The cyber-resilience of financial institutions: A preliminary working paper on significance and applicability of digital resilience

Benoît Dupont, Université de Montréal

Cyber-resilience has recently become one of the most hyped concepts in discussions of cybersecurity, despite – or perhaps because of – its nebulous meaning, which makes it difficult to rigorously define and measure. Its popularity is undoubtedly linked to the numerous headlines about cyberattacks and data breaches that dot the frontpages of newspapers and technology websites, trumpeting information about new and massive hacks that reveal the fragility of our digital infrastructures and the incapacity of organizations to protect the personal data we entrust to them. Even the most tech-savvy and security-conscious organizations are not immune from catastrophic cybersecurity failures. Consider the following two cases: in October 2017, the New York Times and the Washington Post reported a story straight out of a John Le Carré novel, in which it was reported that Israeli spies had infiltrated the systems of the cybersecurity company Kaspersky and were alleged (it is always difficult to disentangle facts from manipulation in intelligence affairs) to have been able to monitor hacking efforts by their Russian counterparts, who were using the telemetry capacity of the company's antivirus product to search for sensitive documents from American intelligence agencies (Nakashima 2017, Perlroth and Shane 2017). Leaks concerning hacking tools developed by the CIA and NSA, although unrelated to this particular incident, seem to confirm that this approach is occasionally successful. A few months later, in a less publicized report, the Dutch internal intelligence agency (the AIVD) disclosed that it had hacked the computer network of a building from which a team of Russian hackers in their country's foreign intelligence service (the SVR) had infiltrated the email accounts of US State Department and Democratic National Committee employees. The digital infiltration, which lasted about a year, was so complete that the Dutch team was able to access the building's CCTV camera video feed and identify the individuals who entered the room from which the hackers operated (Gallagher 2018). These two stories illustrate the impossibility of guaranteeing the integrity of computer systems, even for organizations that maintain the highest operational security standards and have what are arguably the most mature cybersecurity programs.

In this context, the concept of cyber-resilience offers an attractive complement to the 'predict and protect' approach that has dominated information security over the past few decades. Confronted with the bleak realization that no digital system can assure impregnability in the face of constant assaults, organizations are coming to terms with the need to design processes and technologies that provide help after catastrophic attacks. To borrow a powerful metaphor, organizations, once they accept the fact that they operate in a permanent state of cyber-vulnerability while deriving considerable productivity benefits from the technologies that also threaten their existence, must learn to "survive on a diet of poisoned fruit" (Danzig 2014). Far from being unique to the cyber-domain in general or financial institutions in particular, the dilemma of how to effectively respond to and manage disruptions caused by unpredictable adverse events that have the potential to destabilize—and ultimately obliterate – has been a central problem for all complex ecological, social, organizational, and technical systems. The answer is resilience, which will be defined for the moment as the capacity to withstand, recover from, and adapt to external shocks. In the words of one of the founding fathers of the concept (C.S. Holling, a Canadian ecologist), this shift of perspective "does not require a precise capacity to predict the future, but only a qualitative capacity to devise systems that can absorb and accommodate future events in whatever unexpected form they may take" (Holling 1973: 21).

It is important to differentiate resilience from risk management, although they are intertwined. Risk management involves quantification of the probability and severity of risks, making it possible to support decisions about the most appropriate strategy to address them, such as inaction, avoidance, reduction, transfer, or insurance (Button 2008). Resilience is broader in scope and "is essential when risk is incomputable, such as when hazardous conditions are a complete surprise or when the risk analytic paradigm has been proven ineffective" (Linkov et al. 2013: 10108). Resilience takes over from risk management when the latter has been ineffective at shielding an organization from disruptive threats and implies a constant cycle of activities and responses – starting well ahead of an adverse event and concluding well after the event has ended – to implement the adaptive measures needed to counter the next unpredictable shock. In other words, while risk management in cybersecurity is concerned with the minimization of hazards, cyber-resilience seeks to maintain high performance levels irrespective of the presence or absence of hazards (Bagheri and Ridley 2017: 2). This explains why "an organization can have cybersecurity without being resilient, but not the other way around" (Conference Board of Canada 2018: 12)[1].

The need to apply resilience thinking and practices to the digital ecosystem may seem superfluous, since the internet was designed to be a resilient distributed system that could persist in the worst possible situations, such as a nuclear strike (Castells 2001). But this technical resilience, which is limited to one of the basic layers that constitute the internet (Kuehl 2009) and ensures that the routing of data packets can follow multiple alternative paths, reaching recipients even if a nontrivial number of connecting nodes are removed, was never intended to provide a reliable level of security for a world in which every possible social activity and business transaction has migrated online, billions of devices are connected to the web, and people, processes, and policies are routinely and successfully exploited by malicious actors. Given the unprecedented scale and severity of cyber-risks, cyber-resilience must extend beyond the global infrastructure of the internet, focusing instead on the individual organizations that have come to depend on it to fulfill their role.

[1] For an alternative perspective, in which cybersecurity is seen as broader than cyber-resilience, see Bodeau and Graubart (2011: 6).

While the concept of cyber-resilience certainly appears alluring when confronted with such an uncertain and unpredictable environment, it has important limitations that must be acknowledged and surmounted if it is to retain its conceptual edge. The main issue is that the multidisciplinary roots of resilience can prove to be as much a curse as an asset: they provide a rich theoretical toolbox of associated concepts from which insightful perspectives might be translated to the cyber-domain but the lack of a unified definition and the diversity of approaches they entail foster a level of fragmentation that prevents resilience practitioners and policy makers from developing a generalizable approach (Linkov et al. 2013: 10108, Davidson et al. 2016: 1, Bagheri and Ridley 2017: 3). At a fundamental level, for example, there is some disagreement over the true meaning of resilience: 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 (Bagheri and Ridley 2017: 3). At a more practical level, cyber-resilience, rather than being understood as all-encompassing, has sometimes been approached narrowly. For example, company reports, while extolling its virtues, often confuse cyber-resiliency with the incident response practices and methodologies with which their authors are familiar and which can be more easily peddled to potential customers. By the same token, the industry standards that have tried to formalize the concept of cyber-resilience are predominantly focused on its engineering aspects and rarely attach as much importance to its cognitive and social dimensions. Resilience too often remains "a rhetorical device with little influence on actual decision making" (Benson and Craig 2014: 780).

This partly explains why many experts are skeptical about the concept of cyber-resilience, dismissing it as merely one of the latest cybersecurity fads to capture the attention of gullible customers. Far from subscribing to this pessimistic interpretation, I believe that resilience thinking can provide a very useful theoretical and practical framework that will help us extricate ourselves from the cybersecurity rut in which we are trapped. This article therefore attempts to address the limitations identified in the previous paragraph by providing a multidisciplinary review of the literature relevant to the study of cyber-resilience in order to understand both its multiple dimensions and the criteria that can be used to facilitate its implementation and measurement. To achieve this objective I look at three important areas: the first section examines the current risk landscape faced by the financial sector and highlights why a shift to a resilience-oriented mode of thinking is needed. The second section explores the multiple meanings of resilience through its uses in various disciplines, pointing out the theoretical dimensions that seem particularly relevant to cybersecurity. Finally, the third section examines three institutional approaches associated with efforts to make cyber-resilience more practical and systematically applicable for the financial sector.

1. The need for cyber-resilience in the financial sector: the inevitability and disruptiveness of cyberattacks

Cyberattacks have become an inevitable digital hazard that even the most mature financial institutions will never be able to completely eliminate, no matter how much they invest in the latest security technology (Conference Board of Canada 2018). In order to better grasp why cyber-resilience has become such a pressing necessity, it is useful to look at some of the most recent disruptive incidents that have targeted financial institutions. Of particular interest are the diversity of motives behind these attacks, the variable levels of technical expertise displayed by those who plan and execute them, and the individual and collective impacts on victimized organizations. These considerations clarify why, given such a complex and unpredictable risk landscape, the traditional security approach, which rests on the untenable promise of being able to prevent or stop cyberattacks, is futile and should be folded into a more realistic and sober paradigm in which organizations learn to coexist with disruptive hazards (Tedim and Leone 2017).

The nature and origins of cyberattacks against financial institutions

Because of their increasing dependence on digital technologies, modern organizations in general, and financial institutions in particular, are vulnerable to the cascading effects of technical failures, human mistakes, and natural disasters (Gorniak et al. 2011: 5). The digital assets of financial institutions are also attacked by cybercriminals, government hackers, hacktivists, and disgruntled employees, who attempt to infiltrate their computer systems and steal valuable information. The unprecedented level of malicious activity and the constant barrage of attacks create unique challenges for cybersecurity professionals.

Cybercriminals motivated by financial gain pose the most obvious and persistent threat to the financial institutions that act as gatekeepers to the payment system and its electronic instruments. A recent assessment published by the SWIFT Institute describes the growing number, complexity, and sophistication of cyberattacks against bank clients, business customers, and core systems, reflecting the quick pace of innovation among online offenders (Carter 2017). This criminal ingenuity has been greatly aided by the availability of powerful malware tools on underground markets that also provide a support infrastructure that enables even actors with limited technical skills (Holt 2012, Sood and Enbody 2013, Lusthaus 2018), as well as, more recently, the leakage of nation-state hacking tools that can be exploited by petty criminals (Brewster 2017, PandaLabs 2017). Cybercriminals are also launching more systematic and targeted attacks. The 'London Blue' group, operating out of Nigeria and the UK, has assembled a database of 50,000 financial institution employees who can be contacted in business email compromise scams. Profiles of potential targets are carefully considered to increase the chances of success: 71% are CFOs, 12% finance directors, 9% controllers, 6% accountants, and 2% executive assistants (Agari 2018). Some cybercriminal networks have managed to leverage the expertise of cybersecurity insiders, as in the case of the 'Silence' group that has targeted banks in more than 25 countries. One member of this cybercrime ring has demonstrated a high level of familiarity with the penetration-testing techniques used by white hat hackers, as well as having access to non-public malware samples usually exclusively available to security companies and seeming to be very knowledgeable about the operations of ATM systems

(Volkov 2018). Such defections by cybersecurity experts can seriously undermine the cyber-resilience of financial institutions.

Financial institutions have also had to fend off state-sponsored cyberattacks. Since 2016 a group of hackers known as the Lazarus Group and associated with the North Korean regime has launched aggressive attacks against central and retail banks around the world. In 2018, a criminal complaint lodged by the US Department of Justice against a North Korean citizen accused of working on behalf of his government revealed that the Lazarus Group had defrauding the Central Bank of Bangladesh of $81 million in 2016. Between 2015 and 2018 the group had also gained access to bank systems in Vietnam, the Philippines, Africa, Asia, Europe, and North America and attempted to illegally transfer more than a billion dollars (United States of America v. Park Jin Hyok 2018). It has also infected financial networks that handle ATM transactions and has been able to extract tens of millions of dollars from banks in more than 30 countries (Security Response Attack Investigation Team 2018). These attacks, from a group that has also conducted espionage operations against defense and government targets, are characterized by a high level of sophistication and persistence and seem to be motivated by the need to fund a regime weakened by international economic sanctions. In contrast, the extended distributed denial of service (DDoS) campaign that hit the US financial system between December 2011 and mid-2013 and has been attributed to the Iranian government appears to have been driven by a retaliatory rationale. Responding to a cyberattack by the US and Israel against its uranium enrichment program and to its removal from SWIFT's global financial network, Iran targeted 46 US financial institutions in an attempt to damage the US economy by preventing hundreds of thousands of businesses and individuals from accessing their accounts (United States Department of Justice 2016).

State-sponsored actors generally have access to more resources and expertise than their criminal counterparts and can therefore be challenging to defend against. They can also introduce additional legal uncertainty for their private sector targets, as illustrated in a 2018 lawsuit initiated by the Mondelez food conglomerate against its insurer, Zurich, which refused Mondelez's 100-million-dollar claim on the grounds that the ransomware attack to which it had fallen victim has been caused by a government-sponsored actor and could therefore be considered an act of war, explicitly excluded in the contract (Evans 2018).

Ideological motivations have led hacktivists to plan attacks against banks and financial institutions that epitomize the elites they oppose. In December 2010, the Anonymous collective launched a number of DDoS attacks against financial institutions that refused to process donations to WikiLeaks following the release of US diplomatic cables, briefly bringing down Visa and MasterCard's public websites (Coleman 2014). In May 2016, a new wave of attacks, under the Operation Icarus label, was launched against financial institutions and managed to temporarily bring down the websites of the Bank of Greece and the Bank of Mexico (Crosman 2016). Operation Icarus was revived in December 2018 and its victims included the Central Bank of Albania, the Bank of Mexico, and the Central

Bank of the Bahamas (Security G33k 2018). However none of those attacks managed to disrupt the financial institutions' internal production and trading infrastructures as they were focused on static websites whose availability does not affect the institution's ability to deliver services and clear transactions. The tools and tactics used by hacktivists have so far been rudimentary, but their capacity to embrace more innovative approaches should not be discounted. More sophisticated actors could also take advantage of the noise and distraction created by such attacks—usually announced ahead of time—to conceal their own efforts.

The harm caused by threats from insiders (employees or contractors) is more difficult to predict and assess because of their diverse motives (financial, psychological, political) and access to critical systems and data (Randazzo et al. 2005, Warkentin and Willison 2009, Raytheon 2015, Miller and Trotman 2018). However, the available statistics suggest that this risk remains marginal. The report on the 2018 Verizon data breach estimated that internal threat actors were responsible for only 7% of breaches involving financial and insurance victims (Verizon 2018: 31). The ORX database, which aggregates a dataset of incidents contributed by more than eighty financial institutions, shows even lower numbers: out of almost 360,000 operational loss events recorded in the database between 2012 and 2017, only 1.7% (6,086 incidents) involved internal fraud, which resulted in a loss of 3.1 billion euros or 2% of overall operational losses for that period (ORX 2018: 6-7).

The impact of cyber-disruptions on financial institutions

Cybersecurity experts often refer to highly publicized cyber-incidents that have made the headlines over the past few years (Bank of Bangladesh, Equifax, JPMorgan, Tesco Bank, etc.) to illustrate the disruptive potential of adverse events on financial institutions. Horror stories abound of executives losing their jobs, massive fines imposed by regulatory authorities, civil litigation of monstrous proportion, lasting reputational damage, and costly rebuilding efforts (FCA 2018, Forrest 2018, Koenig 2018, Newman 2018). These compelling narratives may encourage some financial institutions to invest more heavily in cybersecurity and cyber-resilience, but they fail to provide a systematic assessment of the true impact of cyber-risks and, by extension, of their capacity to threaten the existence of an organization or to devastate an entire industry.

One approach taken by consulting firms attempting to measure the costs associated with cyber-incidents is to survey a sample of cybersecurity professionals. The Ponemon Institute conducts this type of study with the financial backing of industry sponsors such as IBM. Its 2018 study of the cost of a data breach analysed a survey completed by more than 2,200 respondents from 477 organizations and fifteen countries (16% of whom worked in financial institutions) who were asked to estimate the monetary impact of recent incidents on their organization, including both direct and indirect costs (Ponemon Institute 2018a: 6). Average total cost reported was $3.86 million per data breach (Ponemon Institute 2018a: 3). However the lack of representativeness characteristic of such samples and the inevitable biases introduced make it difficult to generalize this type of results. Surveys conducted by national statistical agencies – such as the one conducted in Canada in 2017 – provide more robust insights into the impact of cyber incidents on organizations (Statistics Canada 2018). Their samples are often large enough to be representative (12,600 companies surveyed in this instance) and the legal requirement to answer the official questionnaire produces very high response rates (85% in our example). In contrast to the Ponemon Institute study, the average cost of recovering from a cybersecurity incident was estimated at CAD$140,957 per event for large financial and insurance organizations, a significant number but definitely not an existential risk. The average annual cybersecurity costs for financial and insurance businesses amounted to CAD$3.9 million for large financial and insurance companies (Statistics Canada 2018).

The ORX consortium, mentioned above, could also be a useful source of anonymized incident-based data except that its coding framework does not seem to include a specific category for cyber-risks, which are instead distributed over three categories – external fraud, internal fraud, and technology and infrastructure failure – that also include adverse off-line events (ORX 2018: 6). Despite these limitations, Bouveret (2018) used a dataset of publicly available data maintained by ORX that covered 341 cyber-incidents between 2009 and 2017 to assess the impact of such incidents on financial institutions. He considered three types of events: online fraud (43%), data breach (34%), and business disruption (23%). His findings indicate average losses for financial institutions of $66 million, with the median at $4.7 million (Bouveret 2018: 18). Using actuarial techniques, Bouveret estimates that aggregate losses generated by cyber-attacks at 7,947 banks worldwide amount to $97 billion yearly (9% of net income), with value-at-risk (VaR) oscillating between $147 and $201 billion (14% to 19% of net income) (Bouveret 2018: 20). When a contagion effect is introduced (the propensity of attackers to target multiple institutions in the same field once they have identified a vulnerability and a high level of interconnection between institutions), projected aggregate losses increase by 20% to reach between 18% and 24% of net income. The most severe scenario suggests an aggregate yearly loss of 51% of net income (Bouveret 2018: 21). While the author readily acknowledges the incomplete and preliminary nature of his model, the implications for financial institutions are alarming and probably explain why financial sector executives rank cyber-risks at their main operational risk concern (ORX 2019), which has led to cyber-resilience becoming a key tool in their risk-management toolbox.

2. Resilience: beyond prediction and protection

Resilience as a general concept has a long history that spans disciplines, from materials engineering to psychology, ecology, urban planning, and computer science to name the most prominent. Although these various approaches share a common set of underlying principles (such as preparation, mitigation, and adaptation) that overlap domains and facilitate transferability, the loose use of the term has also produced some undesirable outcomes, such as loss of precision and fuzziness, that make resilience challenging to define, design, implement, and measure (Manyena 2006: 435, Davidson et al. 2016: 26). There are therefore significant nuances that need to be explored in order to avoid excessive simplification, loss of meaning, or misinterpretation. Recognizing these differences will prevent attempts to transfer analytic approaches that have proved very useful in a particular domain but may be irrelevant to cybersecurity (Holling 1973: 1).

A short history of resilience

The genealogy of the resilience construct is rooted in physics and the material sciences, where resilience denotes the property of a material to absorb energy when subjected to strain and to maintain or resume its original shape or position after being bent, stretched, or compressed (OED Online 2018). By extension, this meaning has been applied in the medical and veterinary sciences to define the natural elasticity of body parts such as the skin, the lungs, or the chest-wall. In these contexts, resilience refers to a limited set of measurable parameters that are defined by their predictability and vary little in time and space; use of the term is recorded as early as the first half of the nineteenth century according to Google Books' Ngram Viewer[2]. In the 1970s the concept's appeal became broader, particularly within the two disciplines that triggered its current popularity – ecology and psychology.

In ecology, Holling's seminal article introduced a more dynamic understanding of the concept of resilience, applying it to situations where a system confronted by profound and unexpected changes could not, unlike materials, be expected to maintain a constant state of equilibrium (Holling 1973: 2). Holling argued instead that the study of resilience should focus on "the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables" (Holling 1973: 14). In practice, persistence is the opposite of stability, which refers to a system's ability to return to a state of equilibrium after disturbance. Persistence can, for example, be achieved in cases of extreme fluctuation in the size of a population and provides lower probabilities of extinction compared to populations that are more stable but less flexible in their ability to absorb environmental extremes. It is important to remember that this perspective on resilience is grounded in ecology, where, in contrast to organizations, the main aim is not necessarily to maximize efficiency but simply to stay in the game. When this framework is transferred to an organizational environment it creates tensions, as, unlike resilient ecological systems, which rely on diversity and variability, the homogeneity that fosters organizational effectiveness does not tolerate high fluctuations and therefore demonstrates lower resilience. In a subsequent article, Holling formalized his thinking on the features – efficiency, constancy, and predictability – that distinguish engineering (or economic) resilience from ecological resilience, which is focused on persistence, change, and unpredictability (Holling 1996: 33). Moving beyond the theoretical intricacies of single-state and multi-stable-state equilibriums, the practical implication of this line of reasoning is that efficiency and resilience are not always aligned. The conditions that produce short-term economic productivity (such as reduced diversity and redundancy, which allow economies of scale and resource optimization) may be detrimental to resilience and

[2] https://books.google.com/ngrams

increase vulnerability (Holling 1996: 38). Although Holling did not intend his work to be generalized beyond the management of ecological systems, his insight is essential for decision makers in other fields, who must realize that achieving resilience requires them to balance conflicting priorities. His ground-breaking contributions have resonated particularly with ecologists, urban planners, and disaster management experts, who have extended them to conceptualize and map the adaptive strategies available to modern societies and their complex—but fragile—socio-technical systems, with particular emphasis on the catastrophic consequences of accelerated climate change (Downes et al. 2013, Davidson et al. 2016). Some have even argued that the concept is so versatile and has become so prominent that "it has helped to unify ecology as a discipline" (Olsson et al. 2015: 7).

Psychology is the second discipline that has made a major contribution to the prominence of resilience. In the 1970s, while ecology was considering the stability, persistence, and adaptation of environmental systems, psychology sought to understand why some individuals and families who find themselves at risk or face a broad range of adverse circumstances (such as poverty, family breakdown, traumatic loss, or natural disaster) seem relatively unaffected and are able to cope and to function normally (Masten 2018), in certain cases emerging even stronger (Waller 2001: 290). Psychology developed the construct of resilience as a way to move beyond its natural tendency to dwell on risk factors and their negative outcomes on mental health, broadening its perspectives to study personal strength, positive forms of adaptation, mitigating factors, and protective influences (Richardson 2002: 309, Masten 2018: 13). Richardson (2002) distinguishes three waves of psychological research on resilience. The first wave identified the personal characteristics and protective factors that support people through adverse life events, creating a long list of individual, family, community, and cultural factors such as self-esteem, effectiveness, problem-solving skills, caring, humor, or a warm personal relationship, to name just a few (Waller 2001: 292). The second wave attempted to understand how these qualities are acquired, while the third wave sought to model the force or motivation that drives a person toward the development or reinforcement of these qualities. This work became instrumental in the development of positive psychology, which eschews the pathologizing of risks to adopt a more holistic approach in which it is understood that the most adverse situations can allow individuals to flourish and imagine creative solutions (Seligman and Csikszentmihalyi 2000). This perspective might be discounted as too optimistic for the harsh realities of our complex world, but, on the contrary, psychological research has found that resilience happens much more frequently than generally assumed. A major insight is that resilience, far from being the sole purview of a small group of 'invulnerable' or 'invincible' individuals, is a very common set of aptitudes and practices displayed by a significant share of the population (Werner and Smith 1992, Richardson 2002: 310, Bonanno 2004). Psychology has managed to demystify the extraordinary powers of resilience and highlight its 'ordinary magic' (Masten 2011: 235).

A third, more disparate, group of scholars who were studying disaster management and urban resilience also found the concept of resilience very attractive. In the 'risk society' we inhabit (Beck 1992), the Anthropocene has unleashed increasingly frequent and severe natural disasters (droughts, fires, floods, heatwaves) that are highly disruptive to our complex technological and urban systems. Additionally, 'manufactured risks', a category of risks created by science and technology and for which we have limited historical records – and therefore very limited actuarial knowledge – have become ubiquitous (Giddens 1999: 4). Manufactured risks, such as financial crashes, nuclear meltdowns, oil spills, or public health scandals, usually unfold on a global scale and generate extreme harm. Given such a radically hostile and uncertain context, it is hardly surprising that both anthropogenic and manufactured risk researchers have embraced the concept of resilience. Two overlapping fields of enquiry in particular have been involved in the development and application of a resilience framework: urban resilience and disaster resilience. While the former is concerned with the capacity of cities to address a broad range of stresses and shocks, the latter focuses on specific large-scale adverse events and how they are managed by organizations and local communities. Both fields have produced a rich literature reviewed elsewhere (Manyena 2006, Tasan-Kok et al. 2013, Davidson et al. 2016, Paton and Johnston 2017). Two insights, however, should be highlighted. The first is that complex organizations and socio-ecological systems interpret the concept of resilience differently, depending on their level of maturity. At a basic level, resilience involves attempts to maintain the status quo and reduce the occurrence or impact of disturbance through absorption, while a more adaptive form of resilience relies on self-organization capacities and the adoption of new practices without compromising structure and function. The most advanced form of resilience is transformative, which implies a shift to a new set of functions, structures, feedbacks, and outputs that are better suited to the changing environment (Davidson et al. 2016: 8). The second insight is that it is impossible to understand – and by extension to foster –resilience in complex systems without paying attention to cross-scale interactions between an array of geographical, temporal, functional, and technological dimensions (Ansell et al 2010). Both insights appear particularly relevant to the emerging field of cyber-resilience.

The five dimensions of resilience

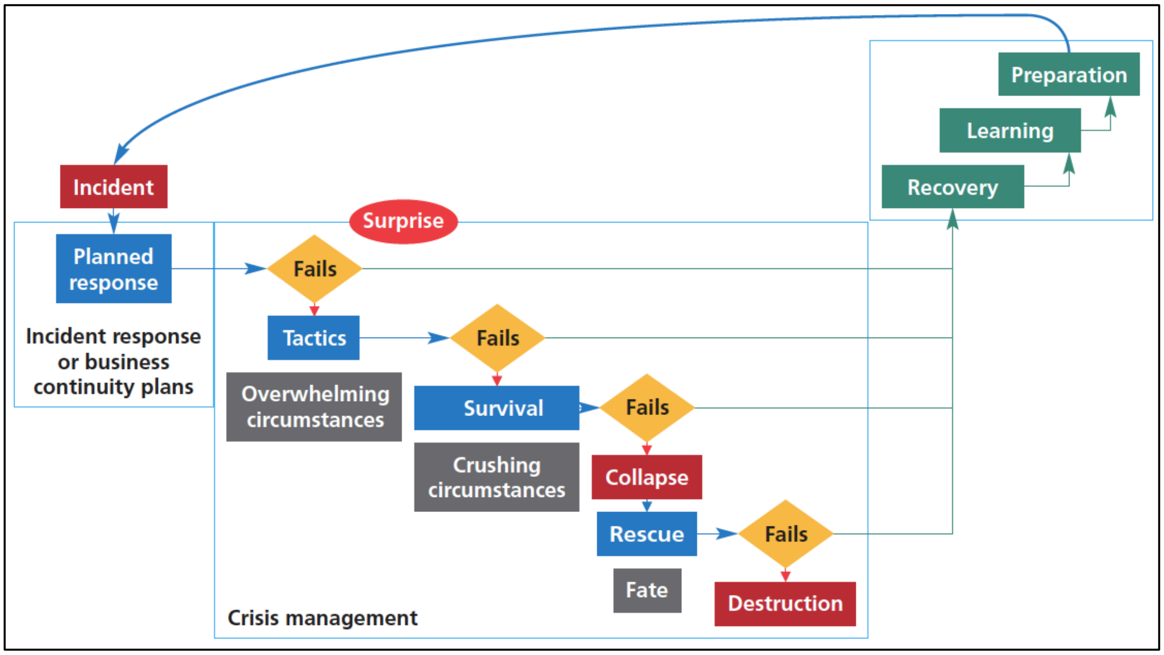
Resilience is both a state or a desired outcome and the process that leads to that state or outcome (Kaplan 1999). In the previous section I examined the diverse disciplines that have adopted the construct of resilience and discussed how they have shaped it. Each discipline studies resilience within the context of a specific unit of analysis such as a material, an organ, an ecosystem, a socio-technical system, a community, an individual, or an organization. Consolidating this general knowledge and translating it into insights that advance our understanding of cyber-resilience requires us to focus on the organizational dimensions of resilience, making it possible to address the technical, social, and psychological aspects of the problem simultaneously. The literature contains many detailed models that attempt to provide a comprehensive description of the conceptual elements that allow organizations to achieve resilience. Based on these contributions, this section summarizes the five high-level dimensions that contribute to or hinder organizational resilience.

Resilience is dynamic

There is consensus in the literature that resilience requires an extended temporal scope that includes activities before, during, and after a shock or a catastrophic incident. This implies that resilience can only be achieved through a near-permanent cyclical and cumulative process in which organizations prepare themselves to confront a variety of risks that vary in severity and frequency (before), deploy protective technologies and policies that can reduce their exposure to these risks, implement detection and response protocols that can facilitate the continuity of their operations, and mitigate the negative impacts of adverse events (during), and, finally, adapt their systems and procedures to absorb the lessons learned (after) (Conference Board of Canada 2018). These three phases unfold at very different tempos: they can be measured in weeks or months for the preparatory and adaptive phases but be reduced to minutes or hours for the detection and response phases. Each phase produces a myriad of decisions that can have salutary or dire consequences, depending on the quality of their calibration.

It is useful to think about those decisions and their potential effects on the unfolding crisis in terms of bifurcations. A bifurcation can be defined as a turning point where a possible path can be selected from a range of two or more options, each choice producing irreversible consequences that in turn produce a new set of contingencies that can improve or impair the situation being managed, increasing or reducing the range of options available to reach a desirable outcome. In other words, a bifurcation is a moment of high uncertainty where a situation can get out of control or order can be restored based on even a seemingly innocuous decision (Grossetti 2004: 26, Grossetti 2009). In crisis management, bifurcations and their outcomes are frequently represented on a “collapse ladder” (see Figure 1), where the cascade of decisions that follow the discovery of a vulnerability or the detection of an incident can prevent, control, or mitigate the aftermath or precipitate an escalation to multiple states of degradation that range from destabilisation and incapacitation to destruction (Gorniak et al. 2011: 42).

Figure 1. ENISA’s collapse ladder model



Source: (Gorniak et al. 2011: 42)

Resilience is networked

Decision making in the context of a resilient organization is not limited to a narrow internal process involving a small group of risk and crisis managers. On the contrary, it reflects the embeddedness of modern organizations and their socio-technical systems into complex webs of interdependencies that simultaneously enable and constrain them. Resilience cannot be fostered in isolation but must be strongly correlated with a dense network of intra- and interorganizational linkages that rely on strong trust and can be activated on short notice to provide additional resources and expertise in an emergency. This network aspect of resilience is particularly vital for organizations that face transboundary crises, which can be defined as adverse events that "affect multiple jurisdictions, undermine the functioning of various policy sectors and critical infrastructures, escalate rapidly and morph along the way" (Ansell et al. 2010). Typical transboundary crises include pandemics, critical infrastructure failures, and cyberattacks, and the networks that manage them must be able to bridge the physical, information, cognitive, and social domains involved (Linkov et al. 2016: 10108).

Internally, resilient organizations develop collaborative ties across business or functional units that facilitate communication and coordination during a crisis. In practice this means that formal procedures can be quickly superseded by informal mechanisms when the pace of a crisis threatens to overwhelm the organization and that decisions made in that context will be authorized by management (de Bruijne and van Eeten 2007: 21). Externally, resilient organizations nurture a diversified portfolio of strong and weak ties with suppliers, customers, competitors, advisors, and regulators in order to maintain high levels of awareness, flexibility, and access to shared resources. Although most of these ties are of an ad hoc nature and crystallise in unpredictable ways during crises, a growing number of formal mechanisms to support networked resilience are being developed, such as information- and threat-intelligence sharing initiatives (Choucri et al. 2016, Bossong and Wagner 2017, Jasper 2017, Sedenberg and Dempsey 2018), Computer Security and Incident Response Teams (Tanczer et al. 2018), and industry-wide restoration and recovery platforms (such as Sheltered Harbor[3]).

Resilience is practiced

The dynamic management of events and networking of expertise and resources discussed above are not capacities that appear ex nihilo when a crisis erupts but are the result of thorough planning efforts to develop sensemaking skills, surge capacity, interpersonal trust, and dependable institutional ties. It is important to remember that in a context of high uncertainty, where the next crisis may bear very little resemblance to the previous shock and can rarely be forecast, “plans are of little importance, but planning is essential”, as Churchill (and Eisenhower in a slightly different wording) so eloquently said. What these two master planners and crisis managers knew was that, however tempting it might be to remain fixated on rigid plans and playbooks that provide comfort in the face of unpredictability, their value resides less in their content than in the latent organizational capacities their design and regular exercise help cultivate. While resilience is not an approach that can be improvised when an adverse event occurs (Gorniak et al. 2011: 10), the improvisation skills of those in charge of managing the crisis are essential. The metaphor of jazz improvisation is one of the most appropriate to explain the complex interplay between practice and creativity, structure and flexibility.

Jazz differs from musical styles that follow a rigid written script and rely on a conductor. In contrast, jazz musicians learn to create musical pieces from minimal structures and to become comfortable with a “turbulent task environment” in which they combine individual invention with group coordination (Kamoche and Pina e Cunha 2001: 745). These minimal structures are both social and technical. Band members learn to communicate seamlessly through hand signals and eye contact, to trust each other, to take calculated risks when performing a solo, and to value the cohesiveness of the ensemble above all else. Achieving such a level of competence requires developing technical skills that include an intimate understanding of the theory and history of jazz, mastery of a wide repertoire acquired over time through extensive practice, and familiarity with a growing range of instruments (Bastien and Hostager 1988). Jazz improvisation seeks to achieve the ideal balance between creativity and structure available only to those who are able to combine spontaneity and intuition with discipline and experience (Weick 1998: 544). This musical metaphor can be translated to organizational environments, where turbulences abound, helping to articulate under what conditions training and practice can become a key component of resilience: it is not the rigid interpretation of pre-planned responses that

[3] https://shelteredharbor.org/about

fosters resilience but the improvisation of innovative solutions to alleviate surprising and unfamiliar hazards.

One of the main benefits of rehearsing crisis scenarios is that it helps overcome the startle and surprise effects. Unexpected events provoke cognitive responses that can range from a reassessment of existing knowledge frames to, at the most extreme end of the continuum, delays in decision making, panic, and paralysis that significantly impair performance in the face of adversity (Staal 2004, Martin et al. 2015, Landman et al. 2017). The practical implications are that regular and well calibrated training exercises—not too predictable but remaining manageable—contribute to the creation of a broader incident-response repertoire that is available when needed. Badly designed crisis rehearsals generate boredom and a dangerous complacency that undermines true organizational resilience (Adey and Anderson 2012).

Resilience is adaptive

I have already mentioned that more mature forms of resilience include adaptive properties. Flexible organizations that can quickly reallocate resources and have developed a culture congenial to improvisation and delegated decision-making are better prepared to face unexpected hazards. The flexibility and responsiveness needed to tackle new, challenging conditions can be achieved through redundancy and diversity. In cybersecurity, redundancy refers to the availability of "multiple protected instances of critical resources (information and services)", while diversity defines the "use [of] a heterogeneous set of technologies to minimize the impact of attacks and force adversaries to attack multiple different types of technologies" (Bodeau and Graubart 2011: 22-24). Diversity minimizes dependence on a single technology or service whose failure may prove catastrophic for an entire organization, while redundancy enhances the quantity of resources available to handle a failure by providing "surge capacity" (Ansell et al. 2010: 198). However, in the current organizational environment, where performance and efficiency considerations reign supreme, advocating the conservation of "generalized resources that may be shifted around and applied when and where they are needed" (Wildavsky 1988: 80) may prove challenging. This dilemma and the contested rationalities at play explain why organizations sometimes find it so difficult to create resilience.

Resilient organizations not only display adaptive capacities during a crisis but, once basic operations have been restored, are able to learn from their experience and identify improvements in their systems and procedures that will enhance their level of preparedness against future hazards. For the most resilient organizations, this post-crisis transformational capacity culminates in the ability to turn disasters into opportunities. Within that optimistic framework, "resilience is a measure of how well people and societies can adapt to a changed reality and capitalize on the new possibilities offered" (Paton and Johnston 2006: 8). In this approach, disaster can become a "catalyst for development". Unfortunately, this transformational dimension is seldom discussed in the organizational resilience literature (Bagheri and Ridley 2017: 7).

Resilience is contested

One would assume that the survivability of an organization would be a consensual goal widely shared by its leadership and employees, but a number of factors often conspire to hinder the implementation of measures needed to promote resilience. I have already alluded to the tension between a performance-oriented rationality that seeks to enhance productivity above all else and a resilience-oriented mindset that requires compromises between efficiency and adaptability. The costs and efforts required to increase organizational resilience can, for example, be considered to be too high or simply disproportionate in comparison with the hypothetical risks they seek to address (Paton and McClure 2017), especially when the initial costs of designing, acquiring, and implementing resilience technologies and practices must be complemented by the support costs required to maintain and facilitate the effective use of the approach, which may lead to consequential costs that can decrease functional effectiveness, performance, usability, and future opportunities (Bodeau and Graubart 2011: 38). Lack of adequate investment was ranked as the main hurdle to cyber-resilience by 60% of respondents in an international survey of 2,848 cybersecurity professionals conducted in 2017 (Ponemon Institute 2018b: 7).

Lack of resources and time are not the only barriers to cyber-resilience – psychological factors and cognitive biases also play an important role. Even a well-resourced organization will have few incentives to improve its preparedness and build up its resilience if its management team underestimates the probability and severity of possible adverse events. I have already mentioned the increasing uncertainty that characterizes the current cyber-risk landscape, but it is important at this stage to distinguish the gradations of knowledge that influence the propensity to adopt or discount resilience measures. When certainty can be defined as “the ability to predict accurately the consequences of actions”, and therefore to fully anticipate risks, uncertainty refers to the knowledge of “the kind or class of events that will occur, but not the probability of their happening”, and ignorance involves “knowing neither the class nor the probability of events”. ‘Superignorance’ is defined in that same typology as a form of thinking where decision makers think they know but don’t know they don’t know (Wildavsky 1988: 93). Organizations that correctly evaluate and accept their level of uncertainty and ignorance can develop methodologies that let them probe the unknown and design contingency plans, while those that overestimate their predictive capacities or are oblivious to their superignorance will see resilience approaches as wasteful.

The perception and calculation of risk is determined not only by the quantity and quality of information available but also by the cognitive biases – or heuristics – that lead individuals and their organizations to make poor decisions, even when they have access to the right information. Building on the behavioural economics approach pioneered by Daniel Kahneman and Amos Tversky (Kahneman 2011), Robert Meyer and Howard Kunreuther (2017) have outlined six biases that prevent people from planning and implementing resilience practices, referring to these self-reinforcing cognitive errors as the ‘ostrich paradox’. These biases include the tendency to focus on present savings rather than on future harms that will need to be mitigated (myopia bias), to quickly forget the lessons of past disasters (amnesia bias), to minimize the impact an adverse event can have on us even if we acknowledge it will affect others (optimism bias), to remain passive when confronted with high levels of uncertainty (inertia bias), to selectively consider only convenient factors when confronted with complex risks (simplification bias), and to align with the actions of others rather than rely on a more specific analysis of the situation (herding bias). Research on disaster risk perception has built on these insights to explain why similar information elicits very different responses. Jennifer Marlon et al. (2015) have, for example, identified five types of behaviour in the face of storm warnings and hurricane evacuation orders (first out, constrained, optimists, reluctant, and diehards), which have very different outcomes in terms of collective resilience. This literature suggests that resilience is not the only compelling risk management narrative in a given organization or community but competes with other attitudes and approaches that must be acknowledged, both theoretically and normatively.

3. Institutionalizing cyber-resilience

This section goes beyond the general principles of organizational resilience discussed above to examine more thoroughly the sector-specific measures that promote, support, or mandate cyber-resilience, as well as the challenges they face. Three types of institutional approach can be identified: 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. Each of these groups has a different understanding of cyber-resilience and how it can be achieved.

Marketing cyber-resilience

During 2013 to 2018, cyber-resilience became a staple in the constant stream of reports produced by a thriving cybersecurity industry. At least eleven companies selling consulting services (Accenture, EY, McKinsey, PwC), best practice certification (Axelos), insurance coverage (AIG), security software and hardware (Cisco, IBM, Symantec, UpGuard), or managed security services (SecureWorks) released marketing materials that extol the virtues of cyber-resilience and introduce existing or potential customers to what they claim is the future of cybersecurity. One company did not hesitate to declare that “cybersecurity is dead”, making a strong case for cyber-resilience as the only viable model left (UpGuard 2017: 2). Table 1 summarizes the main elements used to define and conceptualize cyber-resilience in these reports, enabling us to better grasp the instrumental nature of the concept and the heterogeneity of its meaning for the cybersecurity industry.

INSERT TABLE 1 ABOUT HERE

The first observation is that, despite their strong advocacy, less than half the reports analyzed (four to be precise) provided a definition of what cyber-resilience entails. While most of these definitions contain the usual references to preparation, detection, incident response, and mitigation, some were more cryptic and verged on the grandiose, such as UpGuard's "Cyber resilience is the way technology needs to be used in the enterprise for businesses to succeed" (UpGuard 2017: 9). The seven reports that fail to provide a working definition assume that the concept of cyber-resilience is self-explanatory or intuitively understood by practitioners. Cyber-resilience is thus defined less by what it is than by what it seeks to replace – an obsolete model of traditional cybersecurity unable to deal with the complex and disruptive nature of cyber-risks. None of the eleven reports consulted made any reference to the more general concept of resilience in fields such as engineering, disaster management, management of socio-ecological systems, or psychology, illustrating the narrowness of their scope. The fact that most of these documents rarely exceed ten pages and do not have the luxury to dwell on the rich history of the concept may explain this paucity of contextual information.

While cyber-resilience is vaguely defined, if at all, a broad range of constitutive technologies, processes, and practices are listed to demonstrate increasing organizational capacity in that domain. Twelve elements of cyber-resilience, listed in order of decreasing frequency, were found in the eleven reports: shared responsibility (10), detection of threat (9), incident response (9), prevention (8), risk mapping (7), recovery (6), networked capacity (6), development of crisis scenarios (5), simulations (5), adaptation (5), digital forensics (2), and insurance (1). The notion of shared responsibility, the most frequently mentioned, refers to the need to involve a broader range of business units and executives in the prevention and mitigation of cyber-risks than is usually the case in more traditional approaches to cybersecurity, where chief information security officers (CISOs) are usually in charge. The next three features are more technically focused on the control of, detection of, and response to cyber-incidents. It is interesting to note that more anticipatory measures, such as risk mapping, crisis scenario design, and incident simulations, as well as measures that focus on recovery, networking with third parties, and adaptation, are more sporadically recommended. The transformative potential of cyber-resilience is mentioned only twice (UpGuard 2017, PwC 2018), perhaps because the eleven companies studied do not offer specific products and services to support these more diffuse activities. Finally, outlier measures such as digital forensics and cyber-insurance coverage are suggested only by companies that operate in these particular segments of the cybersecurity market.

The direct link between the paths to cyber-resilience being advocated and the products and services that these reports' corporate sponsors have to offer should not come as a surprise. Some reports are more transparent and straightforward in that regard: Symantec's document ends with a direct invitation to the reader to "contact [her] Symantec account representative or reseller partner today to discuss how [she] can start building cyber resilience into [her] security strategy" (Symantec 2015: 7), Cisco's report emphasizes how its technical products can be leveraged to enhance a resilient network architecture (Cisco 2016), and UpGuard sprinkles screenshots of its CSTAR platform across its report to illustrate how it can help customers implement particular cyber-resilience objectives (as defined by the company). These examples remind us that such reports present a biased and partial view of cyber-resilience that is largely influenced by the interests of their sponsors and that their contribution to the pool of knowledge on cyber-resilience remains fairly modest. There are a few exceptions: PwC's and Accenture's reports include the results of surveys conducted among 9,500 and 4,600 international executives respectively (PwC 2018, Accenture 2018), while IBM commissions a yearly study on cyber resilience from the Ponemon Institute (2018b). Despite these few attempts at developing a more systematic knowledge base of the prevalence of cyber-resilience practices within organizations, most industry reports remain normative without disclosing the evidence that supports their prescriptions. In that respect some reports closely replicate the cyber-resilience frameworks that have been developed by standards organizations, to which we now turn our attention.

Standardizing cyber-resilience

A standard can be defined as a rule or norm that can be measured, tested, examined, and revised, and is sometimes described as a "recipe for reality" (Busch 2011: 24). Standards apply to products, processes, or individuals and have become ubiquitous in a complex world where flows of goods, information, money, and people have to be coordinated and synchronized on a global scale. Standards, while often invisible, support the technical and organizational infrastructures that enable modern life (Leigh Star and Lampland 2009, Gorur 2013). They therefore play a central role in the management of risk by helping to reduce the uncertainties and information asymmetries that plague interactions between business partners. Even optional standards that appear inconsequential and neutral wield great power as they control "the ability to set the rules that others follow, or to set the range of categories from which they may choose" (Busch 2011: 28). The proliferation of standards has been accelerated by the growth of national and international standard-setting bodies that bring together government and industry stakeholders (Brunsson and Jacobsson 2000). The field of cybersecurity is dominated by two general standards that include measures compatible with a cyber-resilience approach: the International Organization for Standardization's 27000-series of information security standards and the National Institute of Standards and Technology's Cybersecurity Framework.

The International Organization for Standardization (ISO) is based in Switzerland and federates 163 national standards bodies. Since its creation in 1947 it has developed more than 22,000 standards. In collaboration with the International Electrotechnical Commission (IEC), it maintains a suite of more than forty information security standards that cover a broad spectrum of issues, from the creation of a shared terminology to the design and implementation of risk management controls and best practices in incident response to forensic investigations (Lewis 2019). This family of standards originates from an earlier effort by the British Standards Institute, which adopted a code of practice for information security management in 1995. This standard was subsequently harmonized by ISO and led to the creation of the ISO/IEC 27001 standard in 2005, which was followed by

39 more specialized but still interconnected standards (Disterer 2013: 93). The ISO/IEC 27001 standard is structured around eight high-level functions (known in the ISO jargon as 'clauses') that range from understanding the 'context of the organization', to 'leadership', 'planning', 'support', 'documented information', 'operation', 'performance evaluation', and 'improvement'. Clauses are then broken down into 35 objectives and 114 controls (or measures) that meet the requirements of this standard (ISO/IEC 2013). The complexity of this structure is compounded by the fact that these measures are not presented or discussed in order of importance or introduced by order of implementation priority, which can make implementing it overwhelming, even for an organization willing to adopt it. As of 2017, more than 39,000 valid certificates had been issued to organizations that had demonstrated their compliance with the standard, but half of these were concentrated in five countries (Japan, UK, India, China, Germany) (ISO 2018), illustrating the persistent low rate and uneven pattern of adoption compared to the much more successful ISO 9000-series of standards (Fomin et al. 2008).

Although the 27000-series family of standards does not explicitly include resilience as one of its goals, it recommends many measures that contribute to the cyber-resilience of an organization, such as 'information security awareness, education and training', 'information backup', 'planning information security continuity' or 'learning from information security incidents', to name a few. The committee in charge of the development of this family of standards (known as ISO/IEC JTC 1/SC 27) also liaises regularly with ISO's resilience committee (ISO/TC 292, in charge of the ISO 22316 organizational resilience standard updated in 2017), as well as the risk management and security committee (ISO/TC 262). A more focused standard (ISO/IEC 27035) provides a set of guidelines to plan, prepare, and conduct cyber incident response activities. Meeting this standard gives organizations the capacity to deal with unexpected and unknown threats and its five phases reflect the dynamic nature of cyber-resilience: plan and prepare, detection and reporting, assessment and decision, responses, and lessons learned (ISO/IEC 2016). Its more detailed measures also emphasize the networked, practiced, and adaptive dimensions of resilience.

The second cybersecurity standard that has attracted a great deal of international interest, ORXdespite its national origins, was developed in the US by the National Institute of Standards and Technology (NIST). Created in 1901, NIST describes itself as a non-regulatory federal agency that provides technologies, measurements, and standards to US industries in order to improve their competitiveness. The Cybersecurity Framework is a voluntary tool, initially developed at the behest of the White House and launched in 2014, to improve the digital security of critical infrastructures (NIST 2018). The Cybersecurity Framework that emerged from an extensive period of consultation with a broad range of industry, government, and academic stakeholders seeks to consolidate existing standards and practices as well as to identify gaps for which updated or new standards are needed (NIST 2014). Unlike its ISO counterpart, which must be bought by companies and provides a conformity certificate delivered by an accredited third party, NIST's Cybersecurity Framework is free and not supported by a formal conformity assessment process, meaning that its implementation remains tailored to the individual needs and capacities of each adopting organization. While it is hoped that this non-constraining approach will achieve broader and faster uptake than the ISO standard, there is no guarantee of the coherence and consistency of implementation. The Framework is organized around a 'Core' of five functions (Identify, Protect, Detect, Respond, and Recover), which are themselves broken down into 23 objectives categories and 108 outcomes subcategories. Each outcome is mapped to similar measures or controls found in other cybersecurity standards such as ISO/IEC 27001 or COBIT 5. Acknowledging that organizations differ greatly in their capacity to adopt the Framework, four 'Implementation Tiers' are provided: Partial, Risk Informed, Repeatable, and Adaptive (Lei 2014: 18, Shackelford et al. 2015: 333). Each tier marks a progression in the degree of cyber-resilience toward more holistic, adaptive, and networked capacities. A library of publications organized by function, a catalog of success stories, and an annual conference are available to support Framework users in their implementation efforts. A significant number of categories and subcategories have a de facto cyber-resilience orientation (such as the testing of response and recovery plans, the implementation of mechanisms to achieve technical resilience in normal and adverse situations, the mitigation of incidents, and the incorporation of lessons learned into recovery plans) but, as in the ISO/IEC standard, there is no explicit distinction between cybersecurity and cyber-resilience and no prioritization or ranking of the measures to indicate those that are the most important in contrast to those that are secondary or should only be considered by the most mature adopters (Collier et al. 2014: 73).

In March 2018, NIST released a draft document that outlines a set of guidelines and asks for comments on how cyber resilient systems should be engineered (Ross et al. 2018). This publication, which is not connected to the Cybersecurity Framework, adopts a highly technical approach that is less concerned with the overall resilience of organizations that confront a cyber shock than with the survivability of their digital assets. Despite its narrower focus, this forthcoming standard explicitly aligns its design principles with the four cyber-resilience goals of anticipation, withstanding, recovery, and adaptation, as well as a more specific set of eight objectives and fourteen techniques (Ross et al. 2018: 17-18) inspired by previous research conducted in the early 2010s at the MITRE Corporation (Bodeau and Graubart 2011).

Moving beyond the generic cybersecurity standards deployed by ISO/IEC and NIST, more specialized standards have been proposed in relation to the various stages and domains of cyber-resilience. The most detailed of these is the CERT Resilience Management Model (CERT-RMM) developed by a division of the Software Engineering Institute at Carnegie Mellon University (Caralli et al. 2016). This 860-page document provides a comprehensive operational resilience framework that is the result of the formalization and consolidation of best practices at the convergence of the IT security, business continuity, and disaster response fields. The CERT-RMM seeks to find ways to decompartmentalize and institutionalize cyber-resilience as well as to identify the right balance between the technical and organizational measures needed to reinforce it, emphasizing the need to maintain high levels of contextual and situational awareness, develop networked and rehearsed threat management skills, and enhance adaptive capacities. It is organized around 26 process areas, which are broken down into 94 specific goals and 256 specific practices. As in the NIST Cybersecurity Framework, a detailed crosswalk table is available to map correspondences and gaps with other standards such as ISO/IEC, COBIT, and many other codes of practice. Although not formally part of the CERT-RMM, a self-assessment tool derived from it, which is more focused on cyber-risks and compatible with the NIST Cybersecurity Framework, is available from the Department of Homeland Security to help organizations evaluate their level of cyber-resilience (DHS 2016).

Across the Atlantic, the European Union Agency for Network and Information Security has, since 2009, monitored and complemented the work of standards bodies in the cybersecurity domain, with cyber-resilience a particular area of interest (Purser 2014: 104). In 2009, it released a good-practice guide on the design, conduct, and evaluation of national exercises to enhance the cyber-resilience of public communications networks (ENISA 2009). In 2011, it published a technical report that reviewed existing measurement frameworks and metrics for resilient networks and services and, lamenting the lack of a standardized framework, offered a unified taxonomy for use by organizations (ENISA 2011). It also maintains an online platform that supports the work of expert groups that are developing sectoral cyber-resilience guidelines[4]. The World Economic Forum, although not technically a standards body, has also made cyber-resilience one of its priority issues, which reflects the rise of cyber-risks as one of the two major concerns of its membership (along with environmental risks) (WEF 2019). In response, it has developed a cyber-resilience framework for boards of directors that contains a set of 10 principles and 47 detailed questions, representing elements or measures that are believed to strengthen the governance of cyber-resilience activities, that boards can use in asking senior executives about their practices in this area (WEF 2017).

All of the voluntary standards examined above, whether general or specialized, share a common underlying assumption: they implicitly assume that cyber-resilience can be achieved almost mechanistically through the time-consuming implementation of a long list of over-specified technical and organizational controls. In this dominant model, inspired by the engineering mindset, the capacity to absorb, withstand, and adapt to cyber shocks is conceptualized as the outcome of a cumulative and stable process in which measures that all seem to make a similar contribution to the final outcome are stacked in no particular order of importance. What is lost in this approach is the unpredictable, surprising, and destabilizing nature of cyber crises and the need to develop generalized resources and capacities that can adapt and endure.

Regulating cyber-resilience

The increasing likelihood and severity of cyber-risks affecting financial institutions, which have the potential to destabilize whole swaths of the financial system, have spurred

[4] https://resilience.enisa.europa.eu/

regulatory agencies to develop a broad range of assessment and compliance tools to help strengthen the cyber-resilience of the institutions they oversee. The regulation of cyber-resilience acknowledges that not all organizations are willing or able to voluntarily adopt the standards and practices that would improve their capacity to sustain a cyber shock. However, given the hyper-connected and interdependent environment in which these organizations operate, this lack of concern and action could become a source of collective harm. Some financial regulators are therefore exploring a number of strategies that cover the full spectrum of the compliance pyramid, from awareness and education to more robust forms of engagement and enforcement. The idea of a compliance pyramid is derived from Ayres and Braithwaite's (1992) theory of responsive regulation, with its core principle of the "benign big gun," which holds that escalating enforcement practices should be considered as a way to individualize the regulatory activity's intensity in relation to the regulated actors' behaviour. The default strategy in this context is non-intrusive and delegated regulation, which is more likely to generate cooperation among private actors by allowing them discretion in deciding how best to achieve regulatory goals (for example, enhancing cyber-resilience). When dealing with private actors unwilling or unable to implement effective strategies (a case of market failure), the state retains the ability to escalate its level of interventionism by shifting to command and control regulations that involve various forms of punishment.

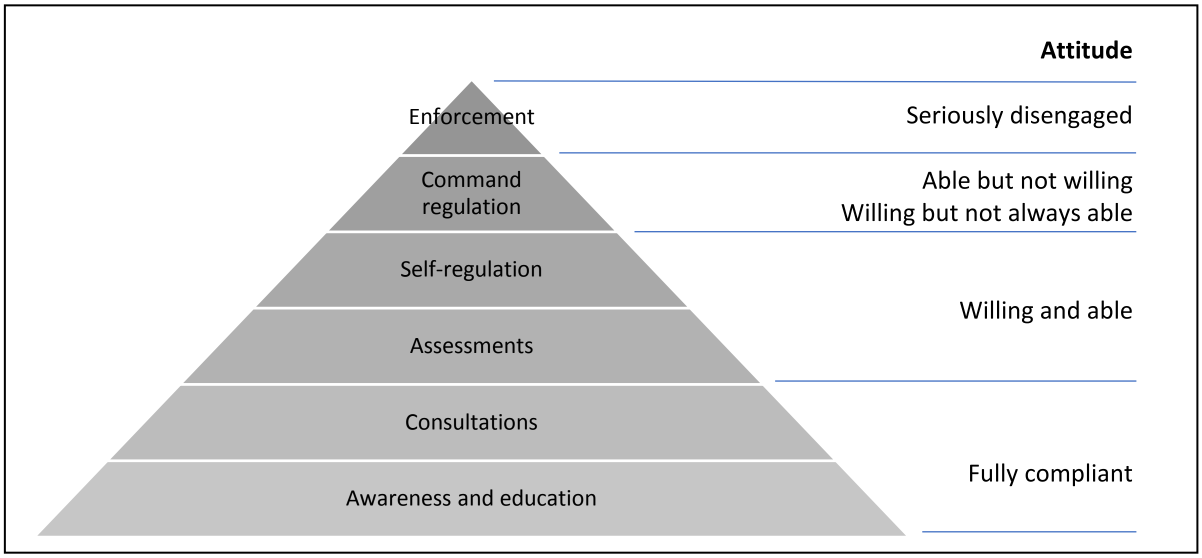


Figure 2. The cyber-resilience regulatory pyramid

For organizations at the base of the pyramid, financial regulators have increased their awareness and education efforts by providing guidance to financial institutions and creating industry forums and working groups designed to socialize the concept of cyber-resilience. On the international stage, the Bank for International Settlements, in collaboration with the International Organization of Securities Commission, published a document that suggests a range of preparations that financial market infrastructures should undertake to enhance their cyber-resilience capabilities (CPMI-IOSCO 2016). Such guidance pays particular attention to the interconnected nature of the financial infrastructure and the need to develop networked modes governance that foster cyber-resilience, as well as the importance of maintaining strong sensemaking capacities that make it possible to quickly understand the fluid and unpredictable nature of emerging and contagious crises, a regular testing program that can identify gaps in resilience, and a learning and evolving mindset that enables effective adaptation to a dynamic threat landscape. Financial institutions are strongly encouraged to develop a cyber-resilience framework that complements their existing cybersecurity and operational risk management frameworks. The distinctive approach required to achieve cyber-resilience is apparent in advice to plan for scenarios in which recovery objectives cannot be achieved (for example, when critical people or systems become unavailable for extended periods) and to operationally and technically rehearse plausible extreme events that have not yet occurred (CPMI-IOSCO 2016: 16). A recently released document prepared by the Basel Committee on Banking Supervision (BCBS) provides a repertoire of existing cyber-resilience practices across jurisdictions, helping financial institutions and their regulators take stock of existing trends (BCBS 2018).

At the regional level, in June 2017 the European Central Bank established the Euro Cyber Resilience Board for pan-European Financial Infrastructures[5], whose main mandate is to foster trust and collaboration between key stakeholders to facilitate adoption of harmonized cyber-resilience practices. In the US, in 2015 the Federal Financial Institutions Examination Council (FFIEC) published a 16-page appendix to its business continuity planning manual, focused on the resilience of outsourced services, in which cyber-risks played a central role (FFIEC 2015: J-1). Finally, in the same year, the Australian Securities and Investments Commission (ASIC) released a report aimed at raising awareness of the necessity of cyber-resilience among the institutions it regulates, using the NIST Cybersecurity Framework as a template for suggested measures (ASIC 2015). Since then, ASIC's Commissioner has made a number of public speeches highlighting the importance of cyber-resilience[6] and a checklist of 11 high-level cyber-resilience good practices was published on the regulator's website in 2018[7]. (It is interesting to note that this list makes only cursory mention of adaptation as a key outcome.)

Two central banks have launched consultations with their regulated populations in an attempt to evaluate the current state of cyber-resilience practices and identify existing gaps. In July 2018, the Bank of England and the UK's Financial Conduct Authority released a discussion paper on operational resilience that outlines the need for financial institutions to assume that their operations, processes, and systems will be disrupted by adverse events (with cyber incidents ranking very high among these) and that they should therefore develop clear expectations and metrics about their tolerance for interruption of vital

[5] https://www.ecb.europa.eu/paym/groups/euro-cyber-board/html/index.en.html.

[6] https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/resources-on-cyber-resilience/

[7] https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/cyber-resilience-good-practices/

services (Bank of England and FCA 2018). This consultation was also aimed at learning the views of the industry on their planned shift in risk management practices. The same year, the European Central Bank (ECB) issued a document dealing with cyber resilience oversight (ECB 2018a), explaining how guidance issued by CPMI-IOSCO (2016) should be operationalized and seeking feedback on a proposed set of regulatory expectations. The 20 submissions that were received expressed concern over the level of prescriptiveness in cyber-resilience regulations and recommended that efforts be made to harmonize the regulatory framework with existing international standards and national initiatives (ECB 2018b).

The next level on the compliance pyramid involves formal assessment of existing cyber-resilience capabilities by regulatory authorities. At the lower end of this category, self-assessment surveys are provided to regulated entities to help them determine their level of cyber-resilience by comparison with a reference population. In 2013, Canada's Office of the Superintendent of Financial Institutions released cyber security self-assessment guidance information (OSFI 2013), while in 2017 Australia's ASIC published the aggregated results of a similar survey completed by 101 financial institutions that rated their capacities across six cyber-resilience dimensions and shared improvement objectives (ASIC 2017). At the higher end, banking regulators in the UK, the Netherlands, and Denmark are preparing to unleash red teams on the institutions they oversee in a stress test of their response and mitigation capacities (Bank of England 2018, Danmarks Nationalbank 2018, DeNederlandscheBank 2018). Red teaming can be defined as a risk assessment activity that challenges an organization's security plans and tactics by helping it understand risk through the eyes of an opponent (Yang et al. 2006). It has a long religious, military, and organizational history (Zenko 2015), but in a cybersecurity environment typically involves an independent team of white hat hackers who conduct offensive operations against a client in an attempt to infiltrate its defenses and identify its vulnerabilities. Following in the footsteps of the UK and the Netherlands, the European Central Bank developed a framework for threat-intelligence based ethical red teaming, which suggests that this assessment practice will soon become standard practice among regulating entities (ECB 2018c).

If self-regulation is implicit in many of the guidance documents mentioned above, the more intrusive assessment instruments discussed in the previous paragraph and their increased expectations for regulated institutions clearly point toward a more prescriptive approach to cyber-resilience. For example, the Bank of England's Financial Policy Committee plans to set baseline expectations for cyber-resilience in financial firms, establish a level of tolerance for disruptions in the delivery of vital services, test how firms plan to handle disruptions within this tolerance boundaries, and impose remedial actions if baseline expectations are not met (Bank of England 2018: 40). The most coercive outcome of this type of command regulation is punitive enforcement, such as the imposition of fines, and the US Security Exchange Commission and the UK Financial Conduct Authority (FCA) have levied fines on a small number of financial institutions for failing to take elementary measures to protect the personal information and accounts of their customers (FCA 2018, Pierotti 2018). Although these fines were justified on the basis of a lack of rudimentary cybersecurity policies or inadequate incident response capacity, the most important one, which amounted to GBP 16.4 million (about USD 21.5 million as of January 2019) and was levied by the FCA on Tesco Bank, explicitly highlighted the necessity for financial institutions to maintain a baseline standard of cyber-resilience (FCA 2018).

Conclusion

It is no accident that the idea of resilience has become such a central response to the two major challenges that threaten the future of our societies: the Anthropocene and a digital world in which humans and machines are becoming increasingly integrated. Both phenomena give rise to new sets of risks that are defined by an unprecedented level of complexity and for which current risk management practices seem inadequate. The institutions that bear responsibility for managing these risks seem overwhelmed, unable to deal with the related disruptions. In this context, such institutions must recognize and accept their intrinsic fallibility and learn to prepare for, withstand, and adapt to risks. This requires a new resilience mindset in which the mirage of protection and prediction is replaced by tolerance for graceful degradation and improvisation.

This article has demonstrated how the polymorphous risks that threaten the critically important digital systems owned and operated by the financial sector—as well as the data that flow through them—require a cyber-resilience approach to augment the clearly failing cybersecurity toolset. Resilience is a powerful concept but is sufficiently ambiguous that it can become counterproductive if used carelessly. It is therefore crucial to understand its multiple origins in the fields of ecology, psychology, and disaster management, as well as the diverse meanings attached to it. The present theoretical overview makes it possible to identify five organizational dimensions of resilience – dynamic, networked, practiced, adaptive, and contested – that both enable its translation into practical activities and measures and encapsulate a broad range of issues and challenges that must be understood and addressed by any organization that hopes to enhance its chances of survival in a turbulent environment.

The third section of this article examined institutional approaches being used at the sectoral level to increase the cyber-resilience of financial institutions. Three categories of approach have emerged over the past decade: a marketing approach promoted by consulting and security firms that, under the unified label of cyber-resilience, offers a range of expertise and tools that is broad but lacks consistency, a standardizing approach strongly influenced by an engineering methodology in which the destabilizing nature of surprise and unpredictability is often minimized—if not denied – and a regulatory approach that covers the full spectrum of the compliance pyramid. All three approaches are in the early stages of implementation and it is much too early to assess their impact and effectiveness.

It would be a truism to end such a review by suggesting that more research is needed and specific research questions are therefore proposed to encourage a much-needed effort to increase our knowledge base about cyber-resilience. As the number of major cyber-incidents increases, it becomes essential to collect data on individual cases to document how financial institutions respond to cyber-shocks and to determine which elements of their mitigation strategies heighten—or undermine—their cyber-resilience. In other words, the rich theoretical and normative literature on cyber-resilience must be complemented by strong empirical evidence on which organizational properties and measures foster or impede cyber-resilience. This effort should aim not only to collect a diverse sample of case studies that can serve as lessons in cyber-resilience but should also improve our ability to measure progress on how cyber-resilience is operationalized. Cyber-resilience metrics remain under-researched and joint efforts involving practitioners and academics should be initiated to ensure that the right tools are available to measure what counts (Somers 2009, Bodeau and Graubart 2011, Linkov et al. 2013, Davidson et al. 2016). Finally, it is important to improve our understanding of how the cyber-resilience of individual organizations affects their surrounding ecosystem. In the same way that cyber-risks are aggregated and propagated from one financial institution to its external partners (Kopp et al. 2017: 9), cyber-resilience measures reverberate across organizational boundaries to strengthen or erode their partners' capacity to withstand digital shocks. They also trigger a range of outcomes across multiple scales, simultaneously affecting individual customers, organizational peers, industry regulators, and national or international financial systems. Documenting how cyber-resilience spreads and is negotiated across organizational interdependencies is vital to guaranteeing that it remains an accountable and collectively effective risk management strategy.

References

Accenture (2018), *Gaining ground on the cyber attacker: 2018 state of cyber resilience*, Accenture, Dublin.

Adey, Peter, and Anderson, Ben (2012), “Anticipating emergencies: Technologies of preparedness and the matter of security”, *Security Dialogue*, 43 (2): 99-117.

Agari (2018), *London Blue: UK-based multinational gang runs BEC scams like a modern corporation*, Agari, Foster City, CA.

Ansell, Chris, Boin, Arjen, and Keller, Ann (2010), “Managing transboundary crises: Identifying the building blocks of an effective response system”, *Journal of Contingencies and Crisis Management*, 18 (4): 195-207.

ASIC (2015), *Cyber resilience: Health check*, Australian Securities & Investments Commission, Canberra.

ASIC (2017), *Cyber resilience of firms in Australia’s financial markets*, Australian Securities & Investments Commission, Canberra.

Ayres, Ian, and Braithwaite, John (1992), *Responsive regulation*, Oxford University Press, New York, NY.

Bagheri, Seyedehsaba, and Ridley, Gail (2017), "Organisational cyber resilience: Research opportunities", *Australasian Conference on Information Systems*, Hobart, 4-6 December.

Bank of England (2018), *Financial stability report - Issue No. 43*, Bank of England, London.

Bank of England and FCA (2018), *Building the UK financial sector’s operational resilience*, Bank of England, London.

Bastien, David T., and Hostager, Todd J. (1988), “Jazz as a process of organizational innovation”, *Communication Research*, 15 (5): 582-602.

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

Beck, Ulrich (1992), *Risk society: Towards a new modernity*, SAGE Publications, London.

Benson, Melinda Harm, and Craig, Robin Kundis (2014), “The end of sustainability”, *Society & Natural Resources*, *27*(7): 777-782.

Bodeau, Deborah, and Graubart, Richard (2011), *Cyber resiliency engineering framework*, The MITRE Corporation, Bedford.

Bonanno, George A. (2004), "Loss, trauma, and human resilience: Have we underestimated the human capacity to thrive after extremely aversive events?", *American Psychologist*, 59 (1): 20-28.

Bossong, Raphael, and Wagner, Ben (2017), "A typology of cybersecurity and public-private partnerships in the context of the EU", *Crime, Law and Social Change*, 67 (3): 265-288.

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

Brewster, Thomas (2017), "Russian cybercriminals are loving those leaked NSA Windows weapons", *Forbes*, 26 April, available online at https://www.forbes.com/sites/thomasbrewster/2017/04/26/shadow-brokers-leaked-nsa-cyber-tools-become-weapons-of-american-enemies/#7776e0a31924.

Brunsson, Nils, and Jacobsson, Bengt (2000), *A world of standards*, Oxford University Press, Oxford.

Busch, Lawrence (2011), *Standards: Recipes for reality*, The MIT Press, Cambridge, MA.

Button, Mark (2008), *Doing security: Critical reflections and an agenda for change*, Palgrave Macmillan, Basingstoke.

Caralli, Richard, Allen, Julia, White, David, Young, Lisa, Mehravari, Nader, and Curtis, Pamela (2016), *CERT Resilience Management Model, Version 1.2*, Carnegie Mellon University, Pittsburgh.

Carter, William (2017), *Forces shaping the cyber threat landscape for financial institutions*, SWIFT Institute, London.

Castells, Manuel (2001), *The internet galaxy: Reflexions on the internet, business, and society*, Oxford University Press, Oxford.

Choucri, Nazli, Madnick, Stuart, Koepke, Priscillia (2016), *Institutions for cyber security: International responses and data sharing initiatives*, Massachusetts Institute of Technology, Cambridge, MA.

Cisco (2016), *Cyber resilience: Safeguarding the digital organization*, Cisco, San Jose, CA.

Coleman, Gabriella (2014), *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*, Verso, New York, NY.

Collier, Zachary, DiMase, Daniel, Walters, Steve, Tehranipoor, Mark Mohammad, Lambert, James, and Linkov, Igor (2014), "Cybersecurity standards: Managing risk and creating resilience", *Computer*, 47 (9): 70-76.

Conference Board of Canada (2018), *Building cyber resilience*, Conference Board of Canada, Ottawa.

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

Crosman, Penny (2016), "The real threat Anonymous poses to banks", *American Banker*, 6 May, available online at https://www.americanbanker.com/news/the-real-threat-anonymous-poses-to-banks.

Danmarks Nationalbank (2018), *TIBER-DK general implementation guide*, Danmarks Nationalbank, Copenhagen.

Danzig, Richard J. (2014), *Surviving on a diet of poisoned fruit: Reducing the national security risks of America's cyber dependencies*, Center for a New American Security, Washington DC.

Davidson, Julie L., Jacobson, Chris, Lyth, Anna, Dedekorkut-Howes, Aysin, Baldwin, Claudia L., Ellison, Joanna C., Holbrook, Neil J., Howes, Michael J., Serrao-Neumann, Silvia, Singh-Peterson, Lila, and Smith, Timothy F. (2016), "Interrogating resilience: toward a typology to improve its operationalization", *Ecology and Society, 21*(2): 1-15.

De Bruijne, Mark, and van Eeten, Michel (2007), "Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment", *Journal of Contingencies and Crisis Management*, 15 (1): 18-29.

DeNederlandscheBank (2018), *TIBER-NL goes Europe*, available online at https://www.dnb.nl/en/news/nieuwsbrief-betalingsverkeer/Juni2018/index.jsp.

DHS (2016), *Cyber Resilience Review (CRR): Self-assessment package*, Department of Homeland Security, Washington DC.

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

Downes, Barbara J., Miller, Fiona, Barnett, Jon, Glaister, Alena, and Ellemor, Heidi (2013), "How do we know about resilience? An analysis of empirical research on resilience, and implications for interdisciplinary praxis, *Environmental Research Letters*, 8 (1): 1-8.

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

ECB (2018b), *Response to the public consultation on the cyber resilience oversight expectations*, European Central Bank, Frankfurt.

ECB (2018c), *TIBER-EU framework: How to implement the European framework for threat intelligence based ethical red teaming*, European Central Bank, Frankfurt.

ENISA (2009), *Good practice guide on national exercises: Enhancing the resilience of public communications networks*, ENISA, Heraklion.

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

Evans, Steve (2018), "Mondelez's NotPetya cyber attack claim disputed by Zurich: Report", *Reinsurance News*, 17 December, available online at https://www.reinsurancene.ws/mondelezs-notpetya-cyber-attack-claim-disputed-by-zurich-report/.

FCA (2018), "FCA fines Tesco Bank £16.4m for failures in 2016 cyber attack", *FCA website*, 1 October, available online at https://www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack.

FFIEC (2015), *Business continuity planning: IT examination handbook*, Federal Financial Institutions Examination Council, Arlington, VA.

Fomin, Vladislav, de Vries, Henk, and Barlette, Yves (2008), "ISO/IEC 27001 Information systems security management standard : Exploring the reasons for low adoption", *EUROMOT: The Third European Conference on Management of Technology*, Nice, 17-19 September.

Forrest, Conner (2018), "Why 31% of data breaches lead to employees getting fired", *TechRepublic*, 14 September, available online at https://www.techrepublic.com/article/why-31-of-data-breaches-lead-to-employees-getting-fired/.

Gallagher, Sean (2018), "Candid camera: Dutch hacked Russians hacking DNC, including security cameras", *Ars Technica*, 26 January, available online at https://arstechnica.com/information-technology/2018/01/dutch-intelligence-hacked-video-cameras-in-office-of-russians-who-hacked-dnc/.

Giddens, Anthony (1999), “Risk and responsibility’, *The Modern Law Review*, 62 (1): 1-10.

Gorniak, Slawomir, Tirtea, Rodica, Ikonomou, Demosthenes, Cadzow, Scott, Gierszal, Henryk, Sutton, David, Theron, Paul, and Vishik, Claire (2011), *Enabling and managing end-to-end resilience*, ENISA, Heraklion.

Gorur, Radhika (2013), “The invisible infrastructure of standards”, *Critical Studies in Education*, 54 (2): 132-142.

Grossetti, Michel (2004), *Sociologie de l’imprévisible: Dynamiques de l’activité et des formes sociales*, Presses Universitaires de France, Paris.

Grossetti, Michel (2009), “Imprévisibilités et irréversibilités : les composantes des bifurcations”, in Michel Grossetti, Marc Bessin and Claire Bidart (eds.), *Bifurcations : Les sciences sociales face aux ruptures et à l’événement*, La Découverte, Paris : 147-159.

Holling, C. S., (1973), "Resilience and stability of ecological systems", *Annual Review of Ecology and Systematics*, 4: 1-23.

Holling, C. S. (1996), “Engineering resilience versus ecological resilience”, in Peter Schulze (ed.), *Engineering within ecological constraints*, National Academy Press, Washinton D.C.

IBM (2017), *Six steps for building a robust incident response function*, IBM Security Group, Somers, NY.

ISO (2018), *The ISO survey of management system standards certifications – 2017 – ISO/IEC 27001 data per country and sector 2006 to 2017*, ISO, Geneva, Excel file downloadable from https://www.iso.org/the-iso-survey.html.

ISO/IEC (2013), *ISO/IEC 27001: Information technology – security techniques – information security management systems – requirements*, ISO, Geneva.

ISO/IEC (2016), *ISO/IEC 27035-1: Information technology – security techniques – information security incident management – part 1: Principles of incident management*, ISO, Geneva.

Jasper, S. E. (2017), “U.S cyber threat intelligence sharing framework”, *International Journal of Intelligence and Counter Intelligence*, 30 (1): 53-65.

Kahneman, Daniel (2011), *Thinking, fast and slow*, Doubleday Canada, Toronto.

Kamoche, Ken, and Pina e Cunha, Miguel (2001), “Minimal structures: From jazz improvisation to product innovation”, *Organization Studies*, 22 (5): 733-764.

Kaplan, Howard (1999), “Toward an understanding of resilience: A critical review of definition and models”, in Meyer D. Glantz and Jeannette L. Johnson (eds.), *Resilience and development: Positive life adaptations*, Springer, Boston, MA: 17-83.

Koenig, David (2018), “A year after Equifax breach, no enforcement actions”, *AP News*, 8 September, available online at https://www.apnews.com/3e135a3f5b1941a48a9cb9692950d11e.

Kopp, Emanuel, Kaffenberger, Lincoln, and Wilson, Christoper (2017), “Cyber risk, market failures, and financial stability”, *IMF Working Paper*, WP/17/185: 1-35.

Kuehl, Daniel (2009), “From cyberspace to cyberpower: Defining the problem”, in Franklin Kramer, Stuart Starr, and Larry Wentz (eds.), *Cyberpower and national security*, National Defense University Press, Washington DC: 1-17.

Landman, Annemarie, Groen, Eric L., van Passen, M. M., Bronkhorst, Adelbert W., and Mulder, Max (2017), “Dealing with unexpected events on the flight deck: A conceptual model of startle and surprise”, *Human Factors*, 59 (8): 1161-1172.

Lei, Shen (2014), “The NIST Cybersecurity Framework: Overview and potential impacts”, *The SciTech Lawyer*, 10 (4): 16-19.

Leigh Star, Susan, and Lampland, Martha (2009), “Reckoning with standards”, in Martha Lampland and Susan Leigh Star (eds.), *Standards and their stories*, Cornell University Press, Ithaca, NY: 3-34.

Lewis, Barnaby (2019), “How to tackle today’s IT security risks”, *ISOfocus*, (132): 6-11.

Linkov, Igor, Eisenberg, Daniel A., Bates, Matthew E., Chang, Derek, Convertino, Matteo, Allen, Julia H., Flynn, Stephen E., and Thomas P. Seager (2013), "Measurable Resilience for Actionable Policy", *Environmental Science & Technology*, 47 (18): 10108-10110.

Lusthaus, Jonathan (2018), *Industry of anonymity: Inside the business of cybercrime*, Harvard University Press, Cambridge, MA.

Manyena, Siambabala Bernard (2006), “The concept of resilience revisited”, *Disasters*, 30 (4): 433-450.

Marlon, Jennifer, Leiserowitz, Anthony, Feinberg, Geoff, and Rosenthal, Seth (2015), *Hurricane attitudes of coastal Connecticut residents: A segmentation analysis to support communication*, Yale Project on Climate Change Communication, New Haven, CT.

Martin, Wayne L., Murray, Patrick S., Bates, Paul R., and Lee, Paul S. Y. (2015), "Fear-potentiated startle: A review from an aviation perspective", *The International Journal of Aviation Psychology*, 25 (2): 97-107.

Masten, Ann S. (2001), "Ordinary magic: Resilience processes in development", *American Psychologist*, 56 (3): 227-238.

Masten, Ann S. (2018), "Resilience theory and research on children and families: Past, present, and promise", *Journal of Family Theory & Review*, 10 (1): 12-31.

Meyer, Robert, and Kunreuther, Howard (2017), *The ostrich paradox: Why we underprepare for disasters*, Wharton Digital Press, Philadelphia, PA.

Miller, Sarah, and Trotman, Jonathan (2018), "Insider threats in finance and insurance", *Insider Threat Blog*, 5 December, available online at https://insights.sei.cmu.edu/insider-threat/2018/12/insider-threats-in-finance-and-insurance-part-4-of-9-insider-threats-across-industry-sectors.html.

Nakashima, Ellen (2017), "Israel hacked Kaspersky, then tipped the NSA that its tools had been breached", *The Washington Post*, 10 October, available online at https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html.

Newman, Lily Hay (2018), "Equifax's security overhaul, a year after its epic breach", *Wired*, 25 July, available online at https://www.wired.com/story/equifax-security-overhaul-year-after-breach/.

NIST (2014), *Framework for improving critical infrastructure cybersecurity*, NIST, Washington DC.

NIST (2018), *History and creation of the framework*, 8 February, available online at https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework.

OED Online (2018), "resilience, n.", *OED Online*, December, available online at www.oed.com/view/Entry/163619.

Olsson, Lennart, Jerneck, Anne, Thoren, Henrik, Persson, Johannes, and O'Byrne, David (2015), "Why resilience is unappealing to social science: Theoretical and empirical investigations of the scientific use of resilience, *Scientific* Advances, 1 (4): 1-11.

ORX (2018), *Annual banking loss report: Operational risk loss data for banks submitted between 2012 and 2017*, ORX, Bath.

ORX (2019), *Operational risk horizon 2019: Summary*, ORX, Bath.

OSFI (2013), *Cyber security self-assessment guidance*, OSFI, Ottawa.

PandaLabs (2017), "Not just WannaCry: The EternalBlue exploit gives rise to more attacks", *PandaLabs Blog*, 18 May, available online at https://www.pandasecurity.com/mediacenter/pandalabs/wannacry-eternalblue-exploit-more-attacks/.

Paton, Douglas, and Johnston, David (eds.) (2006), *Disaster resilience: An integrated approach*, Charles C Thomas, Springfield, IL.

Paton, Douglas, and Johnston, David (eds.) (2017), *Disaster resilience: An integrated approach*, Charles C Thomas, Springfield, IL.

Paton, Douglas, and McClure, John (2017), "Business continuity in disaster contexts", in Douglas Paton and David Johnston (eds.), *Disaster resilience: An integrated approach*, Charles C Thomas, Springfield, IL: 79-93.

Perlroth, Nicole, and Shane, Scott (2017), "How Israel caught Russian hackers scouring the world for U.S. secrets", *The New York Times*, 10 October, available online at https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html.

Pierotti, William (2018), "Cyber Babel: Finding the Lingua Franca in cybersecurity regulation", *Fordham Law Review*, 87 (1): 405-435.

Ponemon Institute (2018a), *2018 cost of a data breach study: Global overview*, Ponemon Institute, Traverse City, MI.

Ponemon Institute (2018b), *The third annual study on the cyber resilient organization*, Ponemon Institute, Traverse City, MI.

Purser, Steve (2014), "Standards for cyber security", in Melissa Hathaway (ed.), *Best practices in computer network defense: Incident detection and response*, IOS Press, Amsterdam:97-106.

PwC (2018), *Strengthening digital society against cyber shocks*, PwC, London.

Randazzo, Marisa Reddy, Keeney, Michelle, Kowalski, Eileen, Cappelli, Dawn, and Moore, Andrew (2005), *Insider threat study: Illicit cyber activity in the banking and finance sector*, Carnegie Mellon Software Engineering Institute, Pittsburgh.

Raytheon (2015), *The financial industry and the insider threat*, Raytheon, Herndon, VA.

Richardson, Glenn E. (2002), “The metatheory of resilience and resiliency”, *Journal of Clinical Psychology*, 58 (3): 307-321.

Ross, Ron, Graubart, Richard, Bodeau, Deborah, and McQuaid, Rosalie (2018), *Systems security engineering: Cyber resiliency considerations for the engineering of trustworthy secure systems*, NIST, Washington DC.

Schackelford, Scott, Proia, Andrew, Martell, Brenton, and Craig, Amanda (2015), “Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST Cybersecurity Framework on shaping reasonable national and international cybersecurity practices”, *Texas International Law Journal*, 50: 305-355.

Security G33k (2018), “Operation Icarus - 2018: An independent research and analysis”, *Security G33k Blog*, 18 December, available online at http://securityg33k.blogspot.com/2018/12/operation-icarus-2018-independent.html.

Security Response Attack Investigation Team (2018), “FASTCash: How the Lazarus Group is emptying millions from ATMs”, *Symantec Threat-Intelligence Blog*, 8 November, available online at https://www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware.

Sedenberg, Elaine M., and Dempsey, James X. (2018), “Cybersecurity information sharing governance structures: An ecosystem of diversity, trust, and tradeoffs”, *arXiv:1805.12266v1*, available online at https://arxiv.org/abs/1805.12266.

Seligman, Martin E. P., and Csikszentmihalyi, Mihaly (2000), “Positive psychology: An introduction”, *American Psychologist*, 55 (1): 5-14.

Somers, Scott (2009), “Measuring resilience potential: An adaptive strategy for organizational crisis planning”, *Journal of Contingencies and Crisis Management*, 17 (1): 12-23.

Sood, Aditya K., and Enbody, Richard J. (2013), “Crimeware-as-a-service—a survey of commoditized crimeware in the underground market”, *International Journal of Critical Infrastructure Protection*, 6 (1): 28-38.

Staal, Mark (2004), *Stress, cognition and human performance: A literature review and conceptual framework*, NASA Ames Research Center, Moffett Field, CA.

Statistics Canada (2018), *Impact of cybercrime on Canadian businesses, 2017*, Statistics Canada, Ottawa

Symantec (2015), *The cyber resilience blueprint: A new perspective on security*, Symantec, Mountain View, CA.

Tanczer, Leonie Maria, Brass, Irina, and Carr, Madeline (2018), "CSIRTs and global cybersecurity: How technical experts support science diplomacy", *Global Policy*, 9 (3): 60-66.

Tasan-Kok, Tuna, Stead, Dominic, and Lu, Peiwen (2013), "Conceptual overview of resilience: History and context", in Ayda Eraydin and Tuna TAsan-Kok (eds.), *Resilience thinking in urban planning*, Springer, Dordrecht: 39-51.

Tedim, Fantina, and Leone, Vittorio (2017), "Enhancing resilience to wildfire disasters: From the "war against fire" to "coexist with fire", In Douglas Paton and David Johnston (eds.), *Disaster resilience: An integrated approach*, Charles C Thomas, Springfield: 362-383.

United States Department of Justice (2016), "Seven Iranians working for Islamic Revolutionary Guard corps-qffiliated entities charged for conducting coordinated campaign of cyber attacks against U.S. financial sector", *Justice News*, 24 March, available online at https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.

United States of America v. Park Jin Hyok (2018), United States District Court for the Central District of California, available online at https://www.justice.gov/usao-cdca/press-release/file/1091951/download.

UpGuard (2017), *Cyber resilience for the C-suite*, UpGuard, Mountain View, CA.

Verizon (2018), *2018 data breach investigations report 11th edition*, Verizon, New York, NY.

Volkov, Dmitry (2018), "Silence: Moving into the darkside", *Group-IB Blog*, 5 September, available online at https://www.group-ib.com/blog/silence.

Waller, Margaret A. (2001), "Resilience in ecosystemic context: Evolution of the concept", *American Journal of Orthopsychiatry*, 71 (3): 290-297.

Warkentin, Merrill, and Willison, Robert (2009), "Behavioral and policy issues in information systems security: The insider threat", *European Journal of Information Systems*, 18 (2): 101-105.

WEF (2017), *Advancing cyber resilience: Principles and tools for boards*, World Economic Forum, Geneva.

WEF (2019), *The global risks report 2019 14th edition*, World Economic Forum, Geneva.

Weick, Karl E. (1998), “Improvisation as a mindset for organizational analysis”, *Organization Science*, 9 (5): 543-555.

Werner, Emmy, and Smith, Ruth S. (1992), *Overcoming the odds: High risk children from birth to adulthood*, Cornell University Press, Ithaca NY.

Wildavsky, Aaron (1988), *Searching for safety*, Transaction Publishers, New Brunswick.

Yang, Ang, Abbass, Hussein, and Sarker, Ruhul (2006), “Characterizing warfare in red teaming”, *IEEE Transactions on Systems, Man, and Cybernetics-Part B*, 36 (2): 268-285.

Zenko, Micah (2015), *Red team: How to succeed by thinking like the enemy*, Basic Books, New York, NY.

Table 1. Elements of cyber-resilience in eleven industry reports

Company	Year	Title of report	Definition	Risk mapping	Crisis scenarios	Simulations	Prevention	Detection	Incident response	Recovery	Forensics	Insurance	Shared responsibility	Networked	Adaptation
Axelos	2014	Cyber resilience: bridging the business and technology divide		●			●	●	●				●	●	●
EY	2014	Achieving resilience in the cyber ecosystem	●	●				●	●	●			●	●	●
AIG	2015	Achieving cyber resilience		●	●		●		●			●	●		
Symantec	2015	The cyber resilience blueprint: A new perspective on security		●		●	●	●	●	●			●	●	●
Cisco	2016	Cyber resilience: safeguarding the digital organization	●				●	●	●	●	●		●	●	
IBM	2017	Six steps for building a robust incident response function		●	●	●		●	●	●	●		●		
SecureWorks	2017	The resilient enterprise: Top recommendations for effective cyber response					●	●	●						
UpGuard	2017	Cyber resilience for the C-suite	●				●	●					●	●	●
Accenture	2018	The 2018 state of cyber resilience	●	●	●	●	●	●	●	●			●		
McKinsey	2018	Digital resilience: seven practices in cybersecurity			●	●	●						●		
PwC	2018	Strengthening digital society against cyber shocks		●	●	●		●	●	●			●	●	●
		Frequency	4	7	5	5	8	9	9	6	2	1	10	6	5