well, they also have those two teams nearby. [CISO, Netherlands 1]
Technology		Discusses how technology decisions are impacting cyber-resilience.	Using good fundamental security architecture and good security practices and the hygiene as your base within the company, you can become resilient to the outcomes of a breach and you do that by compartmentalizing the functionality of business functions within the organization by compartmentalizing systems and how they're interfaced and interact with each other. A lot of companies have moved towards micro-services, container-type architectures. [CISO, Canada 28]
Incentives		Describes incentives driving organizations to improve their cyber-resilience.	But now we also have an extensive intel team on board, so our own people who, let's say, live on the dark web, who therefore hear things that you normally do not hear and that you are not allowed to tell anyone. And I don't know how they got it, but they say: don't ask. But we are able to feed management with very up-to-date information about incidents that occur at colleagues, competitors, that do not go public but that do take place. So that's the scary factor. So we are quite able to tell what is really going on. And we see it getting closer. [SOC Director, Netherlands 6]
Challenges	Contested rationalities	Describes conflicts and tensions between resilience practices and other organizational operational or functional priorities.	Maybe there are others who could say "When I want to invest in resilience, well I lose money." Because there is no return on investment, it's hard to quantify. [Threat Intelligence Team Director, Canada 1]
Challenges	Limited resources	Discusses the reluctance to spend on resilience in the face of other investment priorities.	Money, so yes I understand the need to become cyber resilient but I can't afford it, it's too much, I can't afford to invest in that, sorry the bank can't afford to invest in that new technology that you think is going to make us more resilient. [CISO, Canada 22]

(*continued on next page*)

(*continued*)

Code: parent	Code: child	Definition	Example
Challenges	Sense-making	Describes how people make sense of and interpret risk and how they use these processes to manage risks through technical or organizational controls.	How do we try to understand what resilience is? A lot of people say, resilience, we need to build a robust, agile system. So, I started to think about it. What is this robust, agile system? And then I figured out, that 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. It has to be a tradeoff. [CISO, United Kingdom 2]
Incident response	Autonomy & Creativity	Describes some features of people involved in incident response: how much freedom they have to innovate and take responsibility and how they are able to think outside the box.	You need people that are comfortable with making decisions based on what we know and if we have to backtrack and do something else like that, not feeling ashamed or bad about that. [CISO, Canada 19]
Incident response	Dynamic	Discusses the velocity of responses and the dynamic nature of incidents.	Look at the intelligence sources we use; we have consciously said that we have a kind of agile sources management process in which we continuously assess whether what they deliver adds value to our intelligence requirements. [Threat Intelligence Team Director, Netherlands 5]
Incident response	Flexibility	Discusses the need for teams responding to incidents to remain very flexible, which sometimes implies deviating from established procedures.	You are an outside point of view, you tell them how to change their methodology, that the approach they have been taking for 20 years is the wrong approach. So right there, obviously we're trying to bring it in a more different way, but that alone is enough to create conflict. Basically, we tell them: "your practices that you have been doing since the 90s, they have evolved, they have changed, we have learned to be a little more agile. [Consultant, Canada 11]
Incident response	Luck	Discusses the element of luck in the incident response process that enables an organization to keep operating despite very adverse conditions.	The company I'm thinking of just got very fortunate that they could continue to work with their customers on the predetermined schedules that they had for a period of three-and-a-half weeks before they were able to resume backend functionality. [Consultant, Canada 18]
Incident response	Surprise	Describes the sources of surprise that an unexpected attack might entail and the impact on speed and ability to make decisions (the startle effect).	People find it difficult to envisage a scenario where we lose all the IT. [Business Continuity Unit Director, United States 1]
Incident response	Botched	Describes examples of failed incident responses or incident response decisions that produced unintended short-term or long-term consequences.	I've seen people who just blind panic. I've seen a lot of careers end during and after breaches. I have seen people walk away from companies after being there for twenty-plus years and they're major shareholders, but the incident shocked them so bad that they just felt that they had underperformed or failed during the incident and they walk away from the company. [Consultant, Canada 18]
Incident response	Distrust	Reflects the lack of trust in established systems, procedures and colleagues during an incident, because they could compromise the response.	Only my little group knows about it. There are things that even my managers don't know about… because I can trust them, except if they talk to someone else, I don't trust anyone… and then it ends up coming back to my contact and things get out of hand. So it's really not to lose that trust… so "Shut the fuck up." [CSIRT Director, Canada 15]
Leadership		Describes features of effective resilience leadership.	Leadership and communication are key. It's respect too, because when you become tired sometimes, it's not always easy. Then also to understand that when you are in operation it is not necessarily always "please, thank you, would you try to." Often it is more directive. [Security Advisor, Canada 6]
Human resources		Describes human resource practices (hiring, training, retention) tied to cyber-resilience programs and activities.	At the same time, to go and find people who are on the market, it is possible, who already have some experience. And there, I will also look at students. For me it is important. [name of a competitor] did it a few years ago and it pays off today. They did activities to attract them. So we too have to start doing that. [Security Advisor, Canada 16]
External expertise		Discusses conditions under which external expertise from consultants and service providers is brought in, as well as the pros and cons of such solutions.	As the time passed by we then switched at some point and we outsourced a number of those services. So we have an American party that offers us the scrubbing service but in a situation where we have that on demand. So there is an incident, we see the malfunction, at a certain point it is decided that we need additional scrubbing. Such a process takes about fifteen minutes during which we then switched all our data traffic to that scrubbing service and only received filtered traffic there. [Security Advisor, Netherlands 2]
Stress management		Decision-making and behaviors under stressful conditions.	Yeah, you have to be looking at that right, stress is a key factor in cyber security at the moment right, like it's busy, you're dealing with scary things right… incident response team has gone to looking at bigger things, incidents are bigger nowadays than they used to be. [CISO, Canada 24]
Communications		Describes communication practices regarding cybersecurity and cyber-resilience within the organization.	You have another one, where people want obviously to be updated and know what's happening, because they're engaged, and they want effective communication, but that also slows the team down. [CISO, United Kingdom 1]
Information sharing	positive	Discusses the positive impacts of information-sharing practices.	In another situation it was before an attack, where six weeks before, again a public authority contacted some banks and shared information about an upcoming attack based on weaknesses they had identified on some payment systems. At the time it was in Malaysia. So again, the banks prepared, they protected themselves and when they did that in advance, it worked well. [Consultant, Canada 7]

(*continued on next page*)

(*continued*)

Code: parent	Code: child	Definition	Example
Information sharing	negative	Discusses the downsides and limitations of information-sharing practices.	You just kind of have to hope that you're not the first one because the first one is where the IOCs [indicators of compromise] come from, but they also create a lot of noise. The number of IOCs that come in every day from these feeds is quite overwhelming and a lot of them are duplicates. But even with the deduplication, trying to determine from a list of threats, which ones apply to your environment and which ones don't, or which one could or prioritize even which ones you want to implement first is very difficult. [Incident Response Team Director, Canada 17]
Networked	Internal networks	Discusses connections and communication protocols with internal stakeholders, as well as silos within organizations and the need to break barriers across business units.	We have a seamless relationship; everybody gets on well. We try to be very transparent with one another. We have clear lanes. I have–we have with the CISO. We meet probably once a week in person. We probably talk several times a week and we are at the same meetings and he recognizes that yes, you know what we do is different from him. We are never going to set him for failure, and he knows that. [Security Advisor, Canada 21]
Networked	External networks	Discusses the connections with external stakeholders, as well as the conditions under which trust is built to sustain these networks.	So, we are very actively involved with G7 partners to a group called the Cyber Experts Group, CEG. In terms of doing just that, sharing best practices, developing work streams and agendas among the G7 countries [...]. Through you know, more understanding the different types of robustness challenges and responses and you know identifying an ever-widening set of risks and addressing them as we see them. [Regulator, France 1]
Preparations		Discusses the planning activities that outline responsibilities and capacities in case of an incident.	We have around 16 of them right now. So 16 different, major scenario types, there's lots of nuances that will happen, the main thing is to have thought about what if we get attacked and it's a financial fraud, what if we get hacked and it's ransomware, what if it's data loss, what if it's a data loss of PII data, what if it's a multi country data loss, you know a number of these are sub-scenarios under a main scenario, so we have around 16 but we review them every quarter and decide if we want to add new ones based upon what's happening in the world, or things we've come up with. [CISO, Canada 22]
Practiced	Training	Describes what kinds of training regimes are implemented to enhance cyber-resilience.	And we absolutely do have scenarios, including cyber scenarios, that we do...we engage all the way up to and including the CEO and the board as appropriate, based upon these scenarios so that folks understand this is the way we would respond, these are the roles people would play and we do role playing. [CRO, Canada 23]
Practiced	Red teaming	Describes the practice of tasking an internal or external team with attacking the organization's defenses to identify potential weaknesses and help build up and practice defensive activities.	I think what makes [our methodology] different from regular red teaming is that we really try to mimic, simulate sophisticated criminal groups and nation-state proxies, based on threat intelligence. So it is not just that we look like, what shall we attack in this organization, what crown jewel are we going to take? No, that is based on intelligence. [Regulator, Netherlands 3]
Redundancy		Describes the ability to rely on alternative resources/technologies and spare capacities when main systems are unavailable or disabled.	The system we have in production we have the same system in relief. So, in the event of a breakdown, we are able to recover immediately. We are going to have two servers, we are going to have for example... if we have decided that the pay process is critical for us, we are going to have two pay systems so if one goes down, the other is going to be available immediately. In real-time so they exchange data immediately. [Threat Intelligence Team Director, Canada 9]
Diversity		Discusses how a variety of people, technologies and systems can foster cyber-resilience.	This team must include many skills, including, but not limited to, technical, strategic, communication and planning. It's essential that a team be part of the solution as no one person can possess them all. [Consultant, United States 4]
Surge capacity		Describes the extra resources needed to deal with a crisis / often expensive to justify in standard mode.	The big difference between that attack in 2012 and 2018 is that in 2012 we first started, say, introducing filtering, so through intensive filtering-like techniques within our own infrastructure. So we had then just started building offloaders. We got there in 2012, because that was a DDoS attack, which was the trigger to get a lot of that equipment in-house. Substantial investments have been made there. [Incident Response Team Director, France 7]
Standards		Discusses the relevance and role of standards for cybersecurity.	I see too many companies which are compliant... but which are not. Auditors will come and say "Do you have standards?" "Yes we have standard" "Perfect" ok so check. But the standards, they don't apply them. [Consultant, Canada 14]
Regulation		Discusses the impacts of regulations on cyber-resilience.	I mean I think regulation and legislation have a part to play and you know I do think they build the framework with which we have to operate. So I don't think that's a bad thing, you know, but the struggle that you do have is, when you have competing regulators or competing regulation, it becomes very difficult to operate, so if you take an example of say a privacy breach somewhere, say you're in the US, right, you might have to notify three different regulators across three different timeframes. [CISO, Canada 24]
Adaptation-Learning		Discusses how organizations adapt after incidents and learn from their responses (or failures) to increase their resilience (or fail to do so).	We have always done a post-mortem after the event, once the [crisis] cell is deactivated. What are the main lessons? What are things we could have done differently? What are the things to change? What are the short-term, medium-term, long-term things? [Business Continuity Unit Director, Canada 2]

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.

Ahmad, A., Desouza, K., Maynard, S., Naseer, H., Baskerville, R., 2020. How integration of cyber security management and incident response enables organizational learning. J. Assoc. Inf. Sci. Technol. 71 (8), 939–953. doi:10.1002/asi.24311.

Ahmad, A., Maynard, S., Baskerville, R., 2022. Editorial to the special issue on cybersecurity incident response in organizations. Comput. Secur. 112, 1–3. doi:10.1016/j.cose.2021.102530.

AIR, 2018. Cloud Down: Impacts on the US Economy. Lloyd's.

Alexander, D.E., 2013. Resilience and disaster risk reduction: an etymological journey. Nat. Hazards Earth System Sci. 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., Khurana, R. (Eds.), The Handbook for Teaching Leadership: Knowing, Doing and Being. SAGE, Los Angeles, pp. 3–19.

Anderson, R., Barton, C., Boehme, R., Clayton, R., Ganan, C., Grasso, T., Levi, M., et al., 2019. Measuring the changing cost of cybercrime. The 18th Annual Workshop on the Economics of Information Security doi:10.17863/CAM.41598.

Ansell, C., Boin, A., Keller, A., 2010. Managing transboundary crises: identifying the building blocks of an effective response system. J. Contingen. Crisis Manag. 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. Commun. Res. 15 (5), 582–602. doi:10.1177/009365088015005005.

Bellini, E., Sargsyan, G., Kavallieros, D., 2021. Cyber-resilience. In: Shiaeles, S., Kolokotronis, N. (Eds.), Internet of Things, Threats, Landscape, and Countermeasures, pp. 291–333.

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, pp. 833–844. doi:10.1145/2382196.2382284.

Billups, F., 2022. Qualitative Data Collection Tools: Design, Development, and Applications. SAGE Publications.

Björk, F., Henkel, M, Stirna, J., Zdravkovic, J., 2015. Cyber resilience – fundamentals for a definition. In: Rocha, A., Correia, A.M., Costanzo, S., 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.

Bouveret, A., 2018. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. International Monetary Fund.

Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qual. Res. Psychol. 3, 77–101. doi:10.1191/1478088706qp063oa.

Braun, V., Clarke, V., 2012. In: Cooper, H., Camic, P.M., Long, D.L., Panter, A.T., Rindskopf, D., Sher, K.J. (Eds.). In: APA Handbook of Research Methods in Psychology, 2. Research Designs: Quantitative, Qualitative, Neuropsychological, and Biological, pp. 57–71.

Bridges, R., Rice, A., Oesch, S., Nichols, J., Watson, C., Spakes, K., Norem, S., Huettel, M., Jewell, B., Weber, B., Gannon, C., Bizovi, O., Hollifield, S., Erwin, S., 2023. Testing SOAR tools in use. Comput. Secur. 129, 1–28. doi:10.1016/j.cose.2023.103201.

Busch, L., 2011. Standards: Recipes for Reality. The MIT Press.

Butterfield, L., Borgen, W., Amundson, N., Maglio, A.-S., 2005. Fifty years of the critical incident technique: 1954-2004 and beyond. Qual. Res. 5 (4), 475–497. doi:10.1177/1468794105056925.

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 Secur. Privacy 12 (5), 61–67. doi:10.1109/MSP.2014.85.

Clausmeier, D., 2022. Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). Int. Cybersecur. Law Rev. doi:10.1365/s43439-022-00076-5.

Connelly, E., Allen, C., Hatfield, K., Palma-Oliveira, J., Woods, D., Linkov, I., 2017. Features of resilience. Environ. Syst. Decis. 37, 46–50. doi:10.1007/s10669-017-9634-9.

Da Veiga, A., Martins, N., 2017. Defining and identifying dominant information security cultures and subcultures. Comput. Secur. 70, 72–94. doi:10.1016/j.cose.2017.05.002.

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. Ecol. Soc. 21 (2), 1–15. doi:10.5751/ES-08450-210227.

Dunn Cavelty, M., Eriksen, C., Scharte, B., 2023. Making cyber security more resilient: adding social considerations to technological fixes. J. Risk Res. doi:10.1080/13669877.2023.2208146.

Dupont, B., 2019. The cyber-resilience of financial institutions: significance and applicability. J. Cybersecur. 5 (1), 1–17. doi:10.1093/cybsec/tyz013.

Dykstra, J., Orr, S., 2016. Acting in the unknown: the cynefin framework for managing cybersecurity risk in dynamic decision making. 2016 International Conference on Cyber Conflict CyCon U.S. doi:10.1109/CYCONUS.2016.7836616.

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.

European Council (2022). Digital finance: council adopts digital operational resilience act. council of the European Union. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/.

Fedele, A., Roner, C., 2022. Dangerous games: a literature review on cybersecurity investments. J. Econ. Surv. 36 (1), 157–187.

Fujs, D., Mihelic, A., Vhrovec, S., 2019. 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. Modern Law Review 62 (1), 1–10. doi:10.1111/1468-2230.00188.

Golafshani, N., 2003. Understanding reliability and validity in qualitative research. Qualitative Report 8 (4), 597–607. doi:10.46743/2160-3715/2003.1870.

Granovetter, M., 1973. The strength of weak ties. Am. J. Sociol. 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.

Grøtan, T.O., Antonsen, S., Haavik, T.K., 2022. Cyber resilience: a preunderstanding for an abductive research agenda. In: Matos, F., Selig, P.M., Enriqson, E. (Eds.), Resilience in a Digital Age, pp. 205–229.

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.

Häring, I., Ebenhöch, S., Stolz, A., 2016. Quantifying resilience for resilience engineering of socio-technical systems. Eur. J. Secur. Res. 1 (1), 21–58. doi:10.1007/s41125-015-0001-x.

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: Schulze, P. (Ed.), Engineering within Ecological Constraints, pp. 31–44.

Hoteit, L., 2022. Empowering women can help fix the cybersecurity staff shortage. World Economic Forum Retrieved from https://www.weforum.org/agenda/2022/09/cybersecurity-women-stem/ .

Hu, S., Hsu, C., Zhou, Z., 2022. Security education, training, and awareness programs: Literature review. J. Comput. Inf. Syst. 62 (4), 752–764. doi:10.1080/08874417.2021.1913671.

(ISC)2 (2018). Women in cybersecurity. (ISC)2.

Janis, I.L., 1972. Victims of Groupthink: A Psychological Study of Foreign-Policy Decisions and Fiascoes. Houghton Mifflin.

Joshi, S., 2020. 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: Linkov, I., Kott, A. (Eds.), Cyber Resilience of Systems and Networks, pp. 69–92. doi:10.1007/978-3-319-77492-3_4.

Kirova, D., Baumoel, U., 2018. Factors that affect the success of security education, training, and awareness programs: a literature review. J. Inf. Technol. Theory Appl. 19 (4), 56–83.

Krefting, L., 1991. Rigor in qualitative research: the assessment of trustworthiness. Am. J. Occup. Ther. 45 (3), 214–222. doi:10.5014/ajot.45.3.214.

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. Environ. Syst. Decis. 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: Florin, M.-V., Linkov, I. (Eds.), IRGC Resource Guide on Resilience, pp. 3–14.

Linkov, I., Kott, A., 2019. Fundamental concepts of cyber resilience: introduction and overview. In: Kott, A., Linkov, I. (Eds.), Cyber Resilience of Systems and Networks, p. 1–25.

Linkov, I., Ligo, A., Stoddard, K., Perez, B., Strelzoff, A., Bellini, E., Kott, A., 2023. Cyber efficiency and cyber resilience. Commun. ACM 66 (4), 33–37. doi:10.1145/3549073.

Maitlis, S., Sonensheim, S., 2010. Sensemaking in crisis and change: inspiration and insights from Weick (1988). J. Manag. Stud. 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.

Miles, M., Huberman, A.M., 1984. Drawing valid meaning from qualitative data: toward a shared craft. Educ. Res. 13 (5), 20–30. doi:10.3102/0013189X013005.

Moore, T., Dynes, S., Chang, F., 2015. Identifying how firms manage cybersecurity investments. In: Workshop on the Economics of Information Security (WEIS), pp. 1–27.

Naseer, H., Maynard, S., Desouza, K., 2021. Demystifying analytical information processing capability: the case of cybersecurity incident response. Decis. Support Syst. 143, 1–11. doi:10.1016/j.dss.2020.113476.

Norris, N., 1997. Error, bias and validity in qualitative research. Educ. Action Res. 5 (1), 172–176. doi:10.1080/09650799700200020.

Østgaard Skotnes, R., 2019. Standardization of cybersecurity for critical infrastructures. In: Olsen, O.E., Juhl, K., Lindøe, P., Engen, O.A. (Eds.), Standardization and risk governance, pp. 166–180.

Pala, A., Zhuang, J., 2019. Information sharing in cybersecurity: a review. Decision Anal. 16 (3), 172–196. doi:10.1287/deca.2018.0387.

Paton, D., Johnston, D., 2017. Disaster Resilience: An Integrated Approach. Charles C. Thomas.
Patton, M.Q., 2015. Sampling, qualitative (purposeful). In: Ritzer, G. (Ed.), The Blackwell Encyclopedia of Sociology. John Wiley & Sons doi:10.1002/9781405165518.wbeoss012.pub2.
Pawlowski, S., Jung, Y., 2015. Social representations of cybersecurity by university students and implications for instructional design. J. Inf. Syst. Educ. 26 (4), 281–294.
Pomerleau, P.-L., Lowery, D., 2020. Countering Cyber Threats to Financial Institutions: A Private and Public Partnership Approach to Critical Infrastructure Protection. Palgrave Macmillan.
Poulis, K., Poulis, E., Plakoyiannaki, E., 2013. The role of context in case study selection: an international business perspective. Int. Bus. Rev. 22 (1), 304–314. doi:10.1016/j.ibusrev.2012.04.003.
QSR International (2018), NVivo (Version 12), https://lumivero.com/products/nvivo/.
ResearchAndMarkets (2022). Global cyber security market report (2022 to 2027) - IoT security to play a vital role in cybersecurity. Business Wire, 26 September. Retrieved from https://www.businesswire.com/news/home/20220926005315/en/Global-Cyber-Security-Market-Report-2022-to-2027—IoT-Security-to-Play-a-Vital-Role-in-Cybersecurity—ResearchAndMarkets.com.
Risse, L., Beamond, M., Hall, J., Barua, B., Warren, M., Kondylas, L., 2022. Women in Security: Preliminary Insights Report. RMIT Centre for Cyber Security Research and Innovation.
Rose, A., Miller, N., 2021. Measurement of cyber resilience from an economic Perspective. In: Chatterjee, S., Brigantic, R., Waterworth, A. (Eds.), 2023 Applied Risk Analysis for Guiding Homeland Security Policy and Decisions, pp. 253–274.
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.
Salvi, A., Spagnoletti, P., Saad Noori, N., 2022. Cyber-resilience of critical cyber infrastructures: integrating digital twins in the electric power ecosystem. Comput. Secur. 112, 1–11. doi:10.1016/j.cose.2021.102507.
Sandelowski, M., 1993. Rigor or rigor mortis: the problem of rigor in qualitative research revisited. Adv. Nurs. Sci. 16 (2), 1–8. doi:10.1097/00012272-199312000-00002.
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. Comput. Secur. 97, 1–15. doi:10.1016/j.cose.2020.101996.
Shreeve, B., Gralha, C., Rashid, A., Araujo, J., Goulao, M., 2022. Making sense of the unknown: how managers make cyber security decisions. ACM Trans. Software Eng. Methodol. doi:10.1145/3548682.
Simpson, N., Shearing, C.D., Dupont, B., 2019. Climate gating: a case study of emerging responses to Anthropocene risks. Clim. Risk Manag. 26, 1–10. doi:10.1016/j.crm.2019.100196.
Skopik, F., Settanni, G., Fiedler, R., 2016. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Comput. Secur. (60)„ 154–176. doi:10.1016/j.cose.2016.04.003.
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. Organiz. Stud. 43 (5), 699–724. doi:10.1177/01708406211035511.
Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A., Repchick, K., Zaccaro, S., Dalal, R., Tetrick, L., 2015. Improving cybersecurity incident response team effectiveness using teams-based research. IEEE Secur. Privacy 13 (4), 20–29. doi:10.1109/MSP.2015.71.
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 .
Thangavelu, M., Krishnaswamy, V., Sharma, M., 2022. Impact of comprehensive information security awareness and cognitive characteristics on security incident management – an empirical study. Comput. Secur. 109, 1–24. doi:10.1016/j.cose.2021.102401.
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 Des. Practice 2 (1), 53–74. doi:10.1080/25741292.2018.1507240.
Uchendu, B., Nurse, J., Bada, M., Furnell, S., 2021. Developing a cyber security culture: Current practices and future needs. Comput. Secur. 109, 1–23. doi:10.1016/j.cose.2021.102387.
van der Kleij, R., Kleinhuis, G., Young, H., 2017. Computer security incident response team effectiveness: a needs assessment. Front. Psychol. 8, 1–8. doi:10.3389/fpsyg.2017.02179.
van der Kleij, R., Schraagen, J.M., Cadet, B., Young, H., 2022. Developing decision support for cybersecurity threat and incident managers. Comput. Secur. 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 Administr. 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, 3rd ed. John Wiley & Sons.
Woods, D., 2015. Four concepts for resilience and the implications for the future of resilience engineering. Reliab. Eng. Syst. Saf. 141, 5–9. doi:10.1016/j.ress.2015.03.018.
Zoppi, T., Ceccarelli, A., Puccetti, T., Bondavalli, A., 2023. Which algorithm can detect unknown attacks? Comparison of supervised, unsupervised and meta-learning algorithms for intrusion detection. Comput. Secur. 127, 1–12. doi:10.1016/j.cose.2023.103107.

Benoît Dupont is a Professor of criminology at the Université de Montréal, where he holds the Canada Research Chair in Cybersecurity and the Endowed Research Chair for the Prevention of Cybercrime. He is the Scientific Director of the Human-Centric Cybersecurity Partnership, an interdisciplinary network of academic, government and industry partners.

Clifford Shearing is a Professor Emeritus at the Universities of Toronto and Cape Town and holds professorial appointments at the Universities of Griffith (adjunct), Montreal (associé), and New South Wales (visiting professorial fellow). He is an Associate in the African Climate and Development Initiative, University of Cape Town.

Marilyne Bernier is Principal Advisor in Business Continuity at one of Canada's largest financial institutions. She holds a Masters' Degree in Criminology from the Université de Montréal. Her thesis examined how cyber-resilience practices percolated through business processes in Quebec's financial institutions.

Rutger Leukfeldt (PhD) is senior researcher and the cybercrime cluster coordinator at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR). Furthermore, Rutger is the Director of the Centre of Expertise Cyber Security and leading researcher of the Cybercrime and Cybersecurity Group, The Hague University of Applied Sciences.