The Conference Board of Canada | Le Conference Board du Canada

Building Cyber Resilience.

At a Glance

- The changing cyber threat landscape means that experiencing a cyber incident has become a virtual inevitability. Building a strong cyber security posture is not enough—organizations need to build **cyber resilience**.
- The goal of cyber resilience is to increase an organization's ability to limit the impact of cyber disruptions, maintain critical functions, and rapidly re-establish normal operations following a cyber incident.
- An effective organizational cyber resilience strategy should be built on five key pillars: prepare, protect, detect, respond, and recover.

BRIEFING JULY 2018

Cyber resilience recognizes the inevitability of a successful cyber attack.

Executive Summary

Cyber incidents, intrusions, and attacks threaten organizations on a daily basis. The idea that organizations will fall victim to some form of cyber attack has moved from a possibility to a virtual inevitability. Building a strong cyber security posture alone is not enough. Whether a cyber incident originates from an insider threat or from a zero-day vulnerability, organizations can take several core steps to ensure their resilience.

In order to achieve cyber resilience, organizations should start with adopting a comprehensive definition, which is outlined in the recommendations below.

Two important distinctions separate cyber **resilience** from cyber **security**: business continuity and organizational responsibility. Unlike cyber security, which is usually very focused on protection, cyber resilience recognizes the inevitability of a successful cyber attack and the need to ensure that the business can maintain critical functions and quickly return to normal. In addition, building cyber resilience requires that multiple departments and functions work together—unlike cyber security, which tends to be the domain of a single department. Ultimately, cyber security is one of the building blocks for a more comprehensive cyber resilience strategy.

Based on an analysis of recent literature and discussions at events organized by The Conference Board of Canada, the following recommendations can be made for organizations wanting to build cyber resilience:

Prepare

- Adopt an organizational definition of cyber resilience, which The Conference Board of Canada defines as: **An organization's ability to limit the impact of cyber disruptions, maintain critical**

functions, and rapidly re-establish normal operations following a cyber incident.

- Know your organization's risk tolerance. It is vital to understand what is considered acceptable risk, what your organization is most concerned about protecting against, and where it is willing to invest to offset risk (e.g., insurance). This issue should be revisited regularly and after any significant security incident.
- Design a governance structure for cyber resilience that suits the unique needs of your organization. It should clearly establish roles and responsibilities for ongoing strategy work and in the event of an incident.
- Develop a crisis playbook and relationships with trusted advisors. Knowing whom to call in the event of a major cyber incident, and having guidelines for employees to follow, will help reduce uncertainty.

Protect

- Implement information technology changes, policies, backup procedures, and other precautionary measures to protect your organization in the event of an incident. These activities should be ongoing and audited regularly to verify their efficacy.
- Test your cyber resilience strategy regularly through incident simulation. The level of transparency around exercises should vary from full awareness among employees to ensure everyone knows their roles and responsibilities, to semi-covert red team exercises that truly test your organization's stress response and resilience.
- Encourage partners, particularly within your supply chain, to adopt best practices and share lessons learned to improve resilience and reduce third-party risks.

Detect

- Continuously scan your systems and assets for threats. Minimize the time required to identify and remediate any threats that may have penetrated your systems.
- Leverage information sharing to enhance detection. Use the latest knowledge to keep up with the evolution and emergence of new threats.

Respond

- Utilize your crisis playbook to make timely contact with trusted advisors, particularly legal teams, breach coaches, and communications specialists. Use the developed plans to assign tasks to protect critical operations, re-establish business operations, and restore your organization's data.

Recover

- Leverage the lessons learned from each cyber incident. Your cyber resilience strategy should evolve with the insights gained from dealing with any incident and the changing threat landscape.

Introduction

Cyber incidents, intrusions, and attacks threaten organizations on a daily basis. The idea that organizations will fall victim to a cyber attack has moved from a possibility to a virtual inevitability. Building a strong cyber security posture is not enough—organizations need to build **cyber resilience** in order to survive the inevitable impact of a cyber threat.

As early as 2012, the World Economic Forum identified cyber resilience as a growing organizational need. The report *Partnering for Cyber Resilience* acknowledges that failures will occur, and that the objective is "to restore normal operations and ensure that assets and reputations are protected."[1] Whether a cyber incident originates from an insider threat or a zero-day vulnerability, organizations can take several core steps to ensure their resilience.

To build cyber resilience, organizations should have a common understanding of what resilience is and how to achieve it, both of which can be accomplished by adopting a comprehensive definition. The first objective of this briefing is to propose such a definition. There has been much confusion, however, as to what separates cyber **resilience** from cyber **security**. These two concepts will be differentiated to provide clarity on what organizations should be striving for when they are

1 World Economic Forum, *Partnering for Cyber Resilience*.

building a cyber resilience program. Finally, this briefing will present best practices and The Conference Board of Canada's recommendations for building cyber resilience.

Using Cyber Resilience to Manage IoT Risks

The Internet of Things (IoT) comprises all devices that are connected to the internet. These devices "talk" to each other, and are able to collect, analyze, and share data. The IoT has led to an increase of automation in everything from lightbulbs to airplanes.[2]

Best estimates calculate that 8.4 billion devices were connected to the IoT in 2017, and it is expected to grow to over 20 billion internet-connected devices by 2020.[3] Samsung estimates that businesses will "need to securely manage over 7.3 billion IoT connected points by 2020."[4] The rapid growth in the adoption of IoT devices and their increasing ubiquity creates a new and evolving set of cyber security risks. Each IoT device represents an endpoint that could be used to attack an organization's systems. The low cost of these devices means that security is not always a key consideration in their design.

Hacking and unauthorized surveillance through IoT-connected devices are two of the most widely discussed threats that organizations face.[5] The potential fallout from a targeted hack or unintentional breach of the data collected by devices connected to the IoT represents a significant risk to organizations. These types of incidents, along with flaws in software and code that are discovered on a regular basis,[6] support the argument for building a new approach to dealing with the risks from IoT deployment. Cyber resilience offers a framework that could be used to manage the risk of rapid IoT adoption.

2 Burgess, "What Is the Internet of Things? WIRED Explains"; Ranger, "What Is the IoT? Everything You Need to Know About the Internet of Things Right Now."

3 Gartner, "Gartner Says 8.4 Billion "Things" Will Be in Use in 2017, up 31 Percent From 2016."

4 Samsung, *The Open Economy*, 14.

5 Burgess, "What Is the Internet of Things? WIRED Explains."

6 Ranger, "What Is the IoT? Everything You Need to Know About the Internet of Things Right Now."

Defining Cyber Resilience

A review of literature examining work that specifically addresses the concept of cyber resilience unearthed a wide variety of definitions. From a very concise definition in which cyber resilience limits the impacts of cyber security incidents[7] to viewing cyber resilience as a 360-degree security approach,[8] interpretations of this concept vary widely.

Resilience, generally, is defined as "the ability of a system to return to its original, or desired, state after being disturbed."[9] For example, an ecosystem is resilient if it adapts to survive in the face of environmental stressors or shocks.[10] Human bodies are resilient in their ability to heal after trauma. Resilient communities are able to "minimize any disaster's disruption to everyday life and their local economies."[11]

TechTarget defines business resilience as an organization's ability to "quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and overall brand equity."[12] The University of Kansas' ResiliNets echoes this by defining resilience as "the ability to provide and maintain an acceptable level of service" in the face of challenges to normal operations.[13] The concept of resilience goes beyond emergency response to a larger strategic approach for protecting operations. To this end, the importance of timeliness in protecting an organization's products, people, and value is also important.[14]

At a minimum, definitions of cyber resilience share the core characteristics of recovery and/or survivability.[15] Included in this group of definitions are those that articulate resilience as the ability to withstand

7 Banga, "What Is Cyber Resilience?"

8 Ponemon, "Learning to Thrive Against Threats."

9 Davis, "Building Cyber-Resilience Into Supply Chains."

10 Reef Resilience Network, "Ecological Resilience."

11 Community & Regional Resilience Institute, "What Is Community Resilience?"

12 Rouse, "Business Resilience."

13 Holdman, McQuaid, and Picciotto, "Cyber Resilience for Mission Assurance."

14 Rouse, "Business Resilience."

15 Continuity Central, "How to Develop a Cyber Resilience Framework"; Herrington and Aldrich, "The Future of Cyber-Resilience in an Age of Global Complexity"; IBM Resilient, "Today's Trends in Cyber Resilience: Ask Bruce."

An organization can have cyber security without being resilient.

shocks and to return to business as usual.[16] Definitions that are more detailed begin to introduce additional components under cyber resilience, often to apply the concept to specific fields. For example, one definition from the military sphere adds the maintenance of "mission critical operations" and sustaining or rapidly deploying "alternative means of accomplishing the mission" to the scope of resilience.[17] Other sources identify risk management as a core function of cyber resilience,[18] while yet others apply the concept to protecting an organization's entire supply chain following a cyber incident.[19]

The most common approach to defining cyber resilience takes a 360-degree view of cyber security, and includes prevention, detection, response, and recovery. For example, a Ponemon-Sullivan report defines cyber resilience as the "alignment of prevention, detection, and response capabilities to manage, mitigate, and move on from cyber attacks."[20] The World Economic Forum definition includes "preparations … with regard to threats and vulnerabilities, the defences that have been developed, and the resources available for mitigating a security failure after it happens."[21] This broad approach to defining cyber resilience, however, confuses the term with cyber security. A comprehensive cyber security program should be seen as a core building block in a cyber resilience strategy, but the two should not be confused.

To align an organization's cyber posture to reach beyond cyber security and into aspects of business continuity and protection for employees, customers, and reputation, the Conference Board defines cyber resilience as follows: **An organization's ability to limit the impact of cyber disruptions, maintain critical functions, and rapidly re-establish normal operations following a cyber incident.**

16 Olcott, "Cybersecurity vs. Cyber Resilience."
17 Goldman, *Building Secure, Resilient Architectures for Cyber Mission Assurance*.
18 Grieco, "Why the "Seven Steps of Cyber Resilience" Prove Critical for Digital Transformation."
19 Khan and Sepulveda Estay, "Supply Chain Cyber-Resilience."
20 Ponemon, "Learning to Thrive Against Threats."
21 Dobrygowski, "Cyber Resilience."

Cyber Resilience Versus Cyber Security

As with cyber resilience, there is no single definition of cyber security. Narrowly conceived, it can be synonymous with information technology (IT) security and involves the protection of networks and data. This can sometimes result in cyber security simply being treated as a function of information security.[22] Cyber security can also include the processes and policies to protect individuals and organizations from cyber crime.[23] Effective cyber security includes methods and processes for protecting electronic data, including identifying what the data are and where they reside, and implementing technology and business practices to protect them.[24] These definitions point to two important distinctions between cyber security and resilience: business continuity and organizational responsibility.

Cyber security is heavily focused on protecting data and preventing any malicious action from occurring. Despite these efforts, it is almost impossible to completely secure all of our data and systems in today's complex, evolving IT environment. Cyber resilience recognizes that it is inevitable that a successful attack will occur. Organizations therefore need to minimize any resulting business disruption that arises due to a cyber attack.[25] The continuity of business, through the maintenance of critical functions and the rapid resumption of business as usual, are critical components of cyber resilience that are not normally present in cyber security.

This understanding of cyber resilience implies that it builds on an established cyber security program as an evolutionary step in an organization's overall cyber posture. An organization can have cyber security without being resilient, but not the other way around. Cyber security, therefore, is a necessary pre-condition for achieving cyber resilience.

22 Economic Times, The, "Definition of 'Cyber Security.'"
23 IT Governance, "Cyber Resilience."
24 Olcott, "Cybersecurity vs. Cyber Resilience."
25 Ibid.

Many departments will play a role in building cyber resilience plans and protocols.

The various capabilities that are required to successfully generate cyber resilience must be developed, continuously built, and regularly updated. A resiliency toolkit that ensures business continuity is much broader than cyber security and involves departments from across the organization. The response phase to an incident may call upon everything from protocols for protecting data, to establishing centres of responsibility, to implementing public relations communication plans. Separate plans for tracking activities and costs resulting from the incident, retrieving data, and returning to normal operations will be utilized during the recovery phase. IT, communications, legal, and finance departments of the organization, as well as senior management, all have key roles to play in building a cyber resilience strategy that encompasses all of these aspects.[26]

This multi-departmental approach is a key difference between cyber resilience and cyber security. While cyber security is generally the responsibility of one department such as general security or IT, many departments will play a role in building cyber resilience plans and protocols. The departments concerned and the centre of responsibility for coordinating cyber resilience efforts will vary by organization. While there are useful tools and frameworks that can inform the creation of a cyber resilience strategy, there is no single prescribed approach to building cyber resilience, and its implementation will likely be unique to each and every organization's needs.

Building a Cyber Resilience Strategy

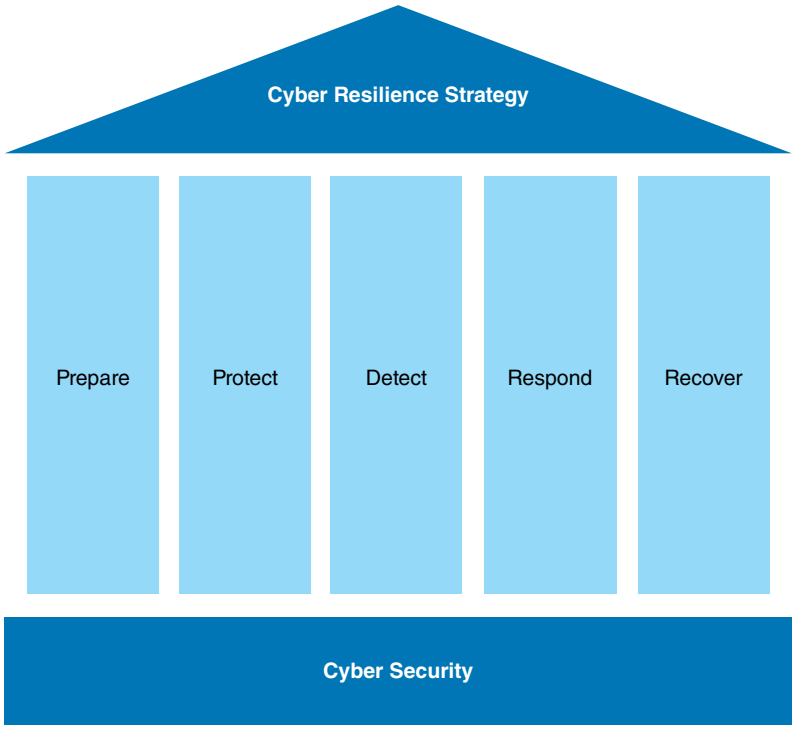
Several experts recommend a five-pillar model for building a cyber resilience strategy.[27] Those pillars are: prepare, protect, detect, respond, and recover. Organizational efforts to build cyber resilience are not equally weighted across the pillars, but they provide a useful framework for conceptualizing and developing a cyber resilience strategy. The review of literature below highlights key insights and themes from academic and industry experts on how to effectively build these pillars.

26 Hult and Sivanesan, "What Good Cyber Resilience Looks Like."

27 Systemic, *The Cyber Resilience Blueprint*; U.S. Department of Homeland Security, *Cyber Resilience White Paper*; Fong, "Cyber Coaching for Resiliency"; Edwards, "Sharing Cyber Threat Information."

These pillars are not mutually exclusive, but work together to build a comprehensive program. The truly resilient organization also understands that the threat environment will continue to evolve. As such, new intelligence, lessons learned, and emerging practices to make organizations more resilient should be continually assessed and integrated into the cyber resilience strategy.

Exhibit 1
Cyber Resilience Strategy



Source: The Conference Board of Canada.

Prepare

This first pillar is by far the most important and involved step in developing a cyber resilience strategy, and is usually the basis upon which all cyber resilience strategies are built. A recent survey of industry professionals conducted by the Ponemon Institute found that

Building a resilient organization starts at the top.

preparedness was the most important factor in achieving resiliency.[28] A comprehensive resiliency plan cannot be achieved without sufficient investment in the "prepare" pillar. During this step, an organization focuses on setting the overall stance for its cyber resilience strategy.

Building a resilient organization starts at the top. Senior executives play a central role in setting expectations for the ability to recover from cyber incidents.[29] Practitioners should begin by working with senior leadership to understand their organization's risk tolerance profile by defining what it considers an acceptable risk and what must be offset through security measures.[30] By establishing clear expectations around business continuity and levels of service, both practitioners and executives can better understand their roles and responsibilities related to investing in and promoting a resilience posture across the organization.[31] This, in combination with training and clear policies, will help to build a culture of awareness and responsibility among all employees.

Once risk tolerance and expectations around recovery are established, an organization's vulnerabilities and assets should be mapped to develop strategies for protecting critical assets and data, and for maintaining essential functions during a cyber crisis. Experts recommend putting a governance structure in place that will meet the specific needs of the organization to build a resilience strategy and meet legal and regulatory responsibilities.[32]

Employee engagement and training will be a key function of the individual or group responsible for developing and implementing a cyber resilience strategy. Employees should be regularly engaged with updates on threats facing the organization and how they can help combat them. They should also be kept up to date on the latest policies for backing up data, how to ensure core capabilities are maintained at all times, and what their roles and responsibilities are during a cyber incident.[33]

28 Ponemon Institute, *The Third Annual Study of the Cyber Resilient Organization*.

29 World Economic Forum, *Partnering for Cyber Resili*ence; Baklouti, "Security Begins With Effective Leadership."

30 Bashir, "Securing the Government of Canada"; Goche and Gouveia, "Why Cyber Security Is Not Enough."

31 Hult and Sivanesan, "What Good Cyber Resilience Looks Like."

32 Continuity Central, "How to Develop a Cyber Resilience Framework."

33 Culp, "How to Make Your Enterprise Cyber Resilient."

A key to successful emergency preparation is developing a comprehensive "crisis playbook." In addition to defining roles and responsibilities during and immediately following a cyber incident, this playbook should include a list of key stakeholders, an internal communication policy, a media strategy, and, possibly most importantly, a list of trusted advisors.[34]

At a minimum, this list of trusted advisors should include legal experts, breach coaches, insurers, relevant regulators, and, public relations experts. Having the right advisors in place in the event of a crisis can help with developing a response that will mitigate damage and help an organization return to business as usual more quickly. It is important to have frank conversations with the board of directors and, potentially, cyber insurers to determine whom to involve in a variety of scenarios. Establishing legal privilege under which to carry out certain sensitive conversations may be essential, as is knowledge of who will manage communications when news of an incident becomes public. Beyond simply knowing who to call, developing strong, positive relationships with these advisors and knowing they will respond to your organization's needs quickly is an important part of ensuring resilience.[35]

Protect

The "protect" pillar involves implementing and testing precautions and policies to confirm that all elements of the organization can ensure the continuity of their specific business lines in the event of a cyber incident. In addition, the overall survivability of the organization falls under the planning for this pillar.

At the department level, managers should implement relevant technological and training solutions to meet their responsibilities within the cyber resilience strategy. Certain precautionary measures should be universal, such as the principle of least privilege and ensuring that an individual does not represent a potential single point of failure, which refers to an individual employee with sole knowledge of critical

34 Fong, "Cyber Coaching for Resiliency"; Mandel-Campbell, "Developing an Effective Communication Strategy for After a Breach"; Cameron, "Surviving a Cybersecurity Breach."

35 Bryson, "Building Cyber Resiliency."

Organizations can increase their cyber resilience by building strong partnerships.

data or processes. Organization-wide, regular precautionary protection measures such as verifying storage and backups of critical and sensitive data should be carried out frequently. Regular IT system maintenance as well as audits of access controls should also be conducted.[36]

These precautionary measures, among others, provide a baseline for protecting an organization; however, they must be tested frequently to ensure their utility and measure their effectiveness. Several expert sources recommend developing a testing regime, using a combination of internal stress tests and red (or purple) teaming exercises[37] to ensure that organizations do not have any major vulnerabilities.[38]

Organizations can also increase their cyber resilience by building strong partnerships. Engaging with key stakeholders, other industry members, and supply chain partners to encourage the adoption of minimum standards and best practices can help improve the resilience of entire business sectors. The World Economic Forum identifies five stages in the maturation of cyber resilience strategies: unaware, fragmented, top-down, pervasive, and networked.[39] The highest level of maturity involves support and engagement from industry and supply chain partners.

Organizations should encourage partners in their supply chains to adopt best practices for cyber resilience as well. Instead of direct attacks, some malicious actors go after supply chains as an easier way of penetrating their target system.[40] The collapse of a supply chain partner due to a cyber attack, even if it isn't aimed at your organization, could result in severe business disruption. Working with supply chain partners can also help to establish common principles and guidelines to use during the response to and recovery from a cyber incident, helping to maintain business continuity across all partners.[41]

36 Continuity Central, "How to Develop a Cyber Resilience Framework."

37 For example, simulated attacks challenge an organization's security and responsiveness to identify weaknesses or vulnerabilities.

38 Hult and Sivanesan, "What Good Cyber Resilience Looks Like"; Edwards, "Sharing Cyber Threat Information"; Goche and Gouveia, "Why Cyber Security Is Not Enough."

39 World Economic Forum, *Partnering for Cyber Resilience*.

40 Krebs, "Target Hackers Broke in Via HVAC Company."

41 World Economic Forum, *Partnering for Cyber Resilience*.

Positive dialogue can also help to build relationships that may offer additional support should your organization face a crisis.[42] Building relationships may also help facilitate information sharing and cooperation. If organizations are able to share information about the threats they face and their institutional insights from combatting these threats, other organizations in the same sector and beyond may benefit from this information and avoid those threats altogether. In return, organizations receiving this threat information may have novel solutions and may be more inclined to share information.[43] Ultimately, information sharing has the potential to bolster the protect pillar through the provision of threat intelligence and potential solutions to emerging threats.

Detect

Under the "detect" pillar, the focus is on activities to identify cyber security events, which includes the ability to detect suspicious activity rapidly and assess its potential impact. One study indicated that the average length of time taken to identify a data breach is 191 days, though it can be much longer. The longer it takes to identify and deal with a breach, the costlier the incident gets.[44] Rapid detection and resolution of a cyber incident is a key requirement for limiting its impact and building cyber resilience. This will require continuous monitoring of all systems, networks, and assets, alongside regular vulnerability and penetration testing. The focus of monitoring should be based on the risk assessments carried out under the prepare pillar, ensuring that adequate resources are allocated to monitoring critical systems and data.

As highlighted in the protect pillar, initiatives to maintain, test, and improve detection procedures should also be in place to ensure the continued success of the detect pillar.

There is also an overlap here with the protect pillar around partnerships and information sharing. Information from other organizations that have been hit by a cyber attack can be used to enhance detection systems to

42 Ibid.

43 Edwards, "Sharing Cyber Threat Information."

44 Ponemon Institute, *2017 Cost of Data Breach Study.*

An effective response to a cyber incident is critical to being able to recover and ensure business continuity.

ensure the same attack cannot perpetuate across other organizations. However, the sharing of cyber threat information continues to be a challenge.[45] A key requirement for enabling cyber resilience is the development of appropriate partnerships and networks that allow an organization to access information on the latest threats for detection and protection.

Respond

An effective response to a cyber incident is critical to being able to recover and ensure business continuity. Cyber security practitioners will have a major role to play during the immediate aftermath of a cyber incident. Working alongside them, cyber resilience practitioners should have policies in place to initiate emergency notifications for executives and employees, to contact trusted advisors, to verify backups, and to execute the broader cyber resilience plan. Much of what needs to be done in this pillar builds directly off the requirements in the prepare pillar and the "crisis playbook" developed as part of it.

The "respond" pillar of a cyber resilience strategy should include contingency plans for a variety of threat scenarios aimed at limiting damage to the organization's assets and/or reputation. Those responsible for cyber resilience should verify that an organization's IT systems and infrastructure are robust and have sufficient redundancies in place to continue critical operations through a variety of potential attack scenarios.[46]

There is also a need to ensure that cyber security capabilities remain resilient following an attack. Cyber security capabilities will need to be able to come back online and continue to defend the organization against threats that may follow a major breach or cyber incident. The lack of resilience in the cyber security system could leave the organization open to follow-on attacks, further increasing the impact of the initial attack and decreasing overall cyber resilience.

45 Leuprecht and MacLellan, *Governing Cyber Security in Canada, Australia and the United States*.

46 Warzala, "What Does Good Cyber Resilience Look Like?; Continuity Central, "How to Develop a Cyber Resilience Framework."

Recover

Re-establishing normal operations or perhaps even improving them is the primary goal of the "recover" pillar. Once again, as with the respond pillar, the actions for the recover pillar should have been prepared and defined in the prepare pillar and detailed in documents such as the "crisis playbook."

Perhaps even more important to long-term resilience is what organizations learn from successfully navigating a cyber incident. Were the necessary stakeholders engaged in a timely manner? Were relationships with trusted advisors in place? Were communications plans effective? Did the cyber resilience pillars reduce the overall impact of the incident? Cyber resilience strategies will have to continually adapt and change as the organization learns from the incidents it experiences, the experiences of other organizations, and the evolving threat landscape. These strategies cannot be static and need to dynamically address a changing threat landscape.

At a recent conference on cyber resilience, one speaker put it best: "The crisis doesn't end when the crisis ends."[47] The lessons learned from the response and recovery to a cyber incident can be invaluable for improving organizational resilience, whether in the maintenance of critical activities, protection of an organization's reputation, or the speed with which normal operations are re-established. These opportunities for growth and improvement should not be wasted.[48]

Challenges

Developing a comprehensive cyber resilience strategy is not without its challenges. A recent study from the Ponemon Institute found that the biggest concern for organizations is the lack of a formal, organization-wide reporting plan for cyber security incidents. Concerns over inadequate budgets for cyber resilience, "lack of investment in new cybersecurity technologies, including artificial intelligence and machine

47 Mandel-Campbell, "Developing an Effective Communication Strategy for After a Breach."

48 Continuity Central, "How to Develop a Cyber Resilience Framework."

Organizations cannot protect themselves from every single cyber threat [with a] need to shift the approach taken from cyber security to cyber resilience.

learning," and insufficient personnel were also top concerns based on a survey conducted for the report.[49]

A report from Accenture echoes the concerns over personnel shortfalls, but frames the issue in terms of a talent shortfall across the sector.[50] Demand for highly specialized information technology skills, as well as the strategic planning skills necessary to conceptualize resilience across an organization is expected to continue to outpace supply.[51] Interestingly, other issues identified by Accenture—organizational silos, insufficient business involvement, and trying to change human behaviour to improve cyber security, for example—are addressed extensively as problems to avoid in the review of literature above.[52]

Research conducted by the Conference Board has also found that communication challenges between cyber security practitioners and boards of directors can hamper the development and implementation of cyber policies, as well as investment in cyber capabilities across an organization.[53]

While many of these challenges will be applicable to most organizations, some challenges will be unique to an organization's business priorities, culture, and leadership. It is important to keep these in mind and to ensure that relevant challenges are dealt with during the development of a cyber resilience strategy.

Recommendations for Building a Cyber Resilience Strategy

Organizations must face the reality that they cannot protect themselves from every single cyber threat. There is a need to shift the approach taken from cyber security to cyber resilience, where organizations look to limit the impact of cyber disruptions, maintain critical functions, and

49 Ponemon Institute, *The Third Annual Study of the Cyber Resilient Organization.*

50 Accenture, "Cyber Risk and Resilience: Weathering the Storm."

51 Cisco, *Mitigating the Cybersecurity Skills Shortage.*

52 Accenture, "Cyber Risk and Resilience: Weathering the Storm."

53 Vroegop, *Communicating Cyber Security to the Board of Directors*; Bryson, *Communicating Cyber Security to the Board of Directors* (webinar).

rapidly re-establish normal operations following a cyber incident. All of this needs to be built on a foundation of good cyber security practices.

From a review of recent literature and insights from Conference Board events, a series of recommendations can be made for organizations that are looking to build cyber resilience. These recommendations are based on five pillars, which are built on top of a foundation of good cyber security. The pillars should be viewed as interdependent and mutually reinforcing when building a comprehensive cyber resilience strategy. Undertaking the entire set of recommendations could require a significant investment of organizational resources and major change management. The Conference Board suggests that organizations take a maturity model approach to adopting the recommendations below; organizations should work their way through them as they are able and as they continue to build their cyber resilience strategies. The determining factor for considering the recommendations below is ultimately your organization's specific circumstances, including risk appetite and cyber resilience goals. While it would be ideal to incorporate all of the recommendations, it may not be necessary to do so to achieve the appropriate level of cyber resilience maturity for your organization.

Prepare

- Adopt an organizational definition of cyber resilience. The Conference Board of Canada proposes the following definition: **An organization's ability to limit the impact of cyber disruptions, maintain critical functions, and rapidly re-establish normal operations following a cyber incident.**
- Know your organization's risk tolerance. It is vital to understand what is considered acceptable risk, what your organization is most concerned about protecting against, and where it is willing to invest to offset risk (i.e., insurance). This issue should be revisited regularly and after any significant security incident.
- Design a governance structure for cyber resilience that suits the unique needs of your organization. It should clearly establish roles and responsibilities for ongoing strategy work and in the event of an incident.

- Develop a crisis playbook and relationships with trusted advisors. Knowing who to call in the event of a major cyber incident, and implementing guidelines for employees to follow, will help reduce uncertainty.

Protect

- Implement information technology changes, policies, backup procedures, and other precautionary measures to protect your organization in the event of an incident. These activities should be ongoing and audited regularly to verify their efficacy.
- Test your cyber resilience strategy regularly through incident simulation. The level of transparency around exercises should vary from full awareness among employees to ensure everyone knows their roles and responsibilities, to semi-covert red team exercises that truly test your organization's stress response and resilience.
- Encourage partners, particularly within your supply chain, to adopt best practices and to share lessons learned to improve resilience and reduce third-party risks.

Detect

- Continuously scan your systems and assets for threats. Minimize the time required to identify and remediate any threats that may have penetrated your systems.
- Leverage information sharing to enhance detection. Use the latest knowledge to keep up with the evolution and emergence of new threats.

Respond

- Utilize your crisis playbook to contact trusted advisors, particularly legal teams, breach coaches, and communications specialists in a timely manner. Use the developed plans to assign tasks to protect critical operations, re-establish business operations, and restore your organization's data.

Recover

- Leverage the lessons learned from each cyber incident. Your cyber resilience strategy should evolve with the insights gained from dealing with any incident and the changing threat landscape.

Acknowledgements

This briefing was prepared by Rachael Bryson, Senior Research Associate, under the guidance of Dr. Satyamoorthy Kabilan, Director, National Security and Strategic Foresight. Glen Hodgson, Senior Fellow, The Conference Board of Canada, provided an internal review. The Conference Board of Canada relies on external reviews to provide constructive, candid comments on most of our reports. Thank you to Dr. Sonia Chiasson, Associate Professor and Canada Research Chair in Human Oriented Computer Security, Carleton University; and Robert Gordon, Executive Director, Canadian Cyber Threat Exchange, for taking on this task.

Any omissions in fact or interpretation remain the sole responsibility of The Conference Board of Canada.

The Conference Board of Canada wishes to acknowledge BlackBerry Limited for funding this briefing.

APPENDIX A

Bibliography

Accenture. "Cyber Risk and Resilience: Weathering the Storm." Accenture, 2018. Accessed May 18, 2018. https://www.accenture.com/ca-en/insight-cyber-resilience-answering-cyber-risk-challenge.

Baklouti, Nadim. "Security Begins With Effective Leadership: How to Build and Facilitate Effective Cyber Security Within Boards." Plenary session at the conference Cyber Security 2018: Building Resilience Now and For the Future, Ottawa, ON, March 1–2, 2018.

Banga, Gaurav. "What is Cyber Resilience?" *The Balbix Blog*, Bablix, 2018. https://blogs.balbix.com/resilience.

Bashir, Imraan. "Securing the Government of Canada in the Age of Digital Transformation." Plenary session at the conference Cyber Security 2018: Building Resilience Now and For the Future, Ottawa, ON, March 1–2, 2018.

Bryson, Rachael. "Building Cyber Resiliency." *Hot Topics in Security and Safety* (blog). The Conference Board of Canada, April 30, 2018. http://www.conferenceboard.ca/topics/security-safety/commentaries/hot-topics-in-security-and-safety/2018/04/30/building-cyber-resiliency.

Bryson, Rachael. "Communicating Cyber Security to the Board of Directors." Webinar. Ottawa: The Conference Board of Canada, 2018.

Burgess, Matt. "What Is the Internet of Things? WIRED Explains." *Wired,* February 16, 2018. Accessed July 6, 2018. http://www.wired.co.uk/article/internet-of-things-what-is-explained-iot.

Cameron, Alex. "Surviving a Cybersecurity Breach." Plenary session at the conference Cyber Security 2018: Building Resilience Now and For the Future, Ottawa, ON, March 1–2, 2018.

Cisco. *Mitigating the Cybersecurity Skills Shortage: Top Insights and Actions From Cisco Security Advisory Services*. Cisco, 2015. https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf.

Community & Regional Resilience Institute. "What is Community Resilience?" Community & Regional Resilience Institute. Accessed March 18, 2018. http://www.resilientus.org/about-us/what-is-community-resilience/.

Continuity Central. "How to Develop a Cyber Resilience Framework." Continuity Central. May 26, 2017. https://www.continuitycentral.com/index.php/news/technology/2023-how-to-develop-a-cyber-resilience-framework.

Culp, Steve. "How to Make Your Enterprise Cyber Resilient," video from Accenture conference, May 10, 2016. https://www.youtube.com/watch?v=aCYX_ZZyq9A.

Davis, Adrian. "Building Cyber-Resilience Into Supply Chains." *Technology Innovation Management Review* 5, no. 4 (April 2015): 19–27.

Dobrygowski, Daniel. "Cyber Resilience: Everything You (Really) Need to Know." July 8, 2016. Accessed May 18, 2018. https://www.weforum.org/agenda/2016/07/cyber-resilience-what-to-know/.

Economic Times, The. "Definition of 'Cyber Security.'" *The Economic Times.* Accessed May 18, 2018. https://economictimes.indiatimes.com/definition/cyber-security.

Edwards, Shawn. "Sharing Cyber Threat Information." Plenary session at the conference Cyber Security 2018: Building Resilience Now and For the Future, Ottawa, ON, March 1–2, 2018.

Fong, Justin. "Cyber Coaching for Resiliency: Applying the Lessons of Prior Breaches." Plenary session at the conference Cyber Security 2018: Building Resilience Now and For the Future, Ottawa, ON, March 1–2, 2018.

Gartner. "Gartner Says 8.4 Billion "Things" Will Be in Use in 2017, up 31 Percent From 2016," February 7, 2017. Accessed July 5, 2018. https://www.gartner.com/newsroom/id/3598917.

Goche, Matthew, and William Gouveia. "Why Cyber Security Is Not Enough: You Need Cyber Resilience," *Forbes,* January 15, 2014. Accessed May 18, 2018. https://www.forbes.com/sites/sungardas/2014/01/15/why-cyber-security-is-not-enough-you-need-cyber-resilience/#3c8428e51bc4.

Goldman, Harriett G. *Building Secure, Resilient Architectures for Cyber Mission Assurance*. MITRE Corporation, 2010. https://pdfs.semanticscholar.org/911a/9c301359a0bcbdc3e49b2f7a04cf7eef14b2.pdf.

Grieco, Anthony. "Why the "Seven Steps of Cyber Resilience" Prove Critical for Digital Transformation." *Cisco Blogs,* Cisco*,* December 13, 2016. https://blogs.cisco.com/security/why-the-seven-steps-of-cyber-resilience-prove-critical-for-digital-transformation.

Herrington, Lewis, and Richard Aldrich. "The Future of Cyber-Resilience in an Age of Global Complexity." *Politics* 33, no. 4 (December 2013): 299–310.

Holdman, Harriet, Rosalie McQuaid, and Jeffrey Picciotto. "Cyber Resilience for Mission Assurance." Published in proceedings of the 2011 IEEE International Conference on Technologies for Homeland Security *(HST),* Waltham, Massachusetts, November 15–17, 2011.

Hult, Fredrik, and Giri Sivanesan. "What Good Cyber Resilience Looks Like," *Journal of Business Continuity & Emergency Planning* 7, no. 2 (Winter 2013–2014): 112–25.

IBM Resilient. "Today's Trends in Cyber Resilience: Ask Bruce." Video, *Ask Bruce*, episode three (video). IBM Resilient, November 2, 2015. https://www.youtube.com/watch?v=5KppAKeoUns.

IT Governance. "Cyber Resilience." IT Governance. Accessed May 18, 2018. https://www.itgovernance.co.uk/cyber-resilience.

Khan, Omera, and Daniel A. Sepulveda Estay. "Supply Chain Cyber-Resilience: Creating an Agenda for Future Research." *Technology Innovation Management Review* 5, no. 4 (April 2015): 6–12. http://timreview.ca/article/885.

Krebs, Brian. "Target Hackers Broke in Via HVAC Company." *Krebs on Security* (blog). February 14, 2014. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

Leuprecht, Christian, and Stephanie MacLellan, eds. *Governing Cyber Security in Canada, Australia and the United States*. Waterloo, ON: Centre for International Governance Innovation, 2018. https://www.cigionline.org/sites/default/files/documents/SERENE-RISCweb.pdf.

Mandel-Campbell, Andrea. "Developing an Effective Communication Strategy for After a Breach." Plenary session at the conference Cyber Security 2018: Building Resilience Now and For the Future, Ottawa, ON, March 1–2, 2018.

Olcott, Jake. "Cybersecurity vs. Cyber Resilience: A Quick Comparison of Terms." *BitSight*, December 7, 2017. https://www.bitsighttech.com/blog/cyber-resilience.

Ponemon Institute. *2017 Cost of Data Breach Study.* Traverse City, Michigan: Ponemon Institute, June 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&.

—. *The Third Annual Study of the Cyber Resilient Organization*. Ponemon Institute, Traverse City, Michigan: Ponemon Institute, March 2018. https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2018_Cyber_Resilient_Organization_Study.pdf?hsCtaTracking=81d7f4d1-c1a7-4ad6-99af-b93cf3a8fe39%7C2480333d-1f9e-4b70-a4e3-d4af11cee2ab.

Ponemon, Larry. "Learning to Thrive Against Threats." *Ponemon Sullivan Privacy Report* (blog), September 18, 2015. http://ponemonsullivanreport.com/2015/09/learning-to-thrive-against-threats/.

Ranger, Steve. "What Is the IoT? Everything You Need to Know About the Internet of Things Right Now." *ZDNet,* January 19, 2018. https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/.

Reef Resilience Network. *Ecological Resilience*. January 26, 2018. Accessed May 18, 2018. http://www.reefresilience.org/resilience/what-is-resilience/ecological-resilience/.

Rouse, Margaret. "Business Resilience," *TechTarget.* TechTarget Network, January 2014. https://searchcio.techtarget.com/definition/business-resilience.

Samsung. *The Open Economy*. Samsung/Knox. 2017. Accessed July 5, 2018 https://samsungatwork.com/files/Samsung_OpenEconomy_Report.pdf.

Systemic. *The Cyber Resilience Blueprint: A New Perspective on Security*. Mountainview, California: Systemic, 2014. https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf.

U.S. Department of Homeland Security. *Cyber Resilience White Paper: An Information Technology Sector Perspective*. March 2017. http://www.it-scc.org/uploads/4/7/2/3/47232717/it_sector_cyber_resilience_white_paper.pdf.

Vroegop, Ruben. *Communicating Cyber Security to the Board of Directors*. Ottawa: The Conference Board of Canada, July 2017.

Warzala, Gary. "What Does Good Cyber Resilience Look Like?: Building a Solid Information Security Strategy," *The AXELOS Blog.* Axelos, February 24, 2016. https://www.axelos.com/news/blogs/february-2016/good-cyber-resilience-info-security-strategy.

World Economic Forum. *Partnering for Cyber Resilience*. Geneva: World Economic Forum, 2012. http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.

Insights. Understanding. Impact.

e-Library.

Do you want to have access to expert thinking on the issues that really matter to you and your organization?

Our e-Library contains hundreds of Conference Board research studies in the areas of Organizational Performance, Economic Trends and Forecasts, and Public Policy.

The Conference Board of Canada
Le Conference Board du Canada

www.e-library.ca

About The Conference Board of Canada

We are:

- The foremost independent, not-for-profit, applied research organization in Canada.
- Objective and non-partisan. We do not lobby for specific interests.
- Funded exclusively through the fees we charge for services to the private and public sectors.
- Experts in running conferences but also at conducting, publishing, and disseminating research; helping people network; developing individual leadership skills; and building organizational capacity.
- Specialists in economic trends, as well as organizational performance and public policy issues.
- Not a government department or agency, although we are often hired to provide services for all levels of government.
- Independent from, but affiliated with, The Conference Board, Inc. of New York, which serves nearly 2,000 companies in 60 nations and has offices in Brussels and Hong Kong.

Insights. Understanding. Impact.

Building Cyber Resilience
Rachael Bryson

To cite this briefing: Bryson, Rachael. *Building Cyber Resilience*. Ottawa: The Conference Board of Canada, 2018.

The Conference Board of Canada

255 Smyth Road, Ottawa ON
K1H 8M7 Canada
Tel. 613-526-3280
Fax 613-526-4857
Inquiries 1-866-711-2262
conferenceboard.ca

Publication 9796 | 9822
PRICE: Complimentary