THE CYBER-RESILIENCE OF FINANCIAL INSTITUTIONS:

A PRELIMINARY WORKING PAPER ON SIGNIFICANCE AND APPLICABILITY OF DIGITAL RESILIENCE

Author: Benoît Dupont
Université de Montréal

GLOBAL RISK INSTITUTE

EXECUTIVE SUMMARY

Recent headlines about cyberattacks and massive data breaches are revealing the fragility of the digital infrastructure and the impossibility of assuring the integrity of computer systems, even for organizations such as financial institutions that maintain the most mature cybersecurity programs. In this context, the concept of cyber-resilience offers an attractive complement to the 'predict and protect' paradigm that has dominated information security over the past few decades.

Cyber-resilience : beyond the 'predict and protect' paradigm

At a general level, resilience can be defined as the capacity to withstand, recover from, and adapt to external shocks. The main tenet of resilience is not to be able to predict precisely the future in order to protect against possible harm. Instead, it seeks to develop a qualitative capacity to design and operate systems that can withstand adverse events, no matter how unexpected they may be.

Resilience is broader in scope than risk management, as it incorporates the ability to respond effectively to unpredictability and surprise and to maintain high levels of performance under the most hostile conditions. Resilience is a concept grounded in a multiplicity of theoretical and practical traditions, explaining why it is surrounded by a certain level of ambiguity: for some, it entails the capacity of a system to withstand a shock and return to its original state, while for others it implies an evolutionary process leading to adaptation and a new state of equilibrium.

At a more practical level, cyber-resilience is often reduced to the engineering properties of computer systems that can resist sophisticated cyber-attacks, or to the incident-response methodologies that are needed to respond to these attacks. This paper argues that the cognitive and social dimensions of cyber-resilience should be paid the same level of attention.

The need for cyber-resilience in the financial sector

The concept of cyber-resilience is of particular relevance to financial institutions that must learn to coexist with a broad range of interdependent disruptive hazards such as technical failures, human errors, and natural disasters. The digital assets of financial institutions are also under constant attack by cybercriminals, government hackers, hacktivists, and disgruntled employees who attempt to infiltrate or cripple computer systems. This unprecedented level of malicious activity can have a very significant impact on the most robust organizations.

Various assessments are available on the impact cyber-disruptions have on financial institutions:

- *The Ponemon Institute evaluated the average direct and indirect costs of a data breach at $3.86 million per incident in 2018;*
- *Statistics Canada's 2017 Survey of Cyber Security and Cybercrime estimated that the average cost of recovering from an impactful cybersecurity incident reached CAD$140,957 per event for large financial and insurance organizations;*

- *An International Monetary Fund study performed in 2018 with data provided by the Operational Riskdata eXchange Association (ORX) found that aggregate losses generated by cyber-attacks at 7,900 banks worldwide reached 9% of net income with value-at-risk oscillating between 14% and 19% of net income.*

The implications for financial institutions are alarming and warrant adding cyber-resilience as a key tool in their risk-management toolbox.

The five dimensions of cyber-resilience

The literature contains many detailed models that provide a comprehensive list of the elements allowing organizations to achieve cyber-resilience. They usually belong to one of the following five high-level dimensions:

- *Cyber-resilience is dynamic: it requires thinking about catastrophic incidents through an extended temporal lens that includes measures implemented before, during and after an event. Cyber-resilience implies a near-permanent cyclical process of preparation, mitigation and adaptation that can prevent an organization from falling down the collapse ladder;*
- *Cyber-resilience is networked: it relies on a dense network of intra- and interorganizational linkages that are characterized by strong trust and can be activated on short notice in an emergency to provide additional resources and expertise;*
- *Cyber-resilience is practiced: regular rehearsals of crisis scenarios enable organizations to develop the improvisation skills that are needed to operate in turbulent environments. They also help overcome the startle effect that impairs incident-response;*
- *Cyber-resilience is adaptive: it allows organizations to learn from their adverse experiences and to enhance their level of preparedness against future hazards. The most cyber-resilient organizations can turn disasters into opportunities for reinvention;*
- *Cyber-resilience is contested: it frequently collides with other organizational priorities that are also legitimate (such as profitability) and therefore requires compromises between efficiency and adaptability. Cyber-resilience can also be hindered by one of the six following biases: myopia, amnesia, optimism, inertia, simplification, and herding.*

Institutionalizing cyber-resilience

Beyond the individual approaches adopted by organizations to improve their cyber-resilience, three types of institutional approaches are also gaining in popularity in the financial sector: marketing, standardization, and regulation. Each approach is executed by a particular group of institutions that pursue different goals and can leverage a broad set of resources that range from mere persuasion and incentivization to coercion:

Marketing cyber-resilience: a thriving security and consulting industry is strongly promoting cyber-resilience as the future of cybersecurity. Most of the reports produced by these companies promote a narrow form of cyber-resilience that focuses on incident detection and response. Most industry reports adopt a framework derived from well-established cybersecurity standards, while very few disclose the evidence-base supporting their recommendations;

Standardizing cyber-resilience: the two standards that dominate the field of cybersecurity – ISO's 27000-series and NIST's Cybersecurity Framework – include measures compatible with a cyber-resilience approach. More specialized cyber-resilience standards have also been proposed by the Software Engineering Institute (CERT Resilience Management Model), Europe's ENISA (cyber-resilience measurement frameworks), or the World Economic Forum (cyber-resilience framework for boards of directors);

Regulating cyber-resilience: regulatory agencies that oversee financial institutions have developed a broad range of assessment and compliance tools aimed at enhancing cyber-resilience. The Bank for International

Settlements, the European Central Bank, and national regulators in the UK, the US, the Netherlands, Denmark, Australia and Canada have all increased their cyber-resilience expectations for financial firms, resorting to more prescriptive approaches on the compliance pyramid.