

20 Questions Directors Should Ask about Cybersecurity

Richard Wilson, CISSP





20 Questions Directors Should Ask about Cybersecurity

Richard Wilson, CISSP

DISCLAIMER

This paper was prepared by the Chartered Professional Accountants of Canada (CPA Canada) as non-authoritative guidance.

CPA Canada and the authors do not accept any responsibility or liability that might occur directly or indirectly as a consequence of the use, application or reliance on this material.

© 2019 Chartered Professional Accountants of Canada

All rights reserved. This publication is protected by copyright and written permission is required to reproduce, store in a retrieval system or transmit in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise).

For information regarding permission, please contact permissions@cpacanada.ca

Preface

The Corporate Oversight and Governance Board (COGB) of the Chartered Professional Accountants of Canada (CPA Canada) has commissioned this *20 Questions Directors Should Ask about Cybersecurity*, to help boards understand their role in overseeing this critical and evolving risk.

The COGB would like to thank the author, Richard Wilson, the significant security and privacy expertise contributed by David Craig, Alexandre Pacheco, Vivek Jassal, and the CPA Canada staff who provided support and direction for the project.

Thomas Peddie, FCPA, FCA

Chair, Corporate Oversight and Governance Board

Author

Richard Wilson, CISSP

Project Direction, CPA Canada

Stefan Mihailovich, GPLLM, CPA, CA

Gigi Dawe, LL.M.

Gord Beal, CPA, CA, M.Ed.

Corporate Oversight and Governance Board

Thomas Peddie, FCPA, FCA

Chair

Hugh Bolton, FCPA, FCA

John E. Caldwell, CPA, CA

Andrew Foley, J.D.

Carol Hansell, LL.B., MBA, F. ICD

Bill McFarland, FCPA, FCA

Kathleen O'Neill, FCPA, FCA, ICD.D

Hari Panday, FCPA, FCGA, ICD.D

Bob Strachan, FCPA, FCMA, C.Dir

John E. Walker, CPA, CA, LL.B.

Table of Contents

Preface	III
Part A: Cybersecurity Strategy, Governance, and Risk	1
1. What should directors look for in a comprehensive cybersecurity strategy?	1
2. How should the board best organize itself to govern cybersecurity effectively?	5
3. How does management identify, assess, prioritize, and report on cybersecurity risk?	6
4. What cybersecurity training and awareness program is in place?	6
5. How is management establishing an effective cybersecurity culture?	7
6. What are the organization's cybersecurity compliance obligations and their implications across all relevant jurisdictions?	8
7. How does management establish independent assurance about the design and effectiveness of their cybersecurity program and controls?	9
8. How does management determine whether they are allocating the appropriate budget and resources to manage cyber risk effectively?	11
Part B: Attackers, Motives, and Techniques	14
9. Who (and what type of attacker) is most likely to successfully compromise the organization and why?	14
10. How is the organization likely to be breached?	15

Part C: Identify What Is Most Important to the Organization and How it Is Vulnerable	16
11. How has management defined and located the most valuable digital and physical assets (aka “Crown Jewels”) that could be compromised by a cybersecurity attack?	16
12. Where are the company’s vulnerabilities located in the corporate IT and operational technology environments?	18
13. How does management confirm that its third-party cybersecurity risks (e.g., contractors, suppliers and partners) are being managed effectively?	20
Part D: Effective Security Protection	22
14. What is management’s “defence-in-depth” strategy for combining layers of protection for the organization’s most valuable assets?	22
15. How is management creating accountability for each component of the security program?	23
16. How does management embed security into the development of new processes and systems?	26
Part E: Detecting Cybersecurity Events	27
17. What processes and tools are in place to alert management when a breach attempt is underway?	27
Part F: Response and Recovery from a Breach	29
18. How are management and the board equipped to respond to, and recover from, a cybersecurity breach?	29
19. What is management’s cyber insurance strategy?	31
Part G: Reporting	34
20. How does management assess and report on its cybersecurity program to the board?	34

PART A

Cybersecurity Strategy, Governance, and Risk

1. What should directors look for in a comprehensive cybersecurity strategy?

To begin a cybersecurity governance dialogue with management, directors are encouraged to apply the same common sense framework as they apply to other organizational strategies. The following are elements that directors can probe for:

Management's cybersecurity strategy:

- a. considers the key cybersecurity risks that could directly prevent the organization from achieving its strategic objectives. For example, a financial institution's cybersecurity strategy would carefully consider the risks to their strategic plan.

Financial Service Organization's Objective	Cybersecurity Risk	Cybersecurity Strategy
Grow retail customer base	theft of customer banking data	strong controls over customer data
Provide accurate financial reporting	compromise of transaction capabilities	redundant transaction systems
Maintain the bank's positive brand image and reputation	release of confidential internal management communications	strong controls over access to management and board communications

- b. prioritizes capital and operational security funding of resources, processes, and technologies as the highest security risks to the organization;
- c. aligns efforts of a cybersecurity program between:

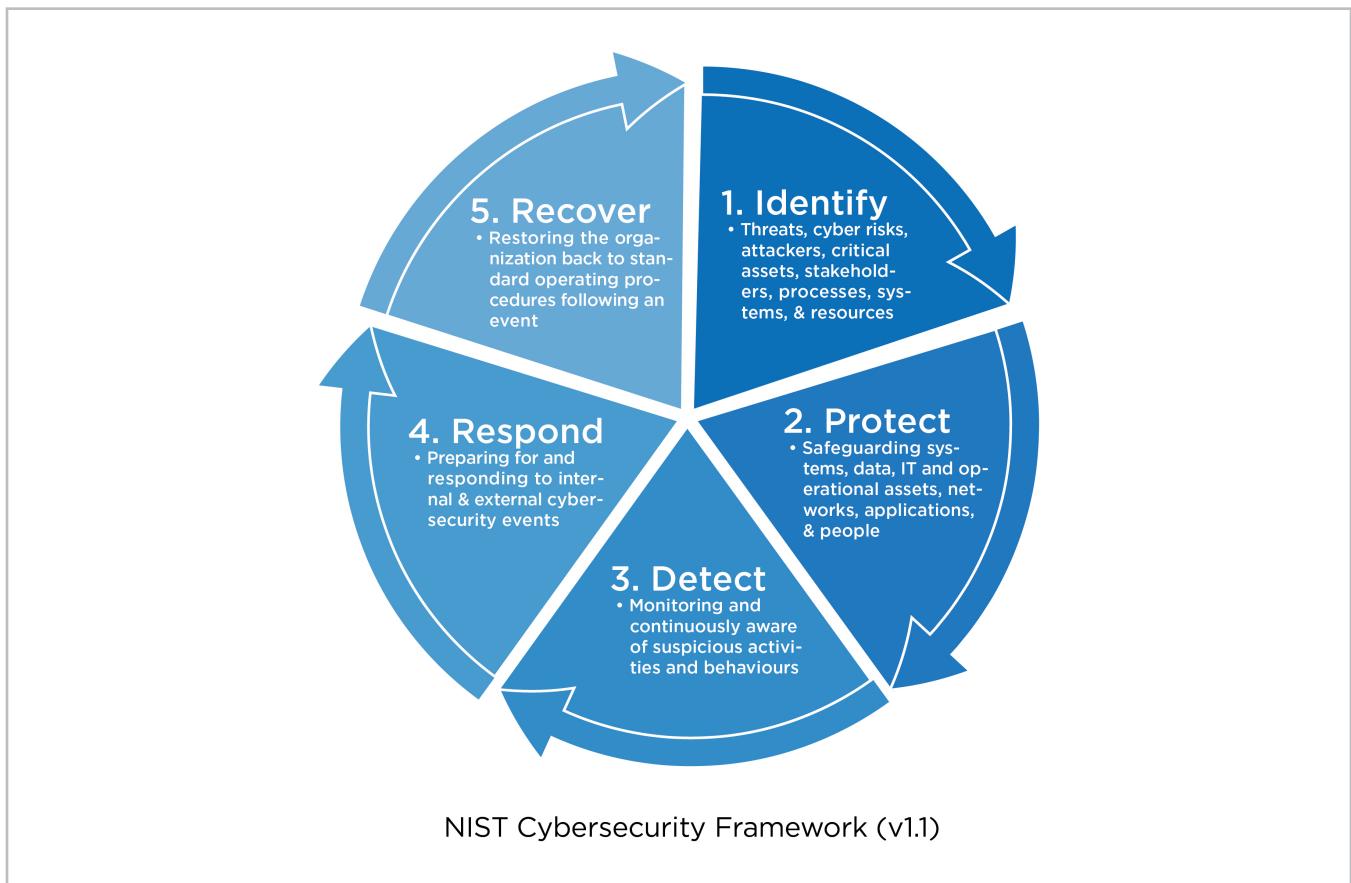
- different organizational divisions and also geographically dispersed teams
- internal, co-sourced and outsourced security teams
- information technology (IT), and operational technology (OT) teams
- cybersecurity programs and privacy programs.

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Layers:

A sound cybersecurity strategy combines multiple layers of security on the reasonable assumption that, if one layer fails, there are subsequent processes, systems, and tools to thwart a breach attempt. Drawing from one of the most recognized cybersecurity frameworks, the National Institute of Standards and Technology, (NIST), there are five layers of protection that directors should look for in an effective cybersecurity strategy (see Figure below).

NIST is intuitive as a sequence of steps.

5 LAYERS OF NIST CYBERSECURITY FRAMEWORK (CSF)



NIST CSF Function (Layers)	Definition of NIST CSF Function	NIST CSF Categories (by Function)
Identify	<p>To operate an effective cybersecurity program, management must first <i>Identify</i> several important components in order to focus time and resources efficiently and effectively. These include:</p> <ul style="list-style-type: none"> internal and external cybersecurity threats and risks internal and external attackers (i.e., threat actors) most important assets to secure against a cyber attack (e.g., customer and employee data, critical IT systems, critical operational systems) stakeholders responsible for establishing an effective cybersecurity program processes, systems, and resources that should be in place to establish and run the cybersecurity program. 	<ul style="list-style-type: none"> asset management business environment governance risk assessment risk management strategy supply chain risk management
Protect	<p>Following the <i>Identify</i> stage, management should take action to adequately <i>Protect</i> the organization.</p> <p>Discussions around cybersecurity protection can become quite technical. Directors who are not able to engage management at a technical level can inquire about the following capabilities:</p> <ul style="list-style-type: none"> Does management have security in place to control access to physical and digital (i.e., logical) assets and associated facilities? Is access limited to authorized users, processes, and devices, and is the level of access consistent with the level of risk associated with each asset? Are the organization's personnel and partners provided with cybersecurity awareness education and training (see Question 4)? Is the security of information and records (data) proportionate to the level of risk of loss or compromise of those data records? Does management have appropriate security policies, processes and procedures that are followed consistently? <p>For additional details about protection, please see Part D: Effective Security Protection, and also Question 14 regarding defence-in-depth.</p>	<ul style="list-style-type: none"> identity management, authentication and access control awareness and training data security information protection processes and procedures maintenance protective technology

NIST CSF Function (Layers)	Definition of NIST CSF Function	NIST CSF Categories (by Function)
Detect	<p><i>Detect</i> is NIST's third layer of a cybersecurity strategy. This layer can be compared to a home security strategy. If the <i>Protect</i> layer includes fences, window bars, and door locks, then the <i>Detect</i> layer would be security cameras, motion sensors, and the security monitoring centre.</p> <p>Directors should be familiar with the term, "anomalous activity," which describes activities by systems or people that fall outside expected behaviours. Anomalies are security triggers that management should watch for.</p> <p>Management should set up detection capabilities that monitor the organization for potential security events, which will trigger responses (see Part E - Detecting Cybersecurity Events for additional details).</p>	<ul style="list-style-type: none"> • anomalies and events • continuous security monitoring • detection processes
Respond	<p>Despite best efforts, security breaches are inevitable. When these events occur management needs to have an effective ability to <i>Respond</i>.</p> <p>NIST prescribes that management's response activities be co-ordinated with internal and external stakeholders (e.g., external support from law enforcement agencies). Analysis of security events should be conducted to inform management about their nature and intent.</p> <p>Effective response activities can prevent or limit the expansion of an event and its impact on the organization. Continuous learning will improve organizational response activities in the future (see Part F: Response and Recovery from a Breach).</p>	<ul style="list-style-type: none"> • response planning • communications • analysis • mitigation • improvements
Recover	<p>Formalized cybersecurity <i>Recovery</i> capabilities are often among the last that management teams master. Directors are encouraged to ask management for evidence that recovery capabilities are in place to:</p> <ul style="list-style-type: none"> • restore systems or assets affected by cybersecurity incidents; these could include data back-ups, application, networks, and IT and operational systems • co-ordinate restoration activities with internal and external stakeholders (e.g., co-ordinating centres, Internet service providers, data centres, cloud system providers, owners of attacking systems, victims, other computer security incident response teams (CSIRTs — see Glossary of Terms), and vendors to name a few (see Part F: Response and Recovery from a Breach) 	<ul style="list-style-type: none"> • recovery planning • communications

2. How should the board best organize itself to govern cybersecurity effectively?

In order to provide effective cybersecurity governance, a board must decide how best to organize itself around the task. There are several models with pros and cons for each (see table below).

In all cases, the board has a responsibility to include cybersecurity as an essential skill within the board's skills matrix, and to populate the board accordingly. It is advisable to have a range of cyber skills spread across multiple directors rather than rely on only one person to interpret cybersecurity reports.

Cyber governance leadership	Pros	Cons	Conclusion
Cyber led by audit committee	<ul style="list-style-type: none"> analytical mindset trust-but-verify approach related IT audit experience 	<ul style="list-style-type: none"> can lean toward a compliance approach may have fewer relevant technical skills 	possible
Cyber led by risk committee	<ul style="list-style-type: none"> risk-based perspective related IT risk governance experience 	<ul style="list-style-type: none"> cyber only one of many risks being examined 	favourable
Cyber led by a cybersecurity committee	<ul style="list-style-type: none"> specialized team skills result in a high-quality governance 	<ul style="list-style-type: none"> sub-committee for each governance topic unrealistic 	favourable
Cyber led by full board	<ul style="list-style-type: none"> aware of key cyber risks and initiatives broad base of questions and perspectives 	<ul style="list-style-type: none"> too many people for governance possible lack of minimum skills to govern responsibly 	possible

While no single governance model applies to all boards, a combination of the above scenarios may be a good solution for many boards.

Recommendation: Assign responsibility for cybersecurity to a risk committee. Dashboard reports with recurring metrics (see [Part G](#)), could be delivered quarterly, with semi-annual presentations to the full board.

3. How does management identify, assess, prioritize and report on cybersecurity risk?

How can a board effectively engage with management on the topic of cybersecurity risk? To do so, management needs to execute a well-designed cyber risk management process. Without being overly prescriptive, directors are encouraged to look for the following elements within an effective cybersecurity risk management program.

- A sound cybersecurity risk program begins with a summary of the organization's strategic priorities (corporate objectives, processes and assets).
- The program should identify the key potential cyber threats, vulnerabilities and risk events that would negatively impact the organization's priorities.
- As with enterprise risk management (ERM) programs, cybersecurity risk events are identified and then assessed using impact and likelihood criteria.
- Management should establish risk targets (using the same impact and likelihood scales) to confirm the acceptable risk level for each potential risk event.
- Management should provide a cybersecurity risk response plan that identifies the controls and other actions needed to reduce each risk to its target level.
- An accountable risk owner should be assigned to each cybersecurity risk event. They may or may not be responsible for implementing controls, but they will retain ultimate accountability for having effective controls in place and operating as expected.
- Management should establish and populate a cybersecurity risk register to hold all pertinent information for their program, such as risk events, assessment scores, risk target scores, related controls for risk events, and comments.

A well articulated cybersecurity risk assessment will enable management to create a cybersecurity operating model prioritized by key risks. This will translate into a prioritized execution plan with a roadmap, resourcing plan and budget to achieve the goals within the cybersecurity operating model.

4. What cybersecurity training and awareness program is in place?

Many cybersecurity breaches originate from employees clicking malicious links within phishing emails. While some phishing attacks are very difficult to detect, an educated workforce that looks for suspicious emails will dramatically reduce this risk. Since elimination of this risk is not likely, continuous education in cybersecurity attack techniques is an essential control for any organization that communicates via email.

The key stakeholders who should receive cybersecurity training are:

- board
- management and staff
- third parties with access to the organization's systems (e.g., contractors, consultants, vendors, partners)

Note: Educate customers to avoid cybersecurity scams that can fool them into revealing confidential data that will expose the organization to fraudulent losses.

Channels that management can employ for cybersecurity training include:

- webinars
- in-person presentations
- eLearning tests
- workstation and worksite posters and signage
- screensavers and on-screen reminders
- simulated attack testing (e.g., simulated email or phone phishing campaigns, USB baiting).

The frequency of training and testing should be proportionate to the risk of attack. Financial service or retail companies will train with greater frequency than an organization with a less networked workforce.

Note: A key cybersecurity metric recommended for board reports is the percentage of employees, (and board members) who succumbed to a simulated cyber attack during a training exercise. The target is 0%!

5. How is management establishing an effective cybersecurity culture?

According to The European Union Agency for Network and Information Security (ENISA), “The concept of Cybersecurity Culture (CSC) refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest themselves in people’s behaviour with information technologies.”¹ Unfortunately, establishing an effective cybersecurity culture can be more difficult than implementing the most complex security software platform. Management teams will encounter many challenges as they try to reach this goal:

- Mistaking cybersecurity for an “IT issue” obscures the role each employee must play in security.
- Translating complex security topics into digestible messages is a skill often still being developed within organizations.
- Convenience at the expense of security can sometimes stall cultural adoption.

Directors play an important role in driving cybersecurity culture. They should direct management to:

- articulate what a target cybersecurity culture should look like so the final vision engages all levels and departments (see [Question 4](#) on Training)
- demonstrate how the directors are driving security culture top-down

¹ Cyber Security Culture in Organisations, November 2017 (www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport)

- present a cybersecurity training curriculum that will help build an effective culture across both IT and OT teams
- demonstrate how management rewards good cybersecurity behaviours such as reporting potentially malicious emails before clicking them.

ARE WE SECURE YET?

Directors may be inclined to ask management about the status of security programs. While this is a legitimate inquiry, directors are encouraged to avoid the question, “Are we secure?”. This implies that security is a project with a point of completion. In fact, cybersecurity is an ongoing process that requires constant review and improvement. External changes such as new threat actors and evolving attack techniques, as well as internal changes to IT and OT environments, will present new vulnerabilities to address.

Additionally, even the most diligent organizations will always have some areas of exposure. It is simply not possible to create an absolute level of security.

For these reasons, directors are encouraged to replace this question with, “How close are we to reducing our cybersecurity risk to targeted levels?”. This will lead to a more productive, risk-based security discussion.

6. What are the organization’s cybersecurity compliance obligations and their implications across all relevant jurisdictions?

Cybersecurity compliance requirements differ across sectors and geographies and over time. Given this, it is therefore impractical to address all compliance standards within this publication. Rather, below is a set of important questions directors should pose to management regarding their organization’s cybersecurity compliance obligations:

- Does management have a comprehensive understanding of the full set of cybersecurity compliance obligations with which the organization must comply?
- Are the compliance standards more directive or principles-based (i.e., requiring interpretation) or are they prescriptive?
- What are the fines and penalties for non-compliance?
- What effort and cost are required to become compliant versus maintaining compliance?
- Once compliant, will we have reduced our risk to acceptable levels, or are additional effort and cost required? If so, what, where and how much?
- Has management designated an internal function accountable for maintaining cybersecurity compliance?

- What are the key standards with which the organization must comply, what are the key dates, and how is management tracking towards successful compliance by the deadline?
- How is management going to engage the regulatory body if compliance is unsuccessful?

To provide insight into the manner of compliance required by current standards, a sample is provided below:

Samples of cybersecurity compliance requirements

- identifying critical cybersecurity assets that could be compromised (risk ranked)
- establishing a minimum standard of security management controls
- training personnel (incl. employees, contractors, and vendors) who have certain levels of access to critical systems
- maintaining general cyber awareness for all employees
- setting both electronic and physical perimeters and deterrents for critical cybersecurity assets
- limiting access to systems and data to only those individuals whose role requires such access
- establishing and rehearsing incident response (IR) and recovery capabilities
- requiring mandatory notifications for stakeholders affected by a breach
- setting and maintaining minimum data encryption requirements
- maintaining confidentiality, integrity, and availability (CIA) of data and systems
- establishing minimum and maximum retention periods before safe disposal of data
- requiring mandatory audit histories
- etc.

Third-party assessments of the organization's cybersecurity compliance requirements via external and internal auditors and other assurance service providers will give the board additional comfort that obligations are being met within each jurisdiction (see also Question 7).

7. How does management establish independent assurance about the design and effectiveness of their cybersecurity program and controls?

Assessments of Established Cybersecurity Frameworks

As with other areas of assurance, management is advised to request independent assessments using established cybersecurity standards. The obvious benefits of these reviews are comfort with current security maturity levels and controls and receipt of recommendations to enhance security risk management and performance.

A non-exhaustive list of general reference standards includes:

- **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)** (see Question 1 for an overview): suitable for organizations of all sizes and sectors
- **AICPA's Description Criteria for Management's** Description of the Entity's Cybersecurity Risk Management Program along with the TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy²
- **ISO/IEC 27001 and 27002:** suitable for organizations of all sizes and sectors
- Control Objectives for Information and related Technology (COBIT): developed by ISACA, a global organization that focuses on IT governance; suitable for medium to large organizations across most sectors
- **The Centre for Internet Security (CIS) Critical Security Controls:** a recommended set of actions for cyber defense that provides specific ways for management to mitigate the most pervasive and dangerous attacks
- **Information Security Forum (ISF) Standard of Good Practice:** originating from Europe, ISF has established a central benchmarking service as part of its standard (requires membership fee); suitable for organizations of all sizes and sectors
- **ANSI/ISA 62443 (formerly ISA-99):** a series of standards and reports focused on establishing electronically secure industrial automation and control systems (IACS).
- **IASME Governance:** a UK-based standard for information assurance at small-to-medium size organizations; achieves an accreditation similar to ISO 27001 with reduced complexity

Note: Standards specific to unique sectors are too many to list here.

² See: www.aicpa.org/cybersecurityriskmanagement or CPA Canada's guide: [Reporting on an Entity's Cybersecurity Risk Management Program and Controls](http://www.aicpa.org/reportingonanentityscybersecurityriskmanagementprogramandcontrols)

Audits

Internal audit is well suited to routinely audit cybersecurity against policy, procedure or compliance obligations. An external audit review of information technology general controls (ITGCs), which can apply to more than just financial systems, components, processes, and data for an organization's IT environment, is another source of independent assessments. But in order to challenge the organization beyond routine audits, the following areas should also be seeded into multi-year audit cycles:

- business compliance with internal cybersecurity policies and procedures
- security incident response processes
- physical security of cyber assets
- compliance with mandatory cybersecurity user education programs
- unauthorized or misconfigured access to devices containing or processing sensitive information
- timely patching of applications, operating systems and other device firmware.

Third-Party Penetration Testing

Penetration testing (pen-testing) is a simulated hacking attempt authorized by the organization against applications, computer systems, digital devices, and/or networks. The goal is to evaluate the security of the target environment, detect vulnerabilities within these environments, and assess the response and recovery capabilities of management's security systems and teams.

A few important insights for directors presented with pen-testing results are:

- A pen-test represents security at a moment in time. If security systems, or attack techniques change, the validity of the pen-test results may diminish.
- Pen-testing an organization is like leak-testing a boat. If the vessel is put in the water before the hull is sound, water will rush in. Similarly, pen-testing a system or environment when its security is known to be immature is not a good use of security funds since a breach will almost certainly be detected.
- When viewing pen-testing results, find out whether breaches were achieved purely through technical compromise or by tricking a person into clicking a malicious email link. The former illustrates technical control issues, whereas the latter is a training and culture issue.

8. How does management determine whether they are allocating the appropriate budget and resources to manage cyber risk effectively?

While cybersecurity can often appear to be a complex technical topic, directors can take comfort that the planning and execution of a cybersecurity program is quite similar to strategic planning conducted for other areas of the organization. Directors should inquire whether management is following these steps in their development of a cyber plan and budget:

1. Show the relationship between the company's corporate objectives & key cyber threats

2. Identify the key cyber risk events that would prevent the company from achieving its objectives

3. Assess to prioritize the cyber risks. Then, agree with management what your cyber risk target levels are

4. Design a Cybersecurity Operating Model that's prioritized based upon the key risks assessed

5. Develop a Roadmap & Resourcing Plan for the Security Operating Model, & Budget (Capex & Opex)

6. Confirm a Cyber Governance Team to approve re-sourcing, process, technology, & funding

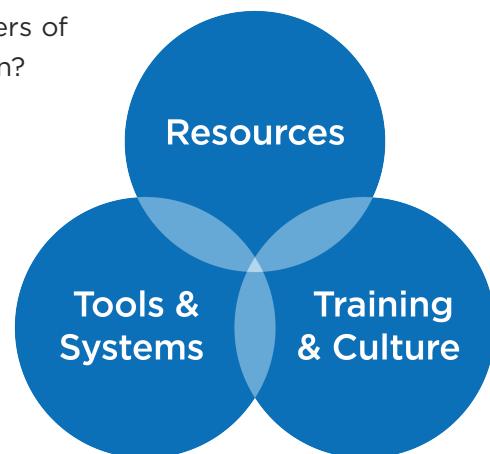
7. Develop a cyber dashboard to track program performance

Insights and context for directors on this process are as follows:

1. The principal reason for cybersecurity programs is to protect the organization and increase the likelihood it will achieve its objectives.
2. Cyber risk to the organization is a combination of threats executed against vulnerabilities in the presence or absence of effective controls and culture. If management is assessing more than 25 types of cyber risk events, then a review of the cyber risk assessment process is in order.
3. The cyber risk assessment process should be aligned with the organization's enterprise risk management (ERM) assessment methodology (e.g., impact and likelihood).
4. Cybersecurity programs should be designed based on previously assessed risks. This drives a top-down, risk-informed cyber program. The absence of risk assessments usually leads to bottom-up designs that can lack prioritization of efforts and spending.
5. Similar to 4, cybersecurity roadmaps should cascade based on risk. The highest risks will be addressed sooner than lower risks. While this sounds highly intuitive, risk-based plans are still new approaches to many cybersecurity teams.
6. Cross-functional cyber governance teams will effectively represent the broad range of disciplines within an organization.
7. Boards should insist on a repeatable set of metrics to be reported (see [Question 20](#)).

When reviewing cybersecurity budgets, directors should be mindful to look for the right combination of factors.

1. Is management hiring or contracting adequate numbers of skilled resources to execute against the proposed plan?
2. Is management enabling the cybersecurity team with the technologies, tools and systems needed to be effective?
3. Has cybersecurity leadership been granted the appropriate authority to execute its role effectively?
4. Has management provided adequate training to reasonably prevent employees and contractors from inadvertently exposing the organization to inbound attacks?



Collaboration with others is now necessary for effective cybersecurity programs. Some industry groups share information about cybersecurity events, trends, insights, etc. Part of sharing is asking others about the size of their budgets for operating expenses and capital programs. Have management share their insights gained through these forums. If they are not participating in them, find out why.

Finally, cyber research agencies such as Forrester have published reports and studies to guide management and the board on industry norms. If a company is just starting on its cybersecurity journey, spending may have to be higher.

**BREAKDOWN OF COMPANIES' IT BUDGET/DEPARTMENT'S BUDGET THAT WILL BE SPENT ON SECURITY IN 2018
(BY INDUSTRY)**

% of budget spent on security	Manufacturing	Retail and wholesale	Business services and construction	Utility and telecom	Financial services and insurance	Public sector and healthcare
0% to 10%	25%	9%	16%	18%	31%	31%
11% to 20%	33%	40%	26%	38%	31%	29%
21% to 30%	18%	19%	23%	32%	20%	21%
Other	23%	33%	35%	12%	18%	19%

Base: 34 to 103 global security technology decision makers at a director or VP level or who report to the CIO (base sizes vary by industry)

Source, Forrester Analytics Global Business Technologies Security Survey, 2018.

PART B

Attackers, Motives, and Techniques

9. Who (and what type of attacker) is most likely to successfully compromise the organization and why?

	Adversary	Motives	Targets	Impact	Threat Vectors
External Threat Landscape	Nation State	<ul style="list-style-type: none"> Economic, political, and/or military advantage Economic, political, and/or military advantage National security Fraud 	<ul style="list-style-type: none"> Trade secrets Sensitive business information Emerging technologies Critical infrastructure 	<ul style="list-style-type: none"> Loss of competitive advantage Disruption to critical infrastructure Loss of intellectual property Monetary loss 	<ul style="list-style-type: none"> Targeted, long term cyber campaigns with strategic focus Insider weakness/lack of knowledge Third party service providers
	Cyber Criminals	<ul style="list-style-type: none"> Immediate financial gain Collect information for the future financial gains Fraud Identity Theft 	<ul style="list-style-type: none"> Financial/Payment Systems Personally identifiable information Payment card information Protected health information Intellectual property 	<ul style="list-style-type: none"> Regulatory inquiries and penalties Consumer/shareholder lawsuits Reputational and financial damage Data breach Loss of intellectual property 	<ul style="list-style-type: none"> Targeted cyber campaigns Insider weakness/lack of knowledge Third party service providers
	Cyber Terrorists	<ul style="list-style-type: none"> Political and/or ideological change Create fear, uncertainty, and doubt Malicious havoc 	<ul style="list-style-type: none"> Critical infrastructure Operational technologies Highly visible 	<ul style="list-style-type: none"> Destabilize, disrupt, and destroy physical and logical assets 	<ul style="list-style-type: none"> Opportunistic vulnerabilities Insider weakness/lack of knowledge Third party service providers
	Hacktivists	<ul style="list-style-type: none"> Influence political and/or social change Pressure business to change their practices 	<ul style="list-style-type: none"> Corporate secrets Sensitive business information Information related to key executives, employees, customers, & business partners 	<ul style="list-style-type: none"> Distribution of business activities Brand and reputation damage Loss of consumer 	<ul style="list-style-type: none"> Targeted organizations that stand in the way of their cause Insider weakness/lack of knowledge Third party service providers
Internal Threat Landscape	Insiders	<ul style="list-style-type: none"> Personal advantages, monetary gain Professional revenge Patriotism 	<ul style="list-style-type: none"> Sales, deals, market strategies Corporate secrets, intellectual property, research, & development Business operations Personnel information 	<ul style="list-style-type: none"> Trade secret disclosure Operational disruption Brand and reputation damage 	<ul style="list-style-type: none"> Pre-authorized access Insider knowledge

With regard to threat actors, boards should understand:

- which threat actors the organization faces
- what the organization does or has that may interest threat actors
- any steps management has taken to mitigate the risk of a repetition of any threats already perpetrated against the company or its industry
- whether the management is staying abreast of current cyber threats by reading cyber threat intelligence reports that can be actioned
- that management is providing meaningful cyber threat and awareness briefings on a regular basis.

10. How is the organization likely to be breached?

Before understanding how the organization may be breached, management must first understand the environment. Understanding what is most important to achieving the organization's aims and strategic objectives will enable informed cybersecurity decisions to be made. A risk assessment will discover the strength and vulnerability of cybersecurity controls. This assessment will tell the board how the organization might be breached, the likelihood of such a breach and its potential impact.

Most importantly, by understanding how the organization might be breached, the board can decide where to invest financial and other resources to mitigate current and emerging threats.

There are many ways an organization can be breached; the next section provides insight into how to manage these risks. Threats can come from a third party, supplier, be internal or (depending on the organization's industry) a cyber criminal organization or nation state.

Boards should verify management has done the following to reduce the impact of a breach:

- completed a risk assessment to provide information as to what cybersecurity controls are in place and any potential gaps in defences
- checked that the tools and processes are in place to enhance the visibility of the organization's environment and that management understands the organization's threat landscape
- conducted a threat-modelling exercise based on the results of the risk assessment and analysis of the threat landscape to simulate how the organization may be breached.

Note: A risk assessment is a snapshot at just one moment in time. It should be constantly updated along with other risk-mitigation plans.

PART C

Identify What Is Most Important to the Organization and How it Is Vulnerable

11. **How has management defined and located the most valuable digital and physical assets (aka “Crown Jewels”) that could be compromised by a cybersecurity attack?**

The NIST Cybersecurity Framework (CSF) was developed knowing that not all information and system assets can be protected all the time from every conceivable threat. Organizations will never have the resources, financial or human, to protect 100% of their valuable assets. As a result, management will have to determine some classification for assets and then take action to protect them using appropriate controls. The most sensitive assets are often referred to as “Crown Jewels,” giving them a special status within an enterprise.

The most common crown jewels include:

- personal data for current and former customers, employees, contractors and investors
- pre-released financial information, merger and acquisition insights, contracts, business agreements, litigation documents, etc.
- intellectual property including designs, network diagrams, recipes, patent applications, etc.
- information and operational technology such as supervisory control and data acquisition (SCADA) systems, customer relationship management applications
- any system/application whose disruption, would have a significant impact on operations
- any system/application whose abuse or compromise could have significant fraud implications.

For example, the personal information of an organization's customers and employees is a very sensitive asset. Loss or theft requires public notification of the individuals affected and, quite often, of a federal or provincial privacy commissioner. An enterprise may also classify its financial data as very sensitive before public release. The price list of goods or services may or may not be sensitive depending on the nature of the business. The more sensitive the data, the tighter and more restrictive the controls needed.

Less certain is whether management considers email a sensitive corporate asset. They should consider, however, that most inadvertent disclosures of sensitive information happen through email. Even more difficult is identifying some of the systems that control the operation and use of information assets. A crown jewel can be both an information asset and a system or application. Some crown jewels are also paper assets such as signed customer contracts.

Directors should ask management:

- Have you established the data classification schema?
- Have you specified the protective controls required at each level?
- What is the current state of the most sensitive data being protected to the level required by policy? For example, if only 10% of the critical data is protected according to policy, it shows that there is much more work to do to protect those crown jewels.
- What is the status of an accurate and current inventory of that data, including where and when it is stored at third-party locations, including the cloud? The accuracy of that inventory is one of the critical success factors for reducing the risk of that data being compromised. Management cannot protect information or any digital asset if they do not know that it is present within its boundary, including when that boundary may be virtual.

Directors should ask management to share the processes for refreshing data classification, the protective controls to be applied based on classification, and how they maintain an accurate inventory of those information assets. Even if the budget is limited, the status of the crown-jewel inventory should be clear.

In general the head of IT is expected to be in charge of developing and maintaining the asset inventory. However, few organizations have centralized control in just that one person or group. Human Resources, for example, likely receives all résumés from job applicants. What do they do with those résumés not needed for current openings? Is the head of Human Resources as engaged in cybersecurity protection as the head of IT? Cybersecurity risk reduction is a team effort.

12. Where are the company's vulnerabilities located in the corporate IT and operational technology environments?

In overseeing an entity's strategy, directors should understand the technology their organization depends on to be successful. Digital technology is dissolving traditional industry boundaries and creating more opportunities for disruptors to displace incumbents. Although technology has historically been viewed as an enabler of business operations, today it is widely seen as a critical driver of growth.

Traditional forms of technology, usually referred to collectively as Information Technology or IT, were the fundamental platforms that supported the front and back office functions for most businesses. These technologies were overseen by the chief information officer (CIO).

There are, however, other technology classes that companies use to execute their strategy. Operational technology (OT) is used to enable the operations of the business. The technology system that controls the operation of an oven at a bakery or the smelter of a steel factory, for example, is OT. NIST defines OT as hardware and software that detect or cause a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. OT was not traditionally the focus of cyber attacks as most systems were not connected to the Internet. This has changed substantially with the pressure on management to increase efficiency and decrease costs. OT was traditionally overseen by the chief technology officer (CTO) or the head of engineering.

Directors need to be assured both IT and OT are included in a comprehensive cybersecurity program. Too often the CIO and CTO are siloed; as a result, the cybersecurity program is not kept equal in both areas. A fully mature IT cybersecurity program becomes less effective if the OT environment is connected to it with fewer controls. The organization may be even more at risk if there are differences. Directors should ask management about the cybersecurity culture across both technology groups.

The table below highlights the forms of IT and OT systems.

INFORMATION AND OPERATIONAL TECHNOLOGY EXAMPLES

Information Technology (IT)	Operational Technology (OT)
<ul style="list-style-type: none"> • email system • customer care and billing system • financial system • ERP system • client-facing website 	<ul style="list-style-type: none"> • point-of-sale (POS) cash registers • heating, ventilation and air conditioning (HVAC) control system • baking furnace control system • CCTV network • building management systems

The connection of more and more devices to the Internet (i.e., the Internet of Things (IoT)) is enabling many corporate strategies. From fitness trackers to home automation to vehicle telematics, these devices create data that can instantaneously help both the customer and the company that provided them.

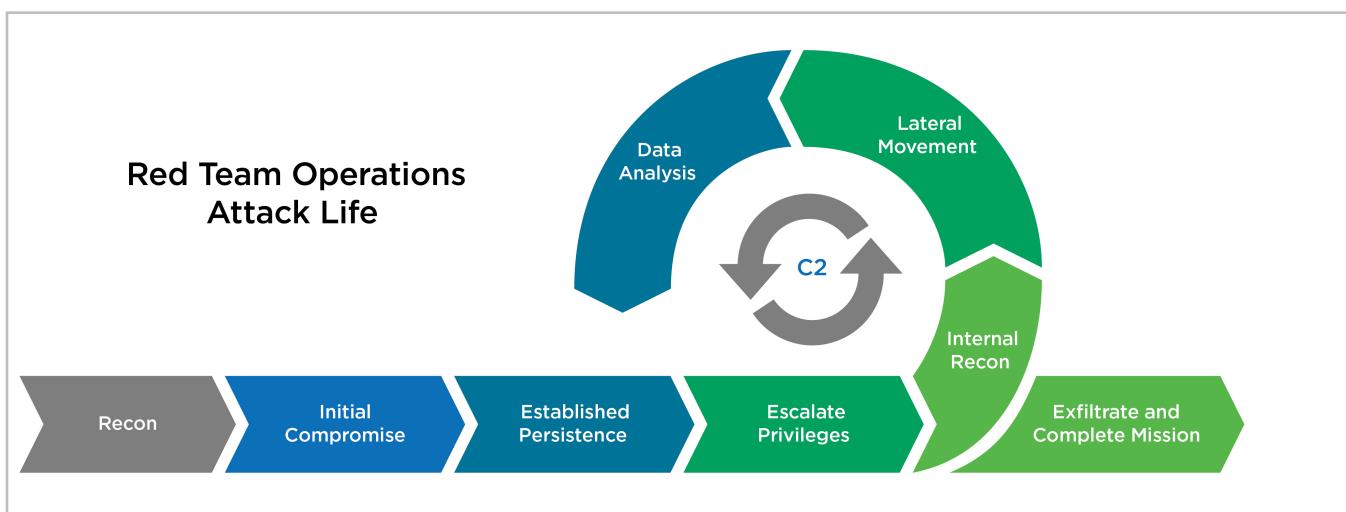
All these technologies are vulnerable to compromise.

Directors must ask management to:

- identify which vulnerabilities are relevant to the entity and put in place steps to reduce either the likelihood or the impact of the compromise (or both)
- describe the actions being taken such as technical risk assessments, penetration testing, vulnerability assessments, etc. so that a defensive course of action can be developed.

People are the core of management's ability to detect and respond to compromise attempts. For example, management could use a "red" team (i.e., a group of highly skilled external professionals) to make a simulated cyber attack on the company to show how they could compromise the environment. The information derived from this exercise would then be used to build better capabilities to detect similar activity and potentially reduce the impact of a compromise attempt.

RED TEAMING AN ATTACK TO DETERMINE VULNERABILITIES

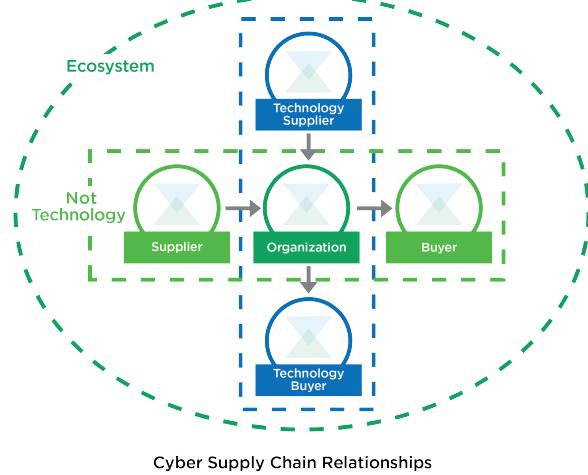


Directors should inquire about the assessments management is undertaking, why those assessments are sufficient, and what programs, such as training, process changes, new detection technologies, etc. are recommended. If directors are not comfortable assessing management's answers to their questions (i.e., competently challenging the answers), they should engage external cybersecurity professionals to provide another perspective.

13. How does management confirm that its third-party cybersecurity risks (e.g., contractors, suppliers and partners) are being managed effectively?

The NIST Cybersecurity Framework, mentioned previously, is now in Version 1.1 (April 2018). One of the key changes from version 1.0 is an emphasis on the importance of supply chain risk management (SCRM), illustrated in the adjacent Figure, in the reduction of cybersecurity risks. Companies today do not operate entirely on their own; they interconnect with clients, suppliers, buy equipment, sell used equipment, share information with external parties, regulators and others. Management must ensure its information controls are as strong, or stronger, when their data is:

- in the possession of those parties
- being transmitted to or from those third parties
- no longer needed by those third parties.



There are three fundamental elements management must have in place and that directors should therefore inquire about before data is exchanged with or obtained from third parties:

1. policies
2. contracts
3. service level objectives/agreements

To help employees and other key stakeholders understand their responsibilities for data, policies should be written and periodically updated. They should specify the acceptable use of technology; the collection, use, protection, sharing and disposal of data, etc. Policies set the guideposts for an organization and are used as the basis for training, systems development and acquisition, discipline, etc. One such policy is the enterprise privacy policy which should clearly describe how an organization will address the generally accepted privacy principles (GAPP) over the use of personal information.

The primary mechanism for the relationship between entities or parties is a commercial contract. Historically, companies would pay little attention to the clauses on information exchange, but, as version 1.1 of NIST articulates, those clauses are now critical to reducing cyber risk. Management should contractually obligate third parties to protect data, participate in resilience exercises, and maintain the confidentiality, integrity and availability (CIA) of data. Clauses should also be added to existing as well as new contracts to specify third-party liability for damages arising from their actions. These will be difficult to negotiate before an incident but will be impossible to negotiate *after*.

The board should note that one of the key contractual terms will be the entity's right to audit the third party's compliance with the information protection clauses. Just because a third party says it will perform background checks on key personnel, for example, there will likely be no assurance it has actually done so. Moreover, most third parties will not allow their customers to actually enter their premises and observe controls in action.

Companies use system and organization controls (SOC) reports to demonstrate to their clients what controls are in place and how effectively they are working over a period of time. Management will likely have to rely on these reports from key suppliers rather than actual audits.

Directors should ensure that:

- policies consistent with the entity's strategy are in place and current
- the entity is appropriately protected through commercial contracts
- there is sufficient assurance the connected third parties are behaving consistently with their obligations.

PART D

Effective Security Protection

14. What is management's "defence-in-depth" strategy for combining layers of protection for the organization's most valuable assets?

Defence-in-depth combines multiple layers of security to identify potential threats and vulnerabilities, protect the organization against internal and external attacks, detect anomalous behaviour, respond effectively to attacks, and efficiently restore the organization to standard operating conditions.

Each layer should combine internal and external resources, security software and hardware, and processes that enable these elements to work together. No single combination of security layers will apply to all organizations. In fact, different security configurations can be equally effective within the same organization.

So how can non-technical boards play a governance role in this complex discussion? The answer is to refer to a security framework such as NIST to organize governance discussions. Directors can use the five NIST CSF elements (i.e., Identify, Protect, Detect, Respond, and Recover) as a basis for governance questions. Refer to the table below as an example.

DEFENCE-IN-DEPTH

Security Layer	Examples of Security	Key Governance Questions
Identify	<ul style="list-style-type: none"> • governance • cyber threat and risk assessments • security vulnerability assessments • threat intelligence • asset management 	<ul style="list-style-type: none"> • How is management identifying the key security risks to the organization? • Where are the organization's security blind spots?
Protect	<ul style="list-style-type: none"> • identity and access management • awareness and training • data security • device and asset security • firewalls • patching • phishing campaign 	<ul style="list-style-type: none"> • Is management relying on inputs from a cyber risk assessment to design their protection strategy? • How does the organization maintain security protection during periods of change?
Detect	<ul style="list-style-type: none"> • security monitoring (e.g., SOC) • anti-malware software • detection software • proactive hunting for any malicious presence in the systems • compromise assessments • behavioural analytics 	<ul style="list-style-type: none"> • How does management measure its detection capabilities? • How does management learn and improve from past breach attempts?
Respond	<ul style="list-style-type: none"> • incident response plans and processes • security forensic analysis • response communications (internal and external) • response services 	<ul style="list-style-type: none"> • Does management have a well rehearsed response plan in place? • When does the board need to play a role in response?
Recover	<ul style="list-style-type: none"> • business continuity plans • data and system restoration/disaster recovery • redundant systems 	<ul style="list-style-type: none"> • Has management tested actual recovery techniques? • Were they successful?

15. How is management creating accountability for each component of the security program?

Whenever a post mortem is held on an incident, it is interesting to observe the behaviour of the participants in the room. Is there “finger pointing” such as, “No one knew marketing had that customer database connected to the Internet”? Is there “denial” such as, “No one said it was my job to perform a criminal background check on the administrator. How was I to know they had a history of using insider information?”



Without accountability, no one feels it is their duty to actively protect the entity. If the CEO does not reassign accountability, the CEO will be accountable for the performance of the cybersecurity function. This is not ideal since another element of accountability is having the competence to effectively execute the requirements of the role; not all CEOs are skilled in this area.

Most organizations today have a role identified as the chief information security officer (CISO). It is becoming more common for the CISO to be the accountable individual who oversees the planning, building, executing and reporting on the cybersecurity activities within the entity.

Whom the CISO reports to is also changing. Traditionally, the CISO reported to the head of IT (i.e., the CIO); however, there can be governance conflicts between the CIO and CISO and these need to be clearly understood.

Directors should be asking:

- Who is accountable for cybersecurity within the entity, and what skills and experience does that person have to be competent in their role? Is that person clearly recognizable as the leader of the cybersecurity function? Is there a need for a CISO, if one does not exist?
- How have any conflicts in reporting structure been addressed by management? Is the CISO free to speak without fear of reprisal?
- Who are the successors to the incumbent? Experienced and qualified security personnel are often heavily recruited. If the CISO left with two-weeks' notice, how has management built a succession plan that mitigates the risk of a leadership vacuum?

As mentioned previously, cybersecurity is not a technology issue; all executives and their departments play a role in reducing cybersecurity risk. The person in the accountable role (e.g., the CISO) must take steps to document the roles and responsibilities of the key cyber functions within the entity.

Key areas for which directors should ensure management has responsibilities in place are:

1. Cybersecurity strategy

This is the two-to-three-year plan for reducing the likelihood and impact of a cyber attack on the entity's vulnerabilities. This strategy is likely to follow a framework such as NIST CSF described earlier.

2. Data Classification and Asset Inventory (aka, Crown Jewel Assessment)

Not every information asset can be protected everywhere and at all times. A program must be in place to identify which data assets are most important and how they should be protected.

3. Continuous/Ongoing Threat Risk Assessment

New threats arise daily whether from the outside or from the disciplining of a troubled employee with significant access privileges on the inside. Someone must be responsible for identifying new threats and instigate appropriate mitigation measures. This will include collaborating with others to gain forward-looking insights.

4. Third-Party Management

Someone must be responsible for dealing with third parties having connections to the entity's systems. Third parties must keep the entity's data secure. The third-party manager must have the authority to disconnect third parties if they are putting the entity's reputation or data at risk.

5. Incident Response Planning and Practice

Someone must be responsible for preparing the entity's response to any compromising event. This role can be combined with business continuity management (BCM) or other disaster recovery and planning (DRP) functions.

6. Training and Awareness

This responsibility takes on additional meaning with the addition of cybersecurity training to the general training program. Stakeholders to be considered include:

- a. customers
- b. employees and contractors
- c. executives and their assistants
- d. investors and board members
- e. third parties.

Enhanced training should be provided to those who hold "privileged access" to systems and accounts, such as senior IT and OT administrators. Keeping these groups aware of their responsibilities to monitor systems for strange events, such as a phishing email or false text message, is critical to reducing the organization's overall risk exposure. As training is often the first casualty of any budget reduction, directors must ask management how these programs are being maintained or what risk is being elevated.

Directors should also be asking management in what cybersecurity programs key personnel have been certified. A well-trained cybersecurity team will have a variety of relevant training certifications as evidence of a more mature organization.

16. How does management embed security into the development of new processes and systems?

Effective security management begins by embedding proper security controls and practices into the organization's processes as early as possible; security should not be an afterthought. Embedding can be achieved by having properly defined security architecture controls and standards in place ahead of any procurement. At the same time, employees must be educated in how security enables the organization. A cybersecurity architecture coupled with security standards will allow the organization to have a "blueprint" for where security is now and the target state to be achieved.

Unfortunately, the security system is all too often retro-fitted to the existing technologies and security controls. Price or functionality is also all too frequently the criterion by which a new process is evaluated and the security function overlooked or not considered.

This approach is sub-optimal as it means the principle of security-by-design has not been followed. Retro-fitting often delays delivery of the project or product and creates the perception that security slows down or delays operations.

Security should therefore be part of any procurements or project requirements in the design and development phase. Security should also be integrated into the project management office (PMO) process or during any reviews or approvals. Proper security practices such as integrated security champions will also help build security as a seamless process across the organization. Depending on the organization's business and culture, a decentralized security resource embedded within business units may be appropriate to act as the "voice" of security during day-to-day activities.

Questions the board should ask management:

- Does the organization have a cybersecurity architecture? Is it maintained and up to date?
- Is cybersecurity included in the requirements of any procurement or new project?
- Are the security requirements for a new product understood?
- Are vendors/third parties being asked to comply with security requirements?
- Is there a process in place to validate the effectiveness of the security controls embedded in the product?
- Is security testing embedded in the development process?

PART E

Detecting Cybersecurity Events

17. What processes and tools are in place to alert management when a breach attempt is underway?

One of the most effective ways to enhance a company's cybersecurity posture is to increase its visibility. While operational cybersecurity staff and management are occupied with their day-to-day roles, technology and monitoring can help keep the organization safe. Enhanced visibility of the company's security activities and detection capability leads to shorter response times to prevent or recover from an incident. There are many components to an organization's IT infrastructure; detecting cybersecurity events can be achieved through monitoring of the following:

- endpoints (tablets, phones, laptops, servers)
- IT network
- OT network (if applicable).

Establishing the "normal" level of IT traffic as a benchmark will allow observation and tracking of anomalous activity. Monitoring through a security operations centre (SOC) will enable the company to track internal and external threats through logging of unauthorised access, abnormal traffic or theft of data and unchecked escalation of privileges. This can help mitigate the risk of an insider threat (whether malicious or accidental) and also assist with recognising where an attack may have come from (attribution) to be able to block or prevent further contact from that location.

An SOC should be seen as a force multiplier during the time the baseline (i.e., normality) is being enhanced by machine learning through threat intelligence (i.e., reports from organizations such as FS-ISAC and CCTX) and the tuning of any sensors by the SOC staff itself. SOC allows the organization to detect potential cyber breaches through observing and monitoring for the absence of the normal and the presence of the abnormal. In this way, cyber

breaches can often be prevented. If a cyber breach does occur, enhanced visibility means it can be more readily contained and, because of being able to respond quicker, the length of time the organization is impacted will be reduced.

Questions the board should ask management:

- What kind of monitoring does the organization have in place (SOC, Endpoint, Network etc.)?
- Does the organization use cyber threat intelligence feeds?
- Does the organization have mechanisms in place such as identity and access management to prevent malicious insiders?
- Is there a connection between monitoring and personnel taking action based on intelligence?

PART F

Response and Recovery from a Breach

18. How are management and the board equipped to respond to, and recover from, a cybersecurity breach?

The perception of the probability of a cyber breach happening to the organization has shifted from “*If* this happens to us.” to “*When* this happens to us”. With this in mind, it is imperative for the organization to be as prepared as possible for that eventuality. This preparation should go across the spectrum of people, process, technology and data. In terms of process, the organization should have an incident response plan and playbooks in place. The plan is the “what” and the playbooks are the “how”. The way the plan is implemented will depend on the type of cyber attack (i.e., internal or external, a disruption of operations vs a data compromise).

Incident response roles and responsibilities should be documented and understood, including communication to both internal and external parties. These parties may include the following:

Internal Communication	External Communication
<ul style="list-style-type: none">employees (consider affected and non-affected)executiveboardshareholders	<ul style="list-style-type: none">regulatory bodiesthird parties/vendorscustomers/clientsmedia/news outletssocial medialaw enforcement

With increased mandatory breach notifications because of the introduction of regulations such as PIPEDA in Canada and GDPR in Europe, mandatory disclosure of privacy violations may be triggered by the occurrence of a cyber incident.

Things the board should consider before a cyber breach occurs:

- Has management devised a meaningful cyber incident response plan and playbooks?
 - This should be refreshed annually.
 - This should be cross-functional across multiple business units; a cyber breach typically involves IT, cybersecurity, HR, legal and communications.
- Has the IR capability, including the plan and playbooks, been tested through breach simulations and/or table-top exercises?
 - The board can be involved in this as spectators or as participants as the incident escalates.
 - The most objective and effective way to do this is through third-party facilitation. As the organization matures, third parties such as law enforcement or vendors can be involved.
- Does management conduct backups on a regular basis (critical applications at a minimum)? This will enable an easier and quicker restoration, if required.
- Discuss the strategy around when the payment of extortion may be a viable option during a cyber incident or a ransomware attack.

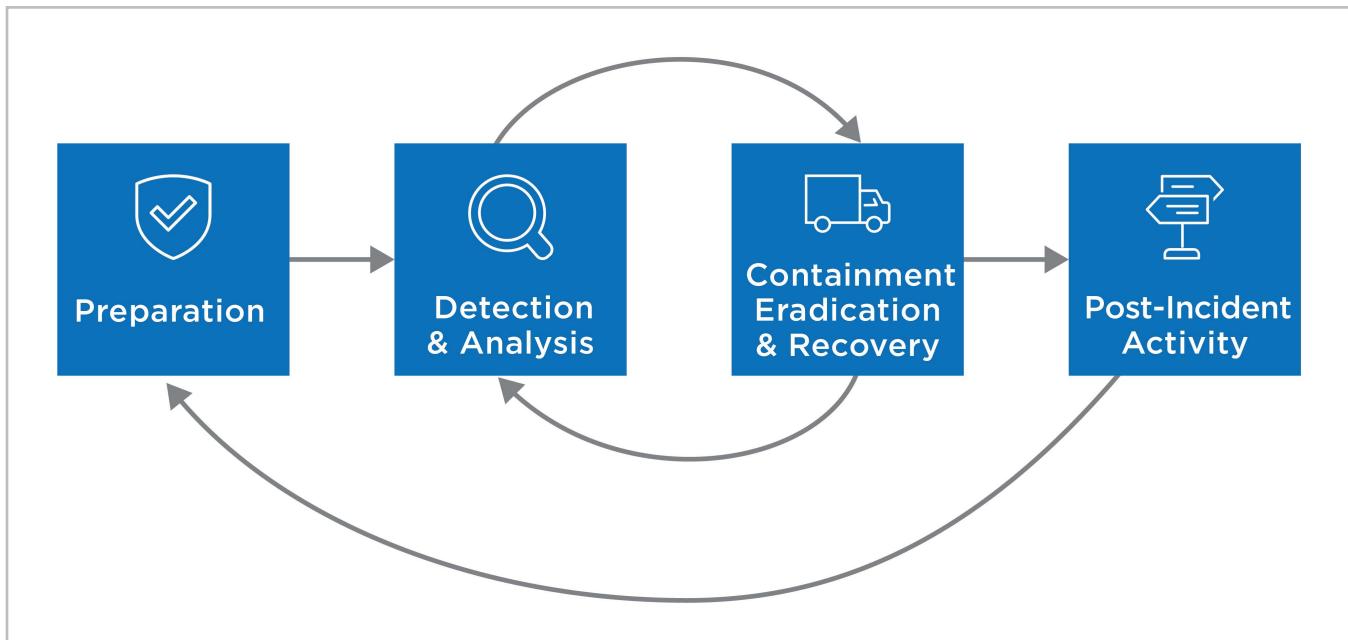
Things the board should consider during a cyber breach:

- A well-prepared and rehearsed team will consult with or inform the board of anything significant such as media statements, regulator notifications or any brand or reputational damage. The plan should be enacted and followed. This will be challenging to do as the organization will be completely engaged in resolving the incident; the incident management team will be focusing on getting the organization back to an acceptable level of operations and in investigating and fixing the incident. The plan should have thresholds for severity and therefore priority, which define which groups of business units should be engaged and at which point. It should also provide guidance as to when the board should be informed. Typically, this will occur if brand or reputation may be impacted, if there have been any regulatory violations or significant financial impact. The board should enquire whether management has these escalation processes in place.

Things the board should consider after a cyber breach:

- Verify that management has conducted root-cause analysis as to why the breach happened.
 - Be sure any remediation steps have been taken such as enhancement of controls, deprovisioning of accounts, training etc.

- Check to see that management has put in place a short-, medium- and long-term strategy to minimise the possibility of this happening again?
- Bring the lessons of the breach back into the preparation phase. Below is the SANS Incident Response Process, which shows the steps management should take before, during and after a cyber breach.

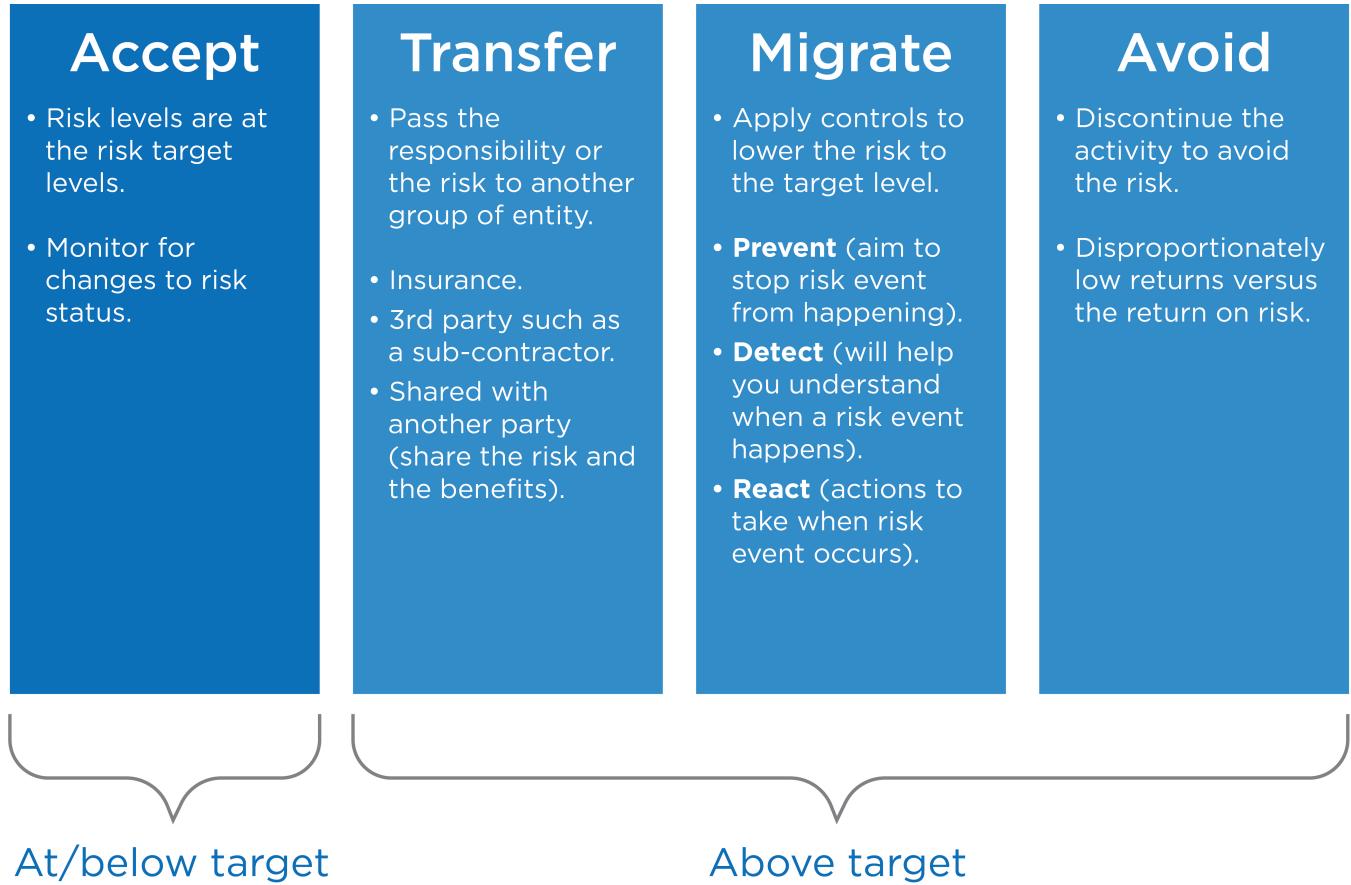


19. What is management's cyber insurance strategy?

Cyber insurance is an emerging offering with growing demand. It offers new opportunities but may also dangerously expose the organization if not understood or managed properly.

Cyber insurance will not reduce the likelihood of a cyber breach happening or help an organization detect or prevent a cyber event or incident. It will, however, allow the organization to transfer some risk to its insurance provider. Cyber insurance gives the organization a control that could reduce the financial impact and/or allow a quicker recovery to an acceptable level of operations.

Below are the four ways in which risk can be managed, and where cyber insurance can act as a risk transference option.



Because little Canadian actuarial data on cyber attacks is publicly available, premiums can be challenging to estimate accurately. Additional information is necessary to build in protective exclusions. Providers may carry out their own assessment or use an objective third party to assess a company's cyber risk maturity and controls. This assessment will enable the organization to become aware of its potential vulnerabilities then take action to improve security and thus reduce the premium.

With gaps between available cyber insurance and general insurance, an option to bridge the gap in coverage is a captive insurer. Captive insurance strategies afford companies more control, may reduce the cost of insurance, create tax benefits and improve cash flow.

Questions the board should ask management:

- Has the organization conducted a thorough risk assessment and considered cyber insurance?
- What are the limits of the cyber insurance available, and how can management determine whether these limits provide sufficient coverage?
- Has management compared the cyber insurance program to the organization's fundamental risk profile?
- Is the organization in compliance with the insurance policy?
- Can the premium be lowered by improving security controls?
- At what stage in a cyber breach is the insurance provider contacted?
- There are clauses and terms within any cyber insurance policy that must be followed to maintain coverage. Failure to follow them can invalidate the policy or leave the organization exposed. Understand what management needs to do and what the exposure is.

PART G

Reporting

20. How does management assess and report on its cybersecurity program to the board?

No topic will be more debated than what, how and when cybersecurity information should be presented by management to the board. This is because no single metric will provide the board with the information it requires to understand how cyber risks are being addressed.

A concept gaining popularity is **HIFO** reporting:

- **Hindsight,**
- **Insight,**
- **Foresight,**
- **Oversight.**

What information is being provided to show what has already happened (hindsight), what will be happening (foresight), how the cybersecurity program is being managed (oversight) and what information is really important for the directors (insight)?

Directors also need to insist that management provide reports that are:

- **Clear:** free from the cybersecurity jargon
- **Concise:** use graphics instead of text, along with other techniques to make reports shorter, easier to read and comprehend
- **Memorable:** make the information easy to recall and use in conversations with stakeholders.

Industry-specific information must be the basis for reporting. While there may be some common elements, cybersecurity needs are different between the banking and mining industries, between the public and private sectors and certainly between for-profit and not-for-profit enterprises. The scope and depth of information at risk will be markedly different.

Hindsight

A variety of key performance indicators (KPIs) can be used to gain hindsight. That said, make sure the KPIs used are relevant to what board members really need to understand. Some management teams highlight the number of attacks that were blocked. This number can run from the tens or hundreds into the thousands. What is much more important, however, is to understand when the attack was detected and if any information was compromised during the attack.

Foresight

Foresight gives directors a sense the enterprise is anticipating who wants to compromise its data, what methods they may be using, and what protections have been put in place to help reduce the likelihood they will be successful. Companies can now purchase information from outside parties on “intelligence” or forward-looking data and on the methods used by those looking to compromise digital assets. Management should also report on the third parties with whom it is collaborating to gain information on the nature of attacks taking place in its industry. Working together with competitors is often necessary for the industry to strengthen its resilience.

Oversight

Governance elements are typically presented in the oversight section. These include how the cybersecurity program is structured and whether a qualified, accountable member of management is in place with appropriate succession planning, and whether the cybersecurity program is fully funded and operational and focused on those projects necessary to reduce future risks.

Insight

Finally, insight is what is gained by combining all the previous elements to show directors that management is acting on historical, future and operational information to reduce the impacts of an increasingly likely attack on an enterprise’s digital assets. In the near term, metrics will need to be provided to the board that speak to the enterprise’s ability to detect anomalous situations and how management is executing the appropriate response to those situations.

ILLUSTRATIVE MANAGEMENT REPORT

NIST Cybersecurity Framework (CSF) Function	2017 Highlight	2016*	2017	2018 Goal
Identity Develop the organizational understand to manage cybersecurity risk to systems, assets, data, and capabilities	<ul style="list-style-type: none"> ↗ Policies, standards and governance processes are well-defined ↗ Risk management activities are continuously prioritizing areas of investment to meet existing and evolving threats 	3.4	3.6	
Protect Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services	<ul style="list-style-type: none"> ↗ Strong fundamentals (eg. Anti-virus, patching) and layers of defense to protect against current threats such as Ransomware and stop low-effort attacker → Recurring low risk Access Control deficiencies due to timely attestation and deprovisioning processes 	3.4	3.5	
Detect	<ul style="list-style-type: none"> ↗ Event monitoring and operations capability are being modernized 			

Because directors often have hundreds of pages of material to read, they should insist that management do the hard work of condensing the material to suit the directors as a distinct audience. Repackaging management reports that are meaningful for running the enterprise is usually not appropriate for those who have to govern. The frequency of the reporting is also something directors should schedule. Today reporting is typically monthly to a sub-committee of the board, with quarterly in-person reporting to that same sub-committee and an annual presentation to the full board. As mentioned previously, this schedule of reporting will depend on the industry (e.g., more frequently with predominantly digital businesses) and the cybersecurity performance of the enterprise. For example, an entity that has suffered through a significant incident may choose to report performance to the board more frequently in response to that incident.



CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

277 WELLINGTON STREET WEST
TORONTO, ON CANADA M5V 3H2
T. 416 977.3222 F. 416 977.8585
WWW.CPACANADA.CA

ISBN-13: 978-1-5254-0350-7

