WITHSTANDING CYBER-ATTACKS:

A CYBER-RESILIENCE PRACTICES IN THE FINANCIAL SECTOR

APRIL 2020

Authors: Benoît Dupont, *Université de Montréal*
Clifford Shearing, *University of Cape Town & Griffith University*
Marilyne Bernier, *Université de Montréal*

GLOBAL RISK INSTITUTE

Over the past 25 years, cyber-risks have morphed from mere annoyances into potentially catastrophic events that threaten the survival of technology-dependent organizations. A number of financial authorities, such as the European Systemic Risk Board and the International Monetary Fund, consider cyber-risk a systemic risk to the financial system and have modelled the massive losses it might generate for financial institutions worldwide, with estimates of value-at-risk (VaR) oscillating between 14% and 19% of net income annually (Bouveret 2018: 20-21). In a hostile digital environment, cybersecurity controls may be quickly overwhelmed by unexpected cyber-risks. Cyber-resilience – "the ability to continuously deliver the intended outcome despite adverse cyber events" (Björk et al., 2015: 312) – is then critical to ensuring organizational survival.

The literature emerging on cyber-resilience comes primarily from the field of computer science, where the main research questions involve identifying the engineering features that make cyber-systems more robust and the metrics that can be used to evaluate their capacity to endure (Bodeau and Graubart, 2011; Linkov et al., 2013). A more holistic approach is needed to explore what kind of preparation, response, recovery, and adaptation activity is needed to enhance an organization's cyber-resilience (The National Academies, 2012). Using qualitative data from a sample of 44 cybersecurity professionals in 28 financial sector organizations in 5 countries (Canada, the UK, the US, France, and the Netherlands), this research describes the organizational measures that foster cyber-resilience in the financial sector. Our general objectives were to learn what works, what does not, and what constraints must be overcome in the process from those who implement cyber-resilience on a daily basis.

For financial institutions, the three most salient dimensions associated with cyber-resilience practices are the sense attributed to cyber-risks, recognizing their inherent uncertainty; the effectiveness of the organizational strategies used to prepare for and mitigate cyber-shocks; and the adaptive outcomes that result from these incidents

SENSEMAKING, CYBER-RISKS, AND THE INSTABILITY OF DECISION-MAKING PROCESSES

Responding to risks requires understanding what is happening. With cyber-risks, framings that make sense of events need to be developed immediately in environments of uncertainty, crisis, and urgency. However several problems can obstruct sensemaking processes and constrain cyber-resilience practices. The first obstacles are related to the features that differentiate cyber-risks from more conventional forms of risk. Cyber-risks are "manufactured" by adversaries and there is very little previous experience available to help understand how to deal with them. As well, these sudden and destabilizing shifts emerge from an ocean of noisy data. Some organizations, for example, have to deal with more than a trillion cybersecurity events per year. The dynamic nature of cyber-risks can also destabilize sensemaking processes during the different stages of an adverse event: respondents recalled many instances where what was initially identified as a fairly minor incident quickly escalated into a much more complex crisis that unfolded over many months. Cyber-risks are often difficult to contain, generating risk-cascades that can quickly amplify a crisis. They may also be incompletely understood due to the secrecy that often envelops the management of incidents.

Not all sensemaking challenges can be attributed to the external pressures of a fast-changing risk landscape. The second source of tension originates in the contested rationalities (or sensemaking frames) between the operational requirements of a business and creating cyber-resilience. To resolve this tension, cybersecurity professionals emphasize the importance of communication. They are mindful of their users' business needs, incorporate these into their risk management mandate, and are careful how they communicate both their mandate and their strategies.

Finally, the third source of sensemaking tension originates from regulators, whose oversight activities generate geographic and temporal pressures. Financial institutions must consolidate regulatory variations into their sensemaking processes to ensure they remain compliant across the whole regulatory spectrum, which introduces an additional level of complexity. As well, the time required to develop a sensemaking frame can be decreased by requirements that the nature and scale of cyberattacks or data breaches be disclosed to the public quickly. This can lead to unexpected and detrimental outcomes as 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 the significance of a crisis (from benign to severe). Institutions forced to make their sensemaking processes transparent in a shorter timeframe may end up providing conflicting information about what occurred, which can erode public trust.

ORGANIZATIONAL PRACTICES OF CYBER-RESILIENCE

Participants often used the "muscle memory" analogy to convey the principles that guide their cyber-resilience practices. Mindful of the intrinsically unpredictable nature of cyber crises, they emphasized the development of general resources and practices that can be adjusted quickly.

MAPPING OF CRITICAL PROCESSES

Planning for cyber-resilience generally starts with comprehensive mapping of the critical functions that a financial institution must recover in case of an extreme adverse event. Such mapping exercises are not new but in the past were often segmented around individual risks, which made it more difficult to uncover interdependencies between critical services. This situation is changing in an environment where the complete loss of IT resources is a possibility, and where different teams must be ready to coordinate their efforts quickly to restore access to markets and resume services to customers. Mapping is not limited to internal processes but must also extend to third parties, which can complicate matters if the latter are reluctant to share sensitive information.

PLAYBOOKS

Mapping assessments are combined with intelligence about the threat landscape to design scenarios of possible adverse events and create response playbooks. The financial institution for which one of our respondents worked maintains sixteen cybersecurity playbooks. These are reviewed every quarter, which can lead to the incorporation of new scenarios to deal with new modes of attacks. However, not all participants were so well prepared and a few had just completed their first cyber-specific playbook or were in the process of developing it. Playbooks take time to develop and often involve several rounds of consultation and testing.

Several respondents warned against over-reliance on playbooks, which cannot possibly anticipate all the surprises encountered in real-life incidents. They highlighted that a cyber-resilient organization must be able to deviate from a playbook—sometimes radically—to adapt quickly to unexpected conditions.

REDUNDANCY AND DIVERSITY

Two technical features usually associated with cyber-resilient systems are redundancy and diversity (Bodeau and Graubart, 2011; Zhang et al., 2016). While redundancy refers to the availability of multiple instances of a particular resource, diversity references the existence of heterogenous resources that can be deployed to minimize exposure to a single type of risk. Both involve "the ability to quickly substitute technologies" and are often identified by practitioners as a "suspenders and belt approach".

THE HUMAN FACTOR

The importance of the human factor as a source of cyber-resilience was highlighted by the most experienced respondents, who often reminded us that people trump systems and procedures when dealing with an extreme cyberattack. When asked to outline what personal traits were particularly useful for those in central roles in cyber-resilience activities, participants mentioned that the best performers in their incident response teams display higher than average curiosity, creativity, and flexibility, which gives them the ability to identify patterns hidden in large amounts of information, to deviate from established procedures (or playbooks) in novel situations, and to quickly improvise new solutions. While not reckless, they are comfortable with imperfect decision-making environments and are not prone to the "startle effect" that can lead to delays, panic, and even paralysis (Staal, 2004). They are good communicators who know how to translate technical approaches in ways that can be understood by those in the organization and they can explain the reasons behind inconvenient or drastic measures. They are also good listeners who can integrate multiple—and sometimes contradictory—perspectives into their decisions.

To avoid boredom and attrition for those on their cyber-resilience teams, some participants have implemented cross-training programs that expose employees to the work of colleagues in different domains, broadening their capacity to identify and address emerging problems. Others use rotation systems in which employees take different positions on the team. Effective cyber-resilience professionals have a lot in common with jazz musicians, who learn to create musical pieces from minimal structures in turbulent task environments where they must balance their individual skills and effective group coordination (Bastien and Hostager, 1988).

TRAINING AND SIMULATIONS

It would be misleading, however, to suggest that only a handful of naturally gifted operators can be responsible for the overall cyber-resilience of an organization. Just like good jazz ensembles who develop their mastery over years of practice, the performance of cyber-resilience teams is improved by focused training and incident rehearsals. Almost all participating organizations conduct simulations and tabletop exercises that try to recreate the conditions of a cyberattack as realistically as possible so that employees in a broad range of functions can familiarize themselves with existing playbooks and practice response and recovery protocols. The most mature financial institutions conduct up to half a dozen simulations per quarter at various levels (head office, specific business lines, regional branches).

Simulation activities are resource-intensive to design and to run, which explains why their quality varies greatly. They sometimes lack the level of detail that allows employees to practice tasks in stressful situations, or they rely on scenarios that are not sufficiently challenging for participants. And they can also be seen as a distraction by senior decision-makers, who send delegates rather than attending themselves, thereby defeating the purpose.

Despite a general consensus among respondents about the need to conduct training and simulation exercises to enhance the cyber-resilience of their organizations, the approaches advocated remained conventional. Very few participants had implemented the more focused evidence-based strategies used by response teams in emergency medicine, the military, or the nuclear industry to improve the five resilience skills outlined in the table below, with the exception of knowledge-sharing activities, which are well developed in financial institutions.

Skills	Activities and outcomes
Adaptability	Perturbation training: counteracts procedural rigidity associated with routine team interactions, for example by disabling technologies critical to incident response during training exercises. Stress exposure training: prepares individuals and teams to maintain effective performance in high-stress situations. Diversified preparatory activities: encourages enhanced adaptive skills though contingency planning, war-gaming, and frame-switching exercises to help trainees think through a broader sample of attack strategies.
Problem-solving	"Thinking like a commander" method: increases the number of domain-specific thought habits used automatically by team members during a crisis and enhances the collective cognitive performance of teams. Team Coordination Model: develops shared mental models in team members to improve team collaboration.
Communication	Mnemonics protocols: improves the quality of handoffs by making exchanges of information clearer and more concise, reducing opportunities for mistakes. Structured communication briefings: reduces communication breakdown and improve understanding of upcoming tasks. Strategy meetings: improve the sharing of mental models and team coordination.
Trust-building	Psychological safety climate: reduces power differences and increases "speaking-up" behaviours, leading to improved learning and a reduction in errors. Shared identity building: promotes higher levels of rapid trust.
Knowledge-sharing	Cross-training: increases sharing and accuracy (who should do what and when) of mental models, leading to improved communications and coordination. Role identification practices: helps team members better understand their colleagues' capabilities and expertise. Guided team self-correction training: helps teams identify and fix performance problems. Structured after-action reviews: improves processes by reviewing recent performance events and providing individual and collective feedback.

Source: Steinke et al., 2015

INTERNAL AND EXTERNAL NETWORKING

The professionals we interviewed relied on dense internal and external organizational networks to improve the speed and effectiveness of communication flows. Despite the natural tendency of many financial institutions to segment expertise and require secrecy when crises unfold, many respondents highlighted the benefits of having developed bridging capital and weak ties throughout the organization to facilitate dealing with adverse events (Granovetter, 1973). Internally, this means embedding security workers inside business units to improve their understanding of the culture and technological constraints or establishing "fusion centres" blending various security units (fraud, cyber, physical, business continuity) to consolidate their sensemaking and decision-making capacities. Awareness campaigns and cybersecurity "ambassador programs" can also contribute to creating internal networks that can be activated in times of crisis. For instance, in a different sector, Netflix has launched a Reservist Program in which auxiliary crisis managers are trained to distribute and scale incident response expertise across the organization (Joshi, 2020).

External networks play a crucial role in organizational cyber-resilience. Financial institutions are embedded in a dense web of business partnerships and their sensemaking and incident response processes rely on the ability to collect information quickly from outside the organization and to access "surge capacities" while limiting bureaucratic or contractual friction. Third parties, especially those providing IT services, require particular attention. Prompted by regulatory requirements, financial institutions are dedicating resources to assess the cyber-resilience of third parties and to monitor how this impacts their own posture. However, as some respondents noted, these processes can expand to unsustainable levels: third parties have their own third parties, not always identified before an incident, and modelling risk-cascades across organizations can quickly become extremely complex.

Many participants extolled information sharing as one of the most effective strategies to stop attacks that could destabilize the financial system when an industry-wide vulnerability is discovered. One participant used the medical analogy of inoculation, although he acknowledged that this approach can protect only against known threats.

External networks conducive to effective information sharing involve informal and formal structures that extend from small peer groups to large industry consortiums. One respondent estimated that the not-for-profit information sharing initiatives his bank participates in gave him access to threat indicators around three and a half weeks earlier than the notifications he received from commercial feeds. Respondents stressed that fully benefitting from these external resources required developing trust and building and maintaining relationships over time so that people have accumulated enough social capital to "call and ask for favours when they need to".

LEARNING TO ADAPT

The ultimate goal of resilience is not mere survival until the next crisis but adaptation to a dynamic environment to achieve a new state of equilibrium. Respondents discussed three different forms of adaptation associated with major adverse events.

The first form of adaptation is voluntary and deals with the learning that takes place after a major unexpected incident or a routine incident that was handled poorly. The lessons learned during these events are usually captured in post-incident reviews and to ensure that all the information needed is collected, including the most sensitive and embarrassing, certain respondents have adopted a "no-fault learning" approach to create a safe environment for those involved.

The second form of adaptation is guided by cybersecurity standards and their cyber-resilience components. Standards gradually incorporate the lessons learned from past incidents and then help propagate best practices, raising the bar for everyone. However some respondents suggested that standards might introduce a false sense of resilience. As well, because of their complexity (often hundreds of criteria or controls to implement), it is almost impossible for an organization to be fully compliant. Standards are also, by definition, rigid and therefore ill-suited to help deal with the unknown. Some respondents believed that their static nature can even become a source of vulnerability as dynamic attackers can use them to calibrate how much effort is needed to overcome a particular system.

The third form of adaptation is forced and involves regulatory activity. Certain jurisdictions are becoming much more directive about cyber-resilience and while a majority of participants preferred principles-based regulatory requirements out of concern that excessively detailed and prescriptive approaches would erode their flexibility, others felt that detailed regulations mandating specific measures could accelerate adaptation. Prescriptive regulations that force a whole industry to adapt can overcome the competitive barrier faced by early adopters and lead to support for investments that would have been much more difficult to justify otherwise.

CONCLUSION

Cyber-resilience appears to be highly contextual and depends on a variety of unique factors, such as the history, size, business culture, international footprint, IT priorities, regulatory environment, and leadership style of each organization. There is no ideal model for cyber-resilience, only customized and tailored practices that can deliver improved levels of reliability and survivability for an organization confronted with severe turbulence.

Cyber-resilience cannot be reduced to business continuity and disaster management. These conventional response models are designed to deal with predictable and stable risks, such as natural disasters, and while climate change means that the frequency and impact of such disasters will increase over the next decades, they are not the result of actions by innovative, thinking adversaries.

None of the professionals we interviewed mentioned a problem that can seriously hinder the preparedness and crisis management capacities of financial institutions — individual and collective cognitive biases. Cybersecurity professionals have not yet integrated these heuristic traps into their risk-management models, despite growing evidence that they can lead to errors of judgement and undermine the resilience of organizations. Ten heuristics deserve particular attention and should lead to remedies informed by the principles of behavioural economics.

Heuristic	Description
Myopia bias	The tendency to focus on present benefits rather than future harms.
Amnesia bias	The tendency to quickly forget the lessons of past disasters.
Optimism bias	The tendency to minimize the impact an adverse event can have on us, even if we recognize it will affect others.
Inertia bias	The tendency to remain passive when confronted with high levels of uncertainty.
Simplification bias	The tendency to consider only convenient factors when confronted with complex risks.
Herding bias	The tendency to align with the actions of others rather than rely on a more systematic analysis of the situation.
Familiarity bias	The tendency to rely on past actions as guides.
Consistency bias	The tendency to maintain an approach once an initial decision about something has been made, even if circumstances change.
Expert halo bias	The tendency to assess leaders' skills based on an overall positive impression rather than specific information.
Social facilitation bias	The tendency to take more risks when other people are present.

Sources: McCammon, 2004; Meyer and Kunreuther, 2017

This research project draws on individual experiences with highly disruptive cyber-shocks in financial institutions to identify practical insights into the benefits and limitations of the most common cyber-resilience activities. But this qualitative methodology can capture only a limited sample of the most memorable incidents experienced by each of the cybersecurity professionals who agreed to be interviewed. A more systematic approach based on information about tens—and possibly hundreds—of cyber-incidents, whose causes, responses, and outcomes were recorded using a set of predetermined criteria, would enable us to make stronger inferences about the efficiency and effectiveness of specific cyber-resilience measures, correcting the current situation in which there are no such cyber-resilience metrics available to assess how best to direct our cybersecurity investments.

REFERENCES

[1] Bastien, D. T., & Hostager, T. J. (1988). Jazz as a process of organizational innovation. Communication Research, 15(5), 582-602.

[2] Björk, Fredrik, Henkel, M, Stirna, Janis, and Zdravkovic, J. (2015), "Cyber resilience – Fundamentals for a definition", in Rocha, Alvaro, Correia, Anna Maria, Costanzo, Sandra, and Reis, Luis Paulo (eds.), New contributions in information systems and technologies, Springer, London, pp. 311-316.

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

[4] Bouveret, Antoine (2018), Cyber risk for the financial sector: A framework for quantitative assessment. IMF Working Paper, WP/18/143: 1-28.

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

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

[7] Linkov, I., Eisenberg, D., Plourde, K., Seager, T., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), 471-476.

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

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

[10] 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.

[11] Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J, Repchick, K. M., Zaccaro, S. J., Dalal, R. S., & Tetrick, L. E. (2015). Improving cybersecurity incident response team effectiveness using teams-based research. IEEE Security & Privacy, 13(4), 20-29.

[12] The National Academies. (2012). Disaster resilience: A national imperative. The National Academies Press.

[13] Zhang, M., Wang, L., Jajodia, S., Singhal, A., and Albanese, M. (2016). Network diversity: A security metric for evaluating the resilience of networks against zero-day attacks. IEEE Transactions on Information Forensics and Security, 11(5), 1071-1086.