

Cybersecurity Best Practices Guide

For IIROC Dealer Members

Table of Contents

Executive Summary	3
Purpose and Applicability	4
Audience	6
1 Background.....	7
1.1 Defining Cybersecurity	7
1.2 Threat Landscape	9
2 Introduction	11
2.1 Purpose and Applicability.....	11
2.2 Document Overview.....	11
2.2.1 Relationship to Other Security Control Publications	11
2.2.2 Management, Operational, and Technical Controls	12
3 Best Practices.....	12
3.1 Governance and Risk Management	12
3.1.1 Governance Framework	12
3.1.2 Board and Senior Management Involvement	14
3.2 Best Practice Recommendations: Small- to Mid-Sized Dealer Members	16
3.3 Personnel Screening and the Insider Threat	17
3.4 Physical and Environmental Security	19
3.5 Cybersecurity Awareness and Training	20
3.6 Assessing Threats and Vulnerabilities	22
3.7 Network Security.....	23
3.7.1 Wireless Network Security.....	25
3.7.2 Remote Access.....	26
3.8 Information System Protection.....	28
3.8.1 Bring Your Own Device	29
3.8.2 Backup and Recovery	30
3.9 User Account Management and Access Control.....	31
3.10 Asset Management	32
3.11 Incident Response	33
3.12 Information Sharing and Breach Reporting	36
3.12.1 Privacy Breach Notification	36
3.12.2 Information Sharing	36
3.13 Cyber Insurance.....	38
3.14 Vendor Risk Management.....	40
3.14.1 Cloud Computing.....	42
3.15 Cyber Policy.....	43
Appendix A – Cybersecurity Incident Checklist.....	44
Appendix B – Sample Vendor Assessment	46
Appendix C – Glossary	50
Appendix D - References.....	52

Executive Summary

In recognition of the importance of proactive management of cyber risk to ensure the stability of IIROC-regulated firms, the integrity of Canadian capital markets, and the protection of investor interests, this document sets forth a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help IIROC Dealer Members manage cybersecurity risks.

The voluntary guidance provided herein offers Dealer Members the ability to customize and quantify adjustments to their cybersecurity programs using cost-effective security controls and risk management techniques. For smaller Dealer Members, this can help in understanding how to provide basic security for computer systems and networks.¹ For larger Dealer Members, this provides a cost-effective approach to securing computer systems based on business needs, without placing additional regulatory requirements on business.

Key points in this report include:

- A sound governance framework with strong leadership is essential to effective enterprise-wide cybersecurity. Board-level and senior management-level engagement is critical to the success of firms' cybersecurity programs, along with a clear chain of accountability.
- A well-trained staff can serve as the first line of defense against cyber attacks. Effective training helps to reduce the likelihood of a successful attack by providing well-intentioned staff with the knowledge to avoid becoming inadvertent attack vectors (for example, by unintentionally downloading malware).
- The level of sophistication of technical controls employed by an individual firm is highly contingent on that firm's individual situation. While a smaller firm may not be positioned to implement the included controls in their entirety, these strategies can serve a critical benchmarking function to support an understanding of vulnerabilities relative to industry standards.
- IIROC Dealer Members typically use third-party vendors for services, which requires vendor access to sensitive firm or client information, or access to firm systems. At the same time, the number of security incidents at companies attributed to partners and vendors has risen consistently, year on year. Firms should manage cybersecurity risk exposures that arise from these relationships by exercising strong due diligence and developing clear performance and verification policies.

This Cybersecurity Best Practices Guide describes common practices and suggestions which may not be relevant or appropriate in every case. It is not intended as a minimum or maximum standard of what constitutes appropriate cybersecurity practices for IIROC Dealer Members. Effective management of cyber risk involves a contextual analysis in the circumstances of each

¹ The customers, employees, and current and/or potential partners of Dealer Members have an expectation that their sensitive information will be respected and given adequate and appropriate protection. Moreover, Dealer Members have certain legal obligations to safeguard personal information.

Dealer Member.

The document is not intended to create new legal or regulatory obligations or modify existing ones, including existing IIROC requirements. The information in this guide is provided for general information purposes only and is not guaranteed to be accurate or complete, nor does it constitute legal or other professional advice. Dealer Members seeking further guidance should consult a cybersecurity professional for specific advice about their cybersecurity program.

Purpose and Applicability

The purpose of this publication is to provide an understanding of the specific, standards-based security controls that make up a best practice cybersecurity program.

Implementation of controls is expected to vary between Dealer Members subject to different threats, different vulnerabilities, and different risk tolerances. Investment industry members can determine activities that are important to critical service delivery, and can prioritize investments to maximize the impact of each dollar spent.

Specific objectives that follow from this publication are:

- Establishing and maintaining a robust and properly implemented cybersecurity awareness program, and ensuring that end-users are aware of the importance of protecting sensitive information and the risks of mishandling information;²
- Facilitating a consistent and comparable approach for selecting and specifying security controls for Dealer Member computer systems.¹
- Providing a catalogue of security controls to meet current information protection needs and the demands of future protection needs based on changing threats, requirements,³ and technologies; and,
- Creating a foundation for the development of internal assessment methods and procedures for determining security control effectiveness.

This best practices framework is intended to function as a living document, and will continue to be updated and improved as industry provides feedback on implementation. Lessons learned from early distribution of this framework to Dealer Members will be integrated into future versions. This will ensure that the document continues to meet the needs of Dealer Members in an environment of dynamic threats and innovative solutions.

² Cybersecurity awareness is a critical component of a comprehensive cybersecurity program. This will be discussed more extensively in subsequent sections, but fundamentally, cybersecurity awareness requires policies and training to enforce awareness (e.g. clean desk policy to avoid breaches through facility support staff such as janitors or security guards, mandatory annual training for all employees, etc.)

³ Some of these information protection categories (e.g. exposure or loss of significant client information) have special, more restrictive regulatory requirements for information security protection. Failure to properly protect this information can result in significant fines and penalties from regulatory agencies in the United States and Canada.

Audience

This guide is applicable to IIROC Dealer Members of all sizes and budgets, but specifically targeted at small and mid-sized firms.

The structure of the publication facilitates communication of cybersecurity activities and outcomes across a Dealer Member enterprise – from the implementation/operations level to the executive level. The document is intended to serve a diverse audience, including senior level management, auditors, end-users, information security professionals, information technology management, and field personnel.

Staff who may benefit from a review of the security controls in this document include:

- Individuals that have access to systems, including **end users**.
- Individuals with **information system, security, and/or risk management and oversight responsibilities** (e.g., chief information officers, senior information security officers, information system managers, information security managers);
- Individuals with **information system development responsibilities** (e.g., program managers, system designers and developers, information security engineers, systems integrators);
- Individuals with **information security implementation and operational responsibilities** (e.g., mission/business owners, information system owners, common control providers, information owners/stewards, system administrators, information system security officers); and
- Individuals with **information security assessment and monitoring responsibilities** (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts, information system owners).

1 Background


1.1 Defining Cybersecurity

There is a wide range of currently accepted cybersecurity definitions:

The **Committee on National Security Systems (CNSS-4009)** defines cybersecurity as the ability to protect or defend an enterprise's use of cyberspace from an attack, conducted via cyberspace, for the purpose of: disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or, destroying the integrity of the data or stealing controlled information.

The **National Institute of Standards and Technology** defines cybersecurity as "the process of protecting information by preventing, detecting, and responding to attacks." Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers.

The **International Organization for Standardization** defines cybersecurity or cyberspace security as the preservation of confidentiality, integrity and availability of information in the Cyberspace. In turn, "the Cyberspace" is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."



At its core, cybersecurity seeks to protect your enterprise from those who wish to do harm to your business, steal your information or your money, or use your systems to target peers in the market.

Cybersecurity is not hard, it is merely complex. The Australian Signals Directorate (ASD) has articulated a set of the top 35 strategies required to protect computer networks.ⁱⁱ Of these, the ASD stresses that implementing just the Top 4 cybersecurity strategies will mitigate at least 85 percent of targeted cyber intrusions. Those top four controls are:

1. Application whitelisting – permitting only those applications that have been approved to do so to operate on networks.
2. Applications Security Patching – enforcing effective practices to deploy new security patches in a timely fashion.
3. Operating System Security Patching – same practice as above, but for the operating system.
4. Limiting Administrative Privileges – allowing only trusted personnel to configure, manage, and monitor computer systems.

The challenge is to accomplish these and other related tasks in a complete and comprehensive manner while facilitating the essential operating functions of a successful business.

This document aids in that effort by providing a readable guide for security professionals, business executives, and employees of IIROC Dealer Members to understand the cybersecurity threat to their businesses, and to develop an effective program to guard against cyber-threats.

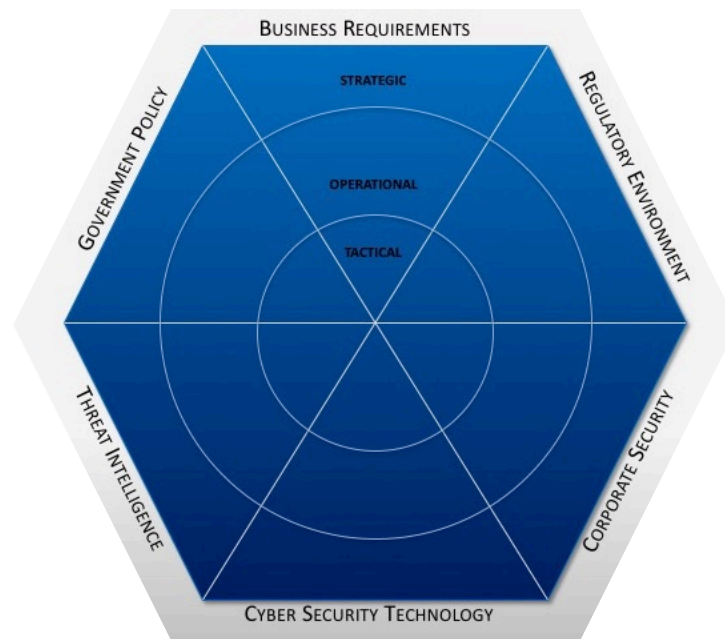


Figure 1 - Cybersecurity Conceptual Framework

Cybersecurity is not only an IT problem, it is an enterprise-wide problem that requires an interdisciplinary approach, and a comprehensive governance commitment to ensure that all aspects of the business are aligned to support effective cybersecurity practices.

Figure 1 provides a conceptual framework upon which to understand all aspects of cybersecurity, including discussions, solutions, and services.

- The industry is guided by both *Government Policies* that shape cyber-defences, and the *Regulatory Environment* that sets standards for conduct.
- *Business Requirements* drive the specific cybersecurity elements that are necessary to achieve business objectives.
- *Threat Intelligence* gleaned from newspapers, governments, industry partners, security vendors, internal efforts, or a combination of all these sources, establishes the landscape that security measures must be ready to respond to, both today and in the future.
- *Corporate Security* activities related to cybersecurity, physical security, and personnel security, collectively provide the integrated elements of an effective protective solution.
- Finally, *Cybersecurity Technology* underpins but does not drive an effective cybersecurity policy. Too often, technology is viewed as the solution rather than merely a component of a broader strategy.

A comprehensive approach that integrates these six elements into an adaptive cybersecurity strategy will frame top priorities and focus actions to mitigate cyber risks to assets, systems, and information.



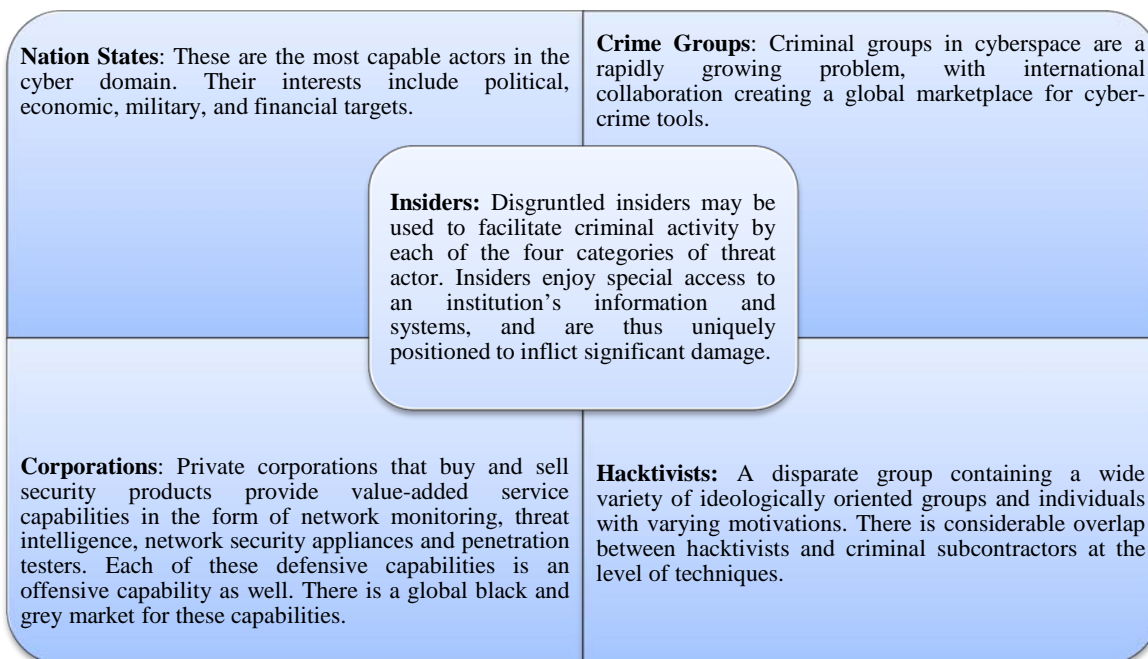
The objective of this publication is to provide IIROC members with the tools needed to design and implement effective cybersecurity programs.

1.2 Threat Landscape

The investment industry faces a variety of rapidly evolving cybersecurity threats, including hackers penetrating systems, insiders compromising firm or client data for commercial gain, nation states that may acquire information to advance national objectives, and hacktivists whose objectives may be to disrupt and embarrass an organization.

Depending on the environment in which an information system or network is located, and the type of information it is designed to support, different classes of threats will have an interest in attempting to gain different types of information or access.

Among the most significant and challenging threats are the sophisticated attacks perpetrated by Advanced Persistent Threats (APTs). APTs involve activity largely supported, directly or indirectly, by a nation-state. APTs target carefully selected, high-value data in every industry, from aerospace to wholesalers, education to finance.





The FINRA cybersecurity surveys of 2011 and 2014 identified the **top three threats to the securities industry** as:

- Hackers penetrating firm systems
- Insiders compromising firm or client data, and
- Operational risks

Firms need to understand which threats are both most likely and most dangerous to their unique situation to effectively develop and implement their cybersecurity strategy.

Business Email Compromise^{xxxii}

One type of wire fraud currently targeting businesses is the Business Executive Scam (BES), which is a type of phishing. The potential victim receives an email that appears to come from their employer's human resources or technical support department. Fraudsters create email addresses that mimic that of the real departments. An email message will be sent to the accounting department advising that the "executive" is working off-site and has identified an outstanding payment that needs to be made as soon as possible. The "executive" instructs the payment to be made and provides a name and a bank account where the funds, generally a large dollar amount, are to be sent. Losses are typically in excess of \$100,000.

Case Study - Business Email Compromise - February 2015

The chief financial officer for Infront Consulting Group Inc., based in Toronto and Las Vegas, received an email that appeared to come from the company's chief executive, instructing her to "process a payment of \$169,705.00 USD." Attached wire transfer instructions directed that payment be made to an investment brokerage in Naples, Florida.

The scheme failed only because the Infront CEO, by coincidence, called the CFO as she was reviewing the request. When she asked what the money was for, the CEO said he knew nothing about it. Further scrutiny revealed that the email was sent from an address similar to the company's, but that lacked the letter "i" in "consulting."

2 Introduction

2.1 Purpose and Applicability

A cybersecurity framework is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. These frameworks can present industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the Dealer Member – from the executive level to the implementation/operations level.

The NIST Cybersecurity Framework consists of five concurrent and continuous Functions: Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The NIST Framework then identifies underlying key Categories and Subcategories for each Function. It further indexes each Subcategory with example Informative References, such as: existing standards, guidelines, and practices.

2.2 Document Overview

2.2.1 Relationship to Other Security Control Publications

This document draws on a variety of sources, including security controls from the defense, audit, financial, industrial/process control, and intelligence communities, as well as controls defined by national and international standards organizations. The guidelines have been developed from a technical perspective to create a sound and broadly applicable set of security controls for computer systems and Dealer Members.

The following documents, principles, and best practices constitute foundational references:

1. SANS Top 20 Critical Security Controls
 - A recommended set of actions for cyber defense that provide specific and actionable ways to thwart the most pervasive attacks.
2. Small Business Information Security: The Fundamentals (NISTIR 7621)
 - Outlines the actions that are *absolutely necessary* for a small business to take to protect its information, systems, and networks.
3. NIST Cybersecurity Fundamentals For Small Business Owners
 - Best practices recommended by the National Institute of Standards and Technology to help small businesses protect the safety and security of information of their customers and their employees.
4. Security and Privacy Controls for Federal Information Systems and Organizations (NIST 800-53r4)
 - The international standard for security controls covering 17 areas, including: access control, incident response, business continuity, and disaster recoverability.
5. Government of Canada's Information Technology Incident Management Plan
 - Addresses cyber-related threats, vulnerabilities, and incidents that affect service to Canadians, government operations, security or privacy of information, or confidence in government.

2.2.2 Management, Operational, and Technical Controls

The catalogue of security controls in this publication can be effectively used to manage information security risk at three distinct tiers – the organization level, the mission/business process level, and the information system level.

Organizations have the responsibility to select the appropriate security controls, to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying established security requirements. This publication is intended to complement, and does not replace, an organization's cybersecurity risk management processes. Users with existing cybersecurity programs can leverage the document to identify opportunities to align with industry best practices, while Dealer Members without an existing cybersecurity program can use the document as a reference to establish one.

3 Best Practices

3.1 Governance and Risk Management

Cybersecurity is not solely an IT issue. It is a multifaceted challenge that requires an enterprise-wide approach to its management. Total protection from cyber threats is unattainable. Rather, a best practice is a risk-based approach that implements a comprehensive strategy to deliberately avoid, mitigate, accept, or transfer risks posed by cyber threats. Companies need to establish and maintain an appropriate governance and risk management framework to identify and address risks for communications networks and services.

3.1.1 Governance Framework

The first step a board or executive team should take is to determine who within the company should be involved in the development of a cybersecurity program. Key initial steps include identifying known risks and established controls. A best practice is to establish a cross-organizational committee of senior executives that brings together the full range of enterprise knowledge and capabilities. This should include IT and corporate security, as well as business owners.

Leadership is key. Selecting an executive with broad cross-functional responsibilities such as the Chief Financial Officer or Chief Operating Officer to lead this committee can help ensure that the effort remains focused upon enterprise-wide concerns, rather than siloed within one reporting chain without the benefit of broader corporate adoption. This effort should report to a specialized committee, such as the Audit or the Risk Committees, or in some cases, to the board itself.

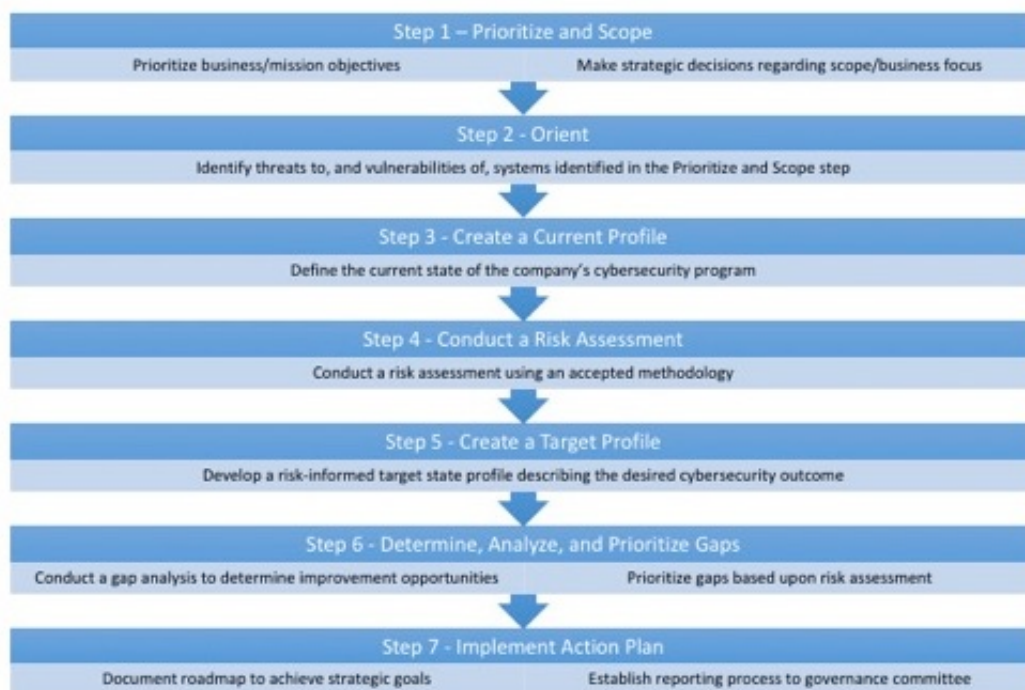


Figure 2 - Cybersecurity Framework Implementation Steps

The NIST Cybersecurity Framework provides a proven process upon which to establish and manage cybersecurity program development. Figure 2 above outlines the steps that boards should direct senior management to implement and report progress upon.

A best practice is to consider appointing a Chief Information Security Officer (CISO) with responsibilities for information security to oversee the cybersecurity efforts within a company. Regardless of who is appointed to oversee cybersecurity efforts, cybersecurity is a shared responsibility across the entire enterprise, including senior management, staff, consultants, partners, and clients. Cybersecurity awareness needs to reach all those constituencies.

The program should begin with the identification of what types of information the company has and where it is located. Information is often duplicated across multiple locations with different controls in place to protect it. A risk-based approach emphasizing critical and mission critical systems as focal points will concentrate efforts on the highest impact areas first. Companies should create an accurate inventory of:

- Physical devices and systems
- Software platforms and applications
- Maps of network resources, connections, and data flows
- Connections to the company's networks
- Prioritized list of resources, based on sensitivity and business value
- Logging capabilities and practices, assessed for adequacy, appropriate retention, and secure maintenance

The focus of the effort should be to identify the company's "crown jewels" and to prioritize remaining data and systems. Once this is completed, the company can move forward with a risk-based cybersecurity program that allocates the highest level of protection to the most valuable data. The company should create a current profile of its cybersecurity protections.

Cybersecurity efforts should be oriented towards threats specific to the industry and similarly situated companies. Companies should conduct threat risk assessments specific to the prioritized systems, with the intention of creating a risk-based understanding of priorities. The operational environment needs to be constantly reviewed to determine the likelihood of a cybersecurity event and the impact that the event could have. This is a continual and iterative process shaped by changes to the company's IT environment, as well as evolutions in its business model.

Based upon knowledge gleaned from the risk assessment, companies should identify the target profile that addresses the company's desired cybersecurity outcomes. This should extend beyond the company's own systems to consider those of external stakeholders upon which they rely, to include sector entities, customers, and business partners.

Upon completion of the target profile, companies need to compare that target profile with the current profile and determine gaps. Those gaps should be prioritized into a roadmap plan that addresses the gaps based upon factors unique to the company, specifically the business requirements, system configurations, and resources available to close gaps. Each company is different; thus, developing an achievable plan with adequate resourcing should be the goal.

Implementing the action plan and monitoring the progress needs to become a core business function. Given today's environment, cybersecurity is not a one-time project but rather an ongoing responsibility for senior management and boards – for companies of all sizes. Senior management needs to monitor its implementation plan and report regularly to the board on progress in achieving its target end-state. While the NIST Cybersecurity Framework provides an excellent set of tools to guide the implementation of a cybersecurity program, each company should determine which standards, guidelines, and practices work best for its needs.

3.1.2 Board and Senior Management Involvement

The National Association of Corporate Directors (NACD) cites five cybersecurity principles for boards. The principles state:

Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

- Boards should recognize that cybersecurity extends beyond the company's networks to suppliers, partners, affiliates, and clients.
- There is a need to understand the entire ecosystem and ensure that senior leadership is comprehensive in its security approach.

Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

- High-profile cyber-attacks have spawned a range of lawsuits. Boards should understand the contours of liability, and adequately protect against those threats.

- Directors should ask management to solicit external counsel’s point of view on potential disclosure considerations in the event of a breach, and incorporate that into breach plans.

Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

- Directors should seek regular advice on cybersecurity including “deep dive” briefings from internal sources and external experts, including cybersecurity firms, government agencies, industry associations, and peer institutions.

Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.

- Directors should ensure that cybersecurity is a cross-departmental function led by a senior executive with cross-departmental authority, such as the CFO or COO.
- Directors should expect regular reporting from management with metrics that quantify the business impact of cyber-threat risk management efforts reported.
- Directors should ensure that a specific cybersecurity budget tied to the execution strategy is established, so that the program is not exclusively tied to one department.

Board and management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

- Total cybersecurity is an unrealistic goal; concentration of resources upon the most critical data assets is a best practice.
- Directors should look to ensure that the company adopts a clear strategy with layered approaches that best fits the specific business needs of the company.

Directing the implementation of a comprehensive cybersecurity program as discussed above is incumbent upon all boards – regardless of company size.

Case Study - Ashley Madison - July 2015^{xxxiii}

Canadian company Ashley Madison was targeted by hackers in July 2015. Calling themselves the Impact Team, the hackers took issue with the company’s business model of providing a forum to facilitate marital infidelity. The aim of the hackers was to force the company to cease its operations.

In August 2015, the hackers released some 39 million customer profiles, including user profiles, names, and email addresses. Lawyers representing Canadian victims launched a class-action lawsuit seeking \$760 million in damages. The parent company, Avid Life Media, has indefinitely postponed Ashley Madison’s upcoming initial public offering, where the company had hoped to raise \$200 million.

3.2 Best Practice Recommendations: Small- to Mid-Sized Dealer Members



Cybersecurity is a shared responsibility – people, processes, tools, and technologies work together to protect an organization's assets.

Protecting your organization's assets requires a focus on the following **three fundamental goals**:ⁱⁱⁱ

- **Confidentiality**
Any important information you have that should be kept confidential. This information should only be accessed by people (or systems) that you have given permission to do so.
- **Integrity**
Maintain the integrity of information assets to keep everything complete, intact, and uncorrupted.
- **Availability**
Maintain the availability of systems, services, and information when required by the business or its clients.

Achieving these goals can be accomplished by performing the Cybersecurity Framework functions outlined below:^{iv}

1. Identify which assets need securing, as well as the threats and risks to them.
2. Protect assets with the appropriate safeguards.
3. Detect intrusions, breaches, and unauthorized access.
4. Respond to a potential cybersecurity event.
5. Recover from a cybersecurity event by restoring normal operations and services.

3.3 Personnel Screening and the Insider Threat

Organizations typically focus primarily on external threats. They implement technical solutions, such as installing antivirus programs to protect their computer systems from malicious software, or firewalls to help protect them from Internet-based threats.

A 2012 survey by cybersecurity vendor, Cyber-Ark, found that 71% of 820 IT managers and C-level professionals interviewed considered insider threats to be their priority cybersecurity concern.^v

An insider threat is defined as “a current or former employee, contractor, or other business partner who has or had authorized access to an organization’s network, system, or data, and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the Dealer Member’s information or computer systems.”^{vi}

Some of the risks posed from insider threats in the financial sector are outlined below:^{vii}

- Undesired disclosure of confidential customer and account data – jeopardizing an organization’s most valuable relationships
- Fraud
- Loss of intellectual property
- Disruption to critical infrastructure
- Monetary loss
- Regulatory repercussions
- Destabilization, disruption, and destruction of financial institutions’ cyber assets
- Embarrassment, and public relations/reputational risk issues

According to the Carnegie Mellon’s CERT Insider Threat Center, the employees who pose the greatest insider threat risk are the following:

- Disgruntled employees who feel disrespected and are seeking revenge.
- Profit-seeking employees who might believe that they can make more money by selling stolen intellectual property.
- Employees moving to a competitor or starting a business who, for example, steal customer lists or business plans to give themselves a competitive advantage.
- Employees who believe they own the intellectual property that they help develop. As a result, they take the intellectual property with them when they leave the organization.

The following are recommendations for addressing the insider threat:^{viii}

- **Build a Multidisciplinary Team**
Where feasible, organizations need to have a dedicated team made up of human resources, security, and legal professionals who create policies, drive training, and monitor at-risk employees.
- **Organizational Issues**
Understand if your organization is at greater risk due to inherent organizational factors. Does your company have remote offices, suppliers, or subcontractors where differences in cultures, politics, or language could lead to potential conflicts?
- **Examine Pre-Employment Screening Processes**
The information collected during these processes will help hiring managers make informed decisions and mitigate the risk of hiring a “problem” employee.
- **Develop Policies and Practices**
This is a checklist of specific policy and practice areas that should be covered within an organization’s basic governance structures.
- **Conduct Training and Education**
These are essential to policy effectiveness since policies and practices that are not recognized, understood, and adhered to may be of limited effectiveness.
- **Monitor and respond to suspicious or disruptive behaviour, beginning with the hiring process**
- **Anticipate and manage negative workplace issues**
- **Enforce separation of duties and least privilege**

By recognizing the potential harm posed by current or departing employees, an organization can help to mitigate the damage that may arise from insider threats.

Case Study - Insider Data Leak - January 2014

The personal data of at least 20 million bank and credit card users in South Korea was stolen from three credit card firms by a temporary consultant working with personal credit ratings firm Korean Credit Bureau (KCB).

The stolen data, which was sold to phone marketing companies, included customers' names, social security numbers, phone numbers, credit card numbers and expiration dates.

In the fallout over the theft, dozens of top executives tendered their resignations, regulators launched investigations into security measures at the affected firms, and the companies were held liable for full financial losses if customers fell victim to scams related to the data theft.

3.4 Physical and Environmental Security

The physical security of IT assets is a cybersecurity first line of defense. The effect of a stolen laptop or smartphone can be just as disruptive to an organization as a cyber attack. As a result, cybersecurity safeguards such as passwords and PINS need to be complemented by other security measures, such as locks that keep laptops from being stolen, or the use of an Uninterruptible Power Supply (UPS) to protect an information system during a power outage.

Physical security encompasses defensive mechanisms to the following threats:

Human threats

Intentional or unintentional damage caused by people, for example, an intruder accessing a restricted area or an employee error.

Environmental threats

Damage caused by the weather such as rain, fires, floods, etc.

Supply system threats

Damage caused by an interruption in energy supply that negatively impacts an information system.

The following are recommendations for physical and environmental security:

- Employees should follow the “clean desktop” principle. This principle means that employees should put away sensitive items before leaving their work area. In addition, a clean desk will keep sensitive information out of the hands of personnel who do not have a legitimate reason for accessing this information. Personnel who have no need-to-know include cleaning staff and security guards.
- Only allow employees into your work area if they have a legitimate business requirement.
- Restrict access to your computer’s contents by locking the screen when you are away.
- Safeguard your information system against fluctuations in electricity or electrical power outages and by ensuring that it is plugged into an Uninterruptible Power Supply (UPS).
- Ensure that backups are performed on a regular basis to safeguard your information against a catastrophic event such as a flood or fire.
- Small- and mid-sized organizations need to have a plan in place to address physical security issues. The physical security controls implemented should be commensurate with the level of sensitivity of the information being protected.

3.5 Cybersecurity Awareness and Training

The risk of a cyber attack to financial institutions continues to grow, as our highly connected world creates more opportunities for cyber criminals. Because financial institutions rely on online tools to help them communicate with stakeholders, they remain the constant target of cyber criminals who want to steal their intellectual property and confidential information. Price Waterhouse Coopers' 2015 *Global State of Information Security® Survey* suggests that businesses that have a security awareness program report significantly lower average financial losses from cybersecurity incidents. It also points out that an effective security awareness program requires adequate funding.^{ix}

Many organizations invest heavily in technical controls to protect their computer systems and data. However, most of these technical controls are rendered useless because employees lack cybersecurity awareness training. Employees take risks online and this greatly increases cyber-related risks to their organization. Risky activities by employees include opening suspicious emails and not protecting sensitive information stored on, or transmitted from, their computers. The 2015 *Cyberthreat Defense Report Survey* reports that low security awareness among employees remains the greatest inhibitor to defending against cyberthreats.^x

Participants in the survey were asked to rate issues that inhibit the defense against cyberthreats.

On a scale of 1 – 5 (with 5 being the highest) survey participants were asked to rate how each of the following issues inhibit their organizations from adequately defending themselves against cyberthreats

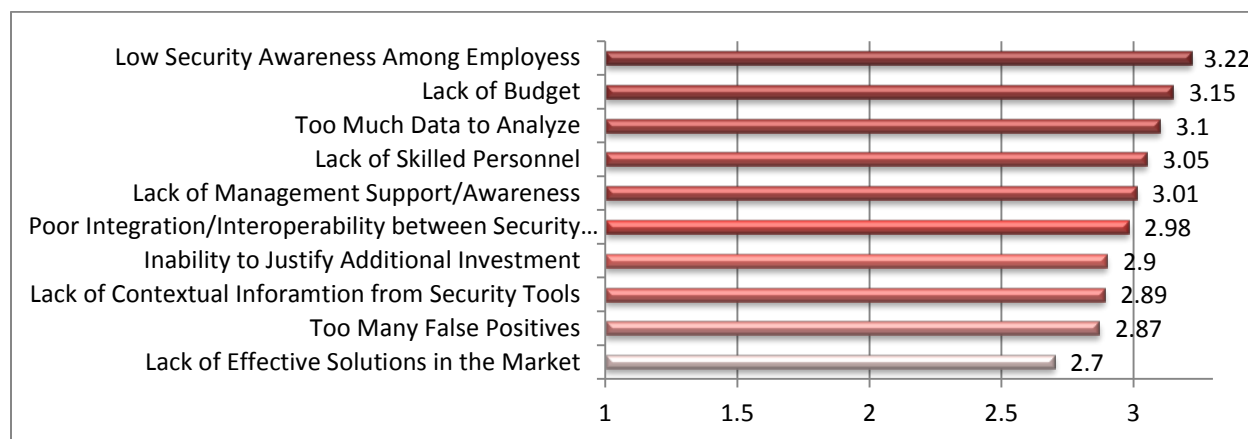


Figure 3 - Inhibitors to Establishing Effective Cyberthreat Defenses (Source: 2015 Cyberthreat Defense Report)

Low security awareness ranked number one. This result highlights the importance of security awareness training as the principal activity that an organization can undertake in order to improve its cyber defenses. Employees should be informed about good cybersecurity practices, and understand that they play a crucial role in safeguarding their organization's information assets. With proper training, employees are the first line of defense against cyber threats.

The following are recommendations for cybersecurity awareness and training:

- Implement policies covering the acceptable use of, as well as the secure use of, computer systems.
- Make cybersecurity training and awareness mandatory for all personnel. Training can take place in a classroom, online, or by video and should be attended on a yearly basis. Hacking attacks (e.g., email phishing) often target executives, so it is important that they attend cybersecurity training as well.
- Ensure that all personnel understand their roles and responsibilities with regard to cybersecurity.
- Users should be instructed not to open suspicious emails or click on suspicious links, regardless of the source.
- Users should be instructed not to connect devices to the network, unless they have a legitimate business reason to do so, or are using pre-approved devices.
- Users should be instructed to follow good password practices.
- Users should understand the dangers and safe use of external media (USB sticks and CDs).
- Users should not download or install unauthorized applications, because they may contain malicious content.
- Users should understand that the appropriate sanctions will be taken against personnel who fail to comply with the cybersecurity awareness principles and security policies.
- Continuing education methods for executive management may include videos or webinars that educate users and share mandated knowledge.

Case Study - Ransomware - June 2015

Mahone Bay and Bridgewater, small towns in Nova Scotia, reported infections in municipal computers that occurred in June 2015. The virus, known as CryptoWall 3.0, attacked non-networked directories either through a spear-phishing email sent to a system user, or perhaps an infected website visited by a town employee. Once the link was clicked, the systems were infected with CryptoWall 3.0 and a second virus called CryptoLocker, meant to encrypt files on the targeted system. Once activated, the viruses delivered an automated message to the user requesting payment of roughly \$900 in return for unlocking the infected files – it is virtually impossible to decrypt the files unless the ransom is paid. The virus is thought to have originated with criminal groups in Russia.

Use of CryptoLocker techniques is widespread. The U.S. Justice Department estimated that CryptoLocker attacks infected more than 234,000 machines – resulting in \$27 million in ransom payments – in just its first two months.

3.6 Assessing Threats and Vulnerabilities

Cyber criminals continue to take advantage of basic security vulnerabilities in computer systems. These include unpatched Windows Operating Systems, weak passwords, and a lack of end-user education. Organizations that do not scan for vulnerabilities and proactively address information system weaknesses face an increased likelihood of having their systems compromised. In order to protect information assets against the growing threat of cyber attacks that target information system vulnerabilities, more organizations have included vulnerability assessments as a component of their cybersecurity programs. Vulnerability assessments are useful for identifying vulnerabilities in computer systems. Assessment results assist the organization in understanding where cyber-related business risks lie.^{xi}

The following are recommendations for assessing threats and vulnerabilities:

- Run an automated vulnerability assessment tool against all systems on the network on a regular basis. Deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator.
- Subscribe to vulnerability intelligence services in order to stay aware of emerging threats and exposures.
- Ensure that the vulnerability scanning tools you use are regularly updated and contain the latest security vulnerabilities information.
- Ensure computer software/applications are updated with security patches regularly.
- Evaluate critical patches in a test environment before pushing them onto production systems.

Unsolicited Computer Repair Services

Generally, this scheme involves individuals calling users and stating, for example, that it is Microsoft calling and that the user's computer is running slow or has viruses. They offer to repair the computer over the Internet, which can involve the installation of software or the user allowing the representatives remote access to their computer.

Recent variations have involved the suspects identifying themselves as the Canadian Cyber Incident Response Centre, and have taken a more aggressive approach. The individuals are stating that the victim's computer is being used by hackers, and that they will be held responsible if they do not allow the suspect to repair their computer.

Allowing a third party to download software or remotely access a computer carries inherent risks. Keyloggers or other malicious software could be installed to capture sensitive data such as online banking user names and passwords, bank account information, identity information, etc.

Case Study - Social Engineering Fraud - April 2015

Mega Metals Inc., a 30-year-old scrap processor, was defrauded in 2015 when the email account used by an Italian-based third party broker was compromised.

Mega Metals had wired \$100,000 to a German vendor to pay for a 40,000-pound container load of titanium shavings. Following the transaction, the vendor complained that it had not received payment. An investigation revealed that malicious software implanted on the third party broker's computer systems allowed criminals to collect passwords that provided access to the broker's email system, and then to falsify wire-transfer instructions for a legitimate purchase.

3.7 Network Security

An organization's constant connectivity to the Internet exposes it to a hostile environment of rapidly evolving threats. In addition, employees can intentionally or unintentionally threaten the network because of their actions.

Network security refers to any activities designed to protect the confidentiality, integrity, and availability of the network, as well as the information assets that rely upon it. In general, network security has three fundamental objectives:^{xii}

- To protect the network itself;
- To reduce the susceptibility of computer systems and applications to threats originating from the network; and,
- To protect data during transmission across the network.

Cyber criminals are continuously searching for weaknesses in an organization's Internet-facing network protection devices (e.g. firewalls). These devices protect an organization from threats that emanate from the Internet. Without a firewall at the network perimeter to protect an organization's network from Internet-based threats, cyber criminals could easily steal intellectual property and sensitive information.

A multi-layered defense comprised of next-generation firewall will substantially reduce the number of successful Internet-based attacks on an organization's internal network.

The following are recommendations for network security:

- Purchase a next-generation firewall. Small businesses can purchase a next-generation firewall for under \$1,000. These firewalls include the following additional security services:
 - Filtering out web sites containing malicious content.
 - Protection from Internet-based viruses and from other malware entering the network.
 - Threat prevention technology that examines network traffic flows to detect and prevent Internet-based vulnerabilities from entering the network.
- Require two-factor authentication for all remote login access such as via a VPN.
- Segment the organization's internal network to limit access by users to only those services that they require for business use.
- Implement a Network Access Control solution to prevent unknown computer systems from communicating with the organization's network.
- Establish a baseline of normal network device behaviour.

3.7.1 Wireless Network Security

While wireless connectivity has the advantage of increased mobility and productivity, it also introduces a number of critical security risks and challenges. In many high profile cases, thefts of intellectual property and sensitive information have been initiated by attackers that gained wireless access to organizations from outside the physical building. Because wireless signals typically broadcast outside a building's physical infrastructure, they bypass traditional wired security perimeter safeguards such as firewalls and Intrusion Protection Systems.

In some cases, cyber criminals have gained unrestricted access to an organization's internal network by installing hidden, unauthorized wireless access points on the network. Disgruntled employees or other personnel with malicious intent, under the guise of cleaning staff or a security guard, are typically responsible for planting these devices. Wireless networks have made it exponentially easier for cyber criminals to penetrate organizations without physically stepping foot inside a building. As a result, it is critical that strong security safeguards be implemented to mitigate these risks.

The following are recommendations for wireless network security:

- Ensure that each wireless device that connects to the network is permitted to do so based on a legitimate business requirement. Organizations should deny access to all other wireless devices, including Bluetooth devices.
- Conduct vulnerability assessment scans of the wireless network. This assessment will help identify vulnerabilities within the wireless network, as well as helping to identify unauthorized devices on the network.
- Deploy a Wireless Intrusion Detection System (WIDS) to identify unauthorized wireless devices, detect attacks, and detect successful compromises. Most major wireless vendors sell all-in-one wireless access, firewall, and WIDS solutions for small businesses for under \$1,000.
- Disable wireless access on computer systems that do not have a legitimate business requirement. To reduce the likelihood that an employee might re-enable wireless access, require a password for anyone attempting to enter the computer's hardware configuration.
- At a minimum, ensure that all traffic that flows across the wireless network is protected by Advanced Encryption Standard (AES) encryption and Wi-Fi Protected Access 2 (WPA2) protection.
- At a minimum, ensure that wireless networks use secure authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS).
- Disable peer-to-peer wireless network capabilities on wireless clients.
-

Case Study - Compromised Wireless Local Area Network - May 2007

Hackers who stole 45 million customer records – including millions of credit card numbers – from The TJX Companies Inc. did so by breaking into the retail company's wireless LAN.

TJX had secured its wireless network using Wired Equivalent Privacy (WEP) – one of the weakest forms of security for wireless LANs. According to The Wall Street Journal, hackers cracked the WEP encryption protocol used to transmit data between price-checking devices, cash registers, and computers at a store in Minnesota. The intruders then collected information submitted by employees logging on to the company's central database in Massachusetts, stealing usernames and passwords. With that information, the hackers set up their own accounts on TJX's system. Over an 18-month period, their software collected transaction data, including credit-card numbers, into approximately 100 large files.

Analysts estimated that the breach would cost the company approximately \$1 billion, excluding any litigation costs.

3.7.2 Remote Access

A variety of technologies are available today that provide secure remote access to an organization's computer systems. Much like wireless technologies, it is critical that remote access be continuously managed and maintained in order to keep unauthorized users from accessing your organization's network.

The following are recommendations for secure remote access:^{xiii}

- Implement a remote access policy and train staff to adhere to it.
- Remote access should only be provided using secure VPN technologies.
- Configure the secure VPN so that split tunnelling is not permitted.
- Monitor and log all remote access sessions.
- Require two-factor authentication for all remote access sessions.

3.7.2.1 Remote Access Endpoint Security

Employees accessing organization resources using a secure VPN should do so using company-owned equipment. In addition to the guidance outlined in the upcoming Information System Protection section, remote access users should follow the advice outlined below.^{xiv}

- Ensure that the anti-malware solution is up to date so that it continuously monitors for malicious activity.
- Do not transfer information to unauthorized destinations (e.g., unauthorized storage devices, Hotmail, Gmail, DropBox)
- Do not plug unauthorized devices into company computers (e.g., smartphones, personal memory sticks and hard drives).
- Do not plug company-owned USB keys into unapproved devices (e.g., Laptops, Computers, Smart TV's, etc.).
- Be suspicious of any phone calls, visits, or email messages from individuals asking about employees, their families, and sensitive business matters.
- Do not answer suspicious emails or click on any links in suspicious emails.
- Do not leave your laptop or related materials unattended in a public workspace, even for a moment.
- Make sure that you guard confidential information on your screen from curious onlookers.
- Avoid unknown, unfamiliar, and free Wi-Fi connections unless they are secured with a password and encryption

Case Study - Remote Access Hacks - June 2014

Attacks involving remote access tools have gained attention since the massive 2013 data breach at Target, in which attackers broke into Target's point of sale (PoS) systems via a remote access account belonging to a Heating, Ventilation and Air Conditioning (HVAC) company.

More recently, hackers broke into payment systems at several northwestern U.S. restaurant and food service companies via a remote access account belonging to a provider of PoS systems. In that incident, a LogMeIn account used by the vendor to remotely support and manage customer networks was breached and then used to plant data-stealing software on PoS systems belonging to the vendor's customers.

3.8 Information System Protection

While it is critical to secure the perimeter of an organization's network from threats that stem from the Internet, it is equally important that the computer systems themselves be protected from attempts to hack them. Similarly, company computers that are used to access company resources remotely should have the same security controls as those that are used onsite.

The following are recommendations for information system protection from cyber threats such as ransomware and viruses:

- Implement secure backup and recovery processes and backup your systems regularly
- Deploy an anti-malware solution that continuously monitors workstations, servers, and mobile devices with anti-virus, anti-spyware, and personal firewalls.
- Deploy an anti-malware solution that includes host-based IPS functionality.
- Implement a policy to control all access to removable media.
- Limit the use of external devices e.g. USB devices, to those that have a legitimate business requirement.
- Utilize the personal firewalls built into Windows- and UNIX-based systems
- Scan all media for malware before importing on to corporate system.
- Install all Application and Operating System security updates such as those available via the built-in Windows Update feature.
- Monitor for the use and attempted use of external devices.
- Remote users should access company resources using a secure VPN and should be authenticated using two-factor authentication.

Vendors such as Norton and McAfee sell all-in-one endpoint security solutions for personal, small business, and enterprise computer systems at a very reasonable price.

3.8.1 Bring Your Own Device

The *Bring Your Own Device* (BYOD) concept has been a growing trend in business. It refers to the policy that allows employees to bring personally-owned devices – including laptops, smart phones and tablets – to their workplace and to use those devices to access the company’s applications and data. While real business benefits can be derived from BYOD in the workplace, it does carry significant risks. For example:

- The employee may lose a personal device that contains business information.
- The employee may unintentionally install applications that are malicious in nature.
- The employee may unintentionally disclose business information, for example, by allowing family members or friends to use a laptop containing sensitive business information.
- The BYOD implementation, itself, may be in breach of applicable laws and regulations wherein an improper BYOD implementation may be in violation of data privacy laws and regulations.

A firm should conduct a risk assessment and seek legal advice before deciding whether or not they should allow BYOD and if they can manage the associated risks. If deciding to move forward with BYOD, a firm should implement a series of mitigating actions and controls. Given that BYOD in the workplace has resulted in significant data breaches,^{xv} it is important that firms consider instituting a comprehensive BYOD policy. At a minimum, the BYOD policy should cover the following:^{xvi}

- Who the policy applies to (e.g., staff, contractors)
- Which devices can be used (e.g., laptops, tablets)
- What services or information can be accessed (e.g., email, calendars, contacts)
- The responsibilities of the employer and staff members (including for security measures that need to be adopted)
- Which applications (apps) can and cannot be installed (e.g., for social media browsing, sharing, or opening files, etc.)
- How business applications and data are accessed
 - Ideally, untrusted devices should access business applications and information via a virtual desktop. Citrix and VMware are examples of companies with virtual desktop products that are well suited for secure BYOD implementations.
- What help and support is available from IT staff; and,
- The penalties for non-compliance (e.g., loss of BYOD privileges and other disciplinary procedures).

3.8.2 Backup and Recovery

A backup plan is essential for any organization in order to prepare for a disaster. It is at risk of losing intellectual property and sensitive information without one. Backups ensure that an organization can recover quickly by restoring lost or damaged files.

For small- and mid-sized business, the following backup options are available:

- Portable or desktop USB hard drive
 - An automated process can backup each information system on a regular basis.
- Server
 - Important user data can be backed up on a server that is connected to the network. An automated process on the server then backs up the user data on a regular basis.

The following are recommendations for backup and recovery.

- Implement a plan and begin backing up data on a regular basis.
- To mitigate the risk of theft/disaster, keep copies of backups in a secure location offsite.
- Include system and software settings as part of your backups.
- Test your backups on a regular basis by restoring files to a test computer, in order to ensure that the backup process is working properly.

Case Study - Backup and Recovery - April 2007

U.S. accounting firm A Desaur & Co. was using a tape-based recovery solution when a server failure occurred in April 2007. The tape restore failed entirely because its IT support company had not carried out trial data restores, which would have revealed that the backups were not working.

After an expensive and time-costly hard disk data restore, only 80% of the data was able to be restored, causing the company to permanently lose valuable historical data (accounts preparation) and work in progress (book keeping).

3.9 User Account Management and Access Control

Access controls determine how employees read their email, access their documents, and connect to other network-based resources. Properly implemented access controls help ensure intellectual property and sensitive data are protected from unauthorized use, disclosure, or modification.

The following are recommendations for user account management and access control:

- Implement an account management process.
- Centrally manage all accounts using an account management system, such as Microsoft Active Directory.
- Configure network and security devices to use the centralized authentication system.
- Limit the number of privileged accounts to those who have a legitimate business requirement.
- Control access to the computer system's audit logs.
- Review all system accounts, and disable any account that cannot be associated with a business process and owner.
- Ensure that all accounts have an expiration date associated with the account.
- Establish a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails should an investigation be necessary, for example.
- Force users to automatically re-login after a standard period of inactivity.
- Require that all employee accounts have strong passwords, which contain letters, numbers, and special characters. Ensure that they are changed every 90 days, and that the previous 15 passwords are not allowed to be used as a new password.
- Require two-factor authentication for privileged accounts or accounts that have access to sensitive data or computer systems. Two-factor authentication can be achieved using Smart cards with certificates, One Time Password (OTP) tokens, or biometrics.

Case Study - Compromised User Accounts - July 2015

In a 'slow-burn' Chinese-origin cyber attack against the United States Office of Personnel Management networks, perpetrators gained authenticated network access to OPM's network by compromising a non-privileged OPM Active Directory domain user account belonging to a KeyPoint contractor.

They used this authenticated non-privileged access to identify the list of all privileged users in OPM's Active Directory deployment, and subsequently engaged in Active Directory Privilege Escalation (using one of these two attack vectors) to compromise a single one of these privileged user accounts, then used it to obtain access to databases. They subsequently exfiltrated the data.

3.10 Asset Management

Managed control of computer systems and software plays a critical role in keeping an organization secure. It is critical to identify and manage all computer systems so that only authorized systems are permitted access to the network. It is just as important to ensure that only authorized software is installed and that unauthorized software is prevented from being executed. Unauthorized, and often insecure, systems and applications typically do not have the latest patches or security updates installed. As a result, they are typically more vulnerable to exploitation.

The following are recommendations for asset management:

- Deploy and maintain an automated asset inventory discovery tool, and use it to build an inventory of systems connected to the organization's private and public network.
- Use Dynamic Host Configuration Protocol (DHCP) server logging to improve the asset inventory and help detect unknown systems through this DHCP information.
- Ensure that the inventory system is updated when newly acquired and approved equipment connects to the network.
- Deploy Network Access Control (NAC) and network level authentication via 802.1x. These security services prevent unauthorized devices from connecting to the network.
- Utilize client certificates to validate and authenticate systems prior to connecting to an organization's network.

Case Study - Application/Program Vulnerabilities - October 2014

A group of attackers operating overseas drilled deep into the computer systems of JPMorgan Chase, compromising the names, addresses, phone numbers, and emails of 76 million households and seven million small businesses.

The hackers obtained a list of the applications and programs that ran on the Bank's computers, which they could crosscheck with known vulnerabilities in each program and web application in search of an entry point into the bank's systems. By the time the bank's security team discovered the breach, hackers had already obtained the highest level of administrative privilege to dozens of the bank's computer servers.

The bank was subsequently required to update its regulators on the extent of the breach, swap out its programs and applications, and renegotiate licensing deals with its technology suppliers.

3.11 Incident Response

Planning and preparing for a cybersecurity incident is one of the greatest challenges faced by any organization. When a cybersecurity incident occurs, it is time to take action and mitigate – as quickly as possible – any threat to the confidentiality, integrity, and availability of an organization’s information assets.

Cyber incident management helps mitigate the risks associated with internal and external threats, as well as helping an organization maintain regulatory compliance where required. An organization must be prepared to handle incidents that may originate from a variety of sources. Sources for cybersecurity incidents include: insiders who act with malicious intent, trusted insiders whose acts cause damage by mistake, and attacks from cyber criminals.

The complexity of malware and the sophistication of cyber criminals’ techniques continue to increase rapidly and, as a result, cybersecurity incidents are becoming more commonplace. Organizations face an uphill battle against cyber criminals who, given enough time and money, can breach the most sophisticated safeguards. Organizations need to perform due diligence and take reasonable measures to respond appropriately in the event of a cybersecurity incident. A poorly executed incident response has the potential to cause an organization significant financial losses, ruin its reputation, and perhaps even drive it out of business altogether.^{xvii} Therefore, creating and implementing an incident response plan is necessary to quickly detect incidents, minimize loss and destruction, mitigate information system weaknesses, and recover from a potential cybersecurity incident.

The following are some of the objectives of cybersecurity incident management:

- Avoid cybersecurity incidents before they occur
- Minimize the impact of cybersecurity incidents to the confidentiality, availability, or integrity of the investment industry’s services, information assets, and operations
- Mitigate threats and vulnerabilities as cybersecurity incidents are occurring
- Improve cybersecurity incident coordination and management within the investment industry
- Reduce the direct and indirect costs caused by cybersecurity incidents
- Report findings to executive management

Key Terms

The definitions below are based on the International Standard for Information Security Incident Management (ISO/IEC 27035).^{xviii}

CYBERSECURITY EVENT

An identified occurrence of a system, service, or network state, **indicating a possible breach** of information security, failure of controls, or a previously unknown situation that may be security relevant.

CYBERSECURITY INCIDENT

A single or a series of unwanted or unexpected information security events that have a **significant probability of compromising business operations** and threatening information security.

Cybersecurity Incidents make up a small proportion of Events.

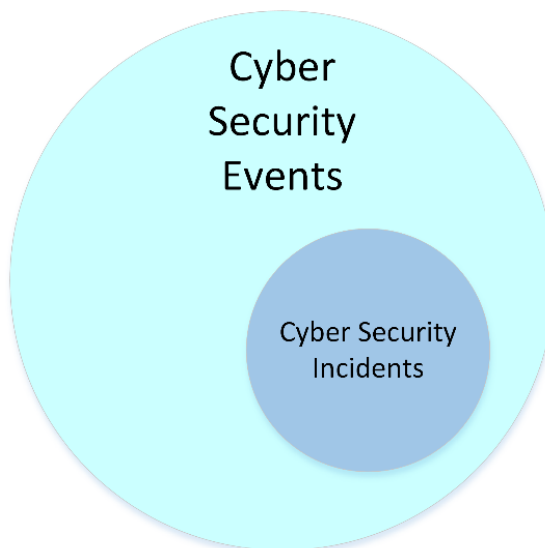


Figure 4 - Cybersecurity Events vs. Cybersecurity Incidents^{xix}

CYBERSECURITY INCIDENT MANAGEMENT

The processes for detecting, reporting, assessing, responding to, dealing with, and learning from cybersecurity incidents.

INCIDENT RESPONSE

The actions taken to protect and restore the normal operational conditions of an information system and the information stored in it when a cybersecurity incident occurs.

INCIDENT RESPONSE TEAM (IRT)

A team of appropriately skilled and trusted members of the organization that handles incidents during their lifecycle.

Once you have detected a cyber incident, immediately contact your legal counsel for guidance on initiating these ten steps:^{xx}

- Record the date and time when the breach was discovered.
- Alert and activate everyone on the response team to begin executing the preparedness plan.
- Secure the premises around the area where the data breach occurred to help preserve evidence.
- Stop additional data loss. Take affected computer systems offline.
- Document everything known about the breach.
- Interview those involved in discovering the breach and anyone else who may know about it.
- Review protocols regarding disseminating information about the breach for everyone involved in this early stage.
- Assess priorities and risks based on what you know about the breach.
- Inform the proper authorities, including your regulator.
- Notify law enforcement, if needed, to begin an in-depth investigation.

The five phases of cybersecurity incident management are outlined in Figure 5 below.

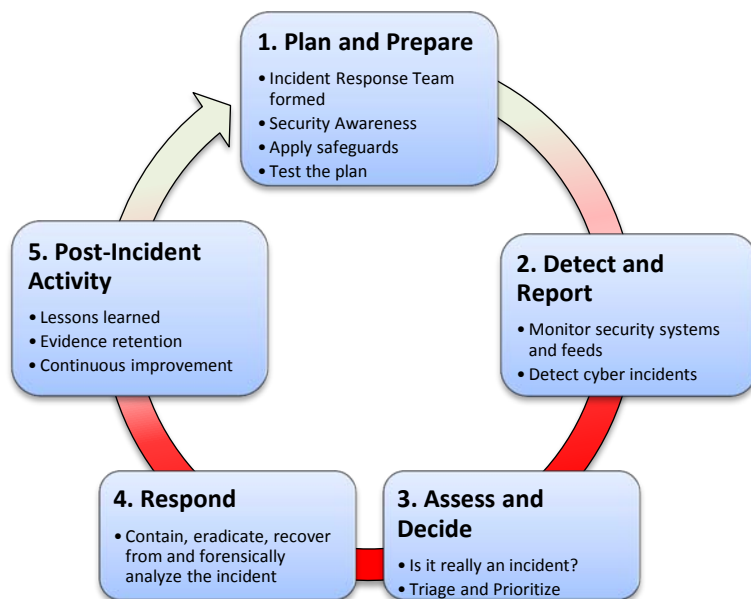


Figure 5 - 5 Key Elements of Cybersecurity Incident Management

1. The first phase involves **Planning and Preparing** for a cybersecurity incident, so that your organization is prepared for a cybersecurity incident when one arises.
2. The **Detect and Report** phase involves the continuous monitoring of information sources, the detection of a cybersecurity event, and the collection and recording of information associated with the event.
3. The **Assess and Decide** phase involves assessing cybersecurity events and deciding whether or not an actual cybersecurity incident has occurred.
4. The **Respond** phase involves containing, mitigating, and recovering from a cybersecurity incident.
5. The **Post-Incident Activity** involves learning from the incident and making changes that improve the organization's security and processes.

➔ **A Cybersecurity Incident Checklist can be found in Appendix A.**

3.12 Information Sharing and Breach Reporting

3.12.1 Privacy Breach Notification

In June, 2015, the Digital Privacy Act amended Canada's foundational Personal Information Protection and Electronic Documents Act (PIPEDA) to state that organizations will be required to notify the Privacy Commissioner and affected individuals of "any breach of security safeguards involving personal information under the organization's control, if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual." The Digital Privacy Act provides for fines up to \$100,000 for knowing violations of the breach notification requirements, and the requirement that organizations keep and maintain a record of every breach of security safeguards involving personal information under the organization's control.

There will be no enforcement of the breach notification requirements in advance of yet to be promulgated regulations. What is clear is that the breach reporting requirements in Canada are changing, and companies need to remain vigilant to their provisions.

PIPEDA does not apply in provinces with privacy legislation that the federal government has deemed to be substantially similar to PIPEDA. Currently, only Alberta, British Columbia and Quebec have comprehensive privacy legislation that has been declared substantially similar to PIPEDA. Of these, only Alberta presently has mandatory breach notification provisions. Companies have an obligation to be aware of the breach notifications in each jurisdiction in which they operate, and to have internal policies consistent with applicable law.

3.12.2 Information Sharing

Cyber-threats are global in nature and not restricted to any one company, industry, or market. Information sharing is an essential element of an effective cybersecurity program. Increasingly within the financial sector, cybersecurity is viewed by market participants as a collective good. Doubts about the integrity of one market participant can quickly shift to others. There is a willingness to participate in sharing of cyber best practices and threat intelligence among members of the financial sector.

The Digital Privacy Act also contains more permissive language than prior statutes to enable organizations to share information amongst themselves for the purposes of detecting or suppressing fraud that is likely to be committed. It is also more permissive for sharing information in furtherance of an investigation a breach of an agreement or a contravention of the laws of Canada or a province that has been, or is reasonably expected to be, committed. While prior legislation required the existence of an accredited investigation body, this legislation appears to permit industries to more effectively exchange relevant cybersecurity as well as other security-related information to protect their interests. The Canadian securities industry is well placed to follow the banking and life insurance industries to establish both ad hoc and structured information sharing arrangements to support companies' cybersecurity programs.

Information sharing is an essential tool for mitigating cyber threats. It spans strategic, tactical, operational, and technical levels, as well as all phases of the cyber incident response cycle. It crosses the boundary of public and private domains. Finally, it can concern sensitive information, which can be potentially harmful for one organisation, while being very useful to others.^{xxi}

For Dealer Members, there are a variety of opportunities and forums for engaging in proactive cyber information sharing. Public Safety Canada operates the Canadian Cyber Incident Response Centre (CCIRC) for the express purpose of facilitating cyber information exchange across Canadian industry and with the Government of Canada. This Centre operates one of the most sophisticated malware labs in Canada and can provide invaluable assistance to Dealer Members that have encountered a cyber threat.

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is a global information sharing resource focused upon cyber and physical threats to the international financial community. FS-ISAC is continually looking for threat data, from its members and which might affect its members, in order to proactively warn of potential threats.

The forgoing examples are just two of a variety of communities operating to effectively share cybersecurity information and best practices. These information sharing communities operate on the principle that effective cybersecurity is a collective good and one institution's security incident is the community's early warning report. Dealer Members are encouraged to support these communities with relevant incident reports and to leverage information received through information sharing to optimize their cybersecurity programs.

Microsoft makes the following eight recommendations for information sharing.^{xxii}

1. Develop a strategy for information sharing and collaboration.

- a. An information sharing strategy can help organizations: identify priorities, establish shared values, and plan to build effective information sharing processes.
- b. The information sharing strategy should contain answers the following questions:
 - i. Who needs to share information, and who can resolve the issues that emerge?
 - ii. What information is being shared, and what is the purpose of sharing it?
 - iii. What is the impetus behind information sharing? Is it shared voluntarily or a regulated requirement?
 - iv. What is the organizational structure for sharing information?
 - v. How is the information actually shared securely?
 - vi. How is an information exchange structured to ensure that it delivers the greatest value?

2. Design with privacy protections in mind.

Information sharing efforts must respect privacy, and should be designed with the aim of protecting this to the highest degree.

3. **Establish a meaningful governance process.**

Ensuring that members follow information sharing rules is essential to the credibility of the effort and builds trust. A meaningful governance process should include appropriate management of the data shared, from its creation and release to its use and destruction.

4. **Focus sharing on actionable threat, vulnerability, and mitigation information.**

Sharing actionable information empowers organizations to improve their defense of networks and mitigate threats.

5. **Build interpersonal relationships.**

Building trust between information sharing participants, along with trust in the program itself, is critical. The more that information sharing participants act in good faith, the more likely other participants are to share information on threats and vulnerabilities.

6. **Require mandatory information sharing only in limited circumstances.**

In some instances, such as in the case of national security and public safety, there may be a need for mandatory incident reporting. Such mandatory approaches should be narrowly defined and implemented through trusted mechanisms.

7. **Make full use of information shared, by conducting analyses on long-term trends.**

An analyses of trends gleaned from shared information can help build knowledge of long-term trends, giving network defenders a better understanding of emerging cyber-threats and helping them defend against or prevent future threats.

8. **Encourage the sharing of best practices.**

The exchange of best practices with peer organizations can allow organizations to play a proactive role, by engaging with each other as well as external organizations.

3.13 Cyber Insurance

Coverage for data breaches under traditional commercial policies has become increasingly uncertain. In the early 2000s, insurers began to offer insurance policies specifically geared towards protecting against financial losses from data breaches.

Types of risks and potential losses include:

- Identify theft
- Business interruption
- Damage to reputation and goodwill
- Investigation and remediation costs
- Restoration of property costs
- Theft of digital assets
- Malware and viruses
- Human error
- Litigation costs

Insurance coverage for certain losses may be available under existing traditional insurance policies:

- Directors and Officers (D&O)
- Errors and Omissions (E&O) / Professional Liability
- Crime / Theft
- Property
- Commercial General Liability (CGL)

In many cases, traditional insurance coverage does not cover the full range of risks and potential losses posed by cyber risks. When reviewing potential insurers, it is important to be aware that this sub-specialty remains in the formative stages, thus there are no standard policy terms within the industry.

A best practice is to carefully review existing company and D&O insurance policy provisions as they relate to data breach and privacy claims, and ensure that such claims are not excluded. As part of a comprehensive cybersecurity strategy, determine the type and extent of coverage that best serves the interests of the firm, and seek a tailored package of insurance that covers the full range of potential exposure to which a cyber-incident would subject the firm.

Retroactive coverage is a key consideration. Cyber-breaches can go months if not years without detection, thus members should consider that they may have already been the victim of an undetected breach at the time that they are seeking coverage. In some cases, insurers may be willing to provide retroactive coverage for up to two years before writing the policy. This feature is highly dependent upon the unique risk profile of the potential insured party and the nature of their pre-existing cybersecurity program.

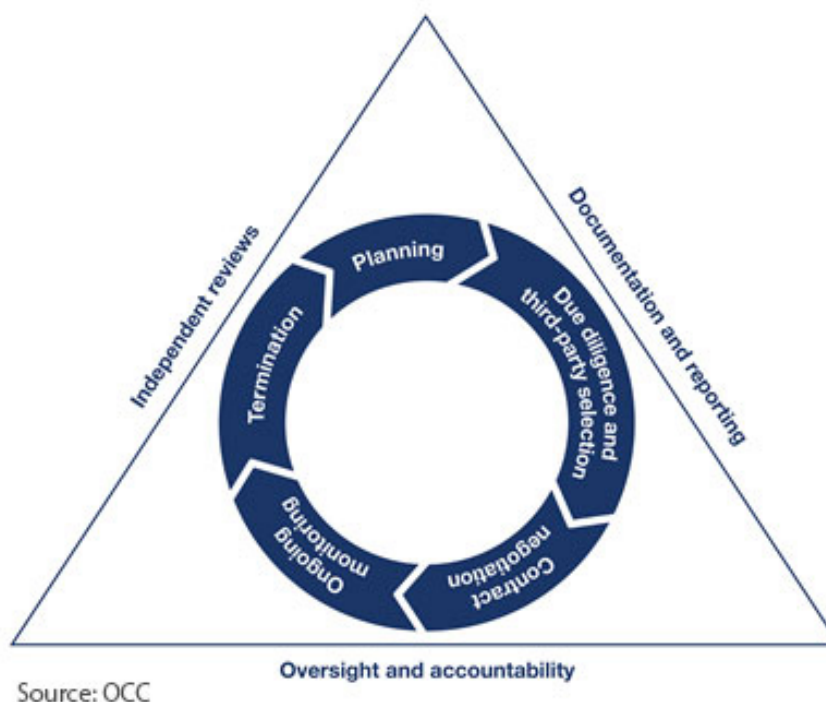
Typical coverage offered within cyber policies currently may include:

Examples of Cyber-insurance Coverage	
First-party Coverage	Third-party Coverage
<p>Hiring professional response:</p> <ul style="list-style-type: none"> • Attorneys to advise • Public relations firms • Crisis management firms • Computer forensics firms <p>Notification costs:</p> <ul style="list-style-type: none"> • Direct costs including printing/mailing • Credit monitoring services for affected persons <p>Administrative safeguard costs:</p> <ul style="list-style-type: none"> • Training employees • Establishing information portals • Creating security and incident response templates • Compensating the insured for lost income as result of breach • Restoring lost data 	<ul style="list-style-type: none"> • Cost of regulatory defense including fines and punitive damages • Cost of litigation defence • Litigation damages

3.14 Vendor Risk Management

The number of security incidents at companies that are attributed to client systems, partners and vendors has risen from 20 percent in 2010 to 28 percent in 2012.^{xxiii} Perhaps the best-known example of vendor risk was the massive 2013 data breach at Target Corp, where hackers gained access to Target's credit card data through a third-party heating and air conditioning contractor. Up to 40 million credit and debit card numbers were exposed in that breach.

The essential elements of a vendor risk management program include: risk ranking vendors, developing clear policies which vendors are expected to adhere to, making conditions explicit within contracts, and establishing a program to verify the performance of vendors.



*Figure 6 – Risk Management Life Cycle for Third Party Risk
Office of the Comptroller of the Currency (OCC)*

It is virtually impossible to find a business today that does not rely on third-party vendors. Given the cyber risks that third-party vendor relationships pose, firms impute the security practices of those vendors into their own risk profile. The U.S. Office of the Comptroller of the Currency (OCC) developed an excellent framework upon which to develop an effective vendor risk management program (see Figure 6 above). This lifecycle model highlights the key preliminary planning, diligence, and negotiations steps to ensure that vendors adhere to the firm's security policies. While ongoing monitoring is critical, so too is planning for the termination of the relationship to ensure that access to networks is severed and confidential data is returned.

A best practice is to approach vendor risk management in a tiered fashion with highest risk relationships approached first. Vendor Stratification^{xxiv} can be approached with the following considerations:

Service Risks:

- Volume of financial transactions processed
- Concentration associated with service
- Sensitivity risk of the data to which the vendor could potentially have access
- Compliance and regulatory risk related to the service
- Customer and financial impact

Vendor Risks:

- Location of the vendor (subject to multinational laws, regulations, etc.)
- Previous data or security breaches
- Extent of outsourcing performed by the vendor
- Performance history

Common Deficiencies with 3rd Party Vendors:

- Incident Response Management Plan
- Inadequate Security Awareness
- Data Loss Prevention
- Encryption for data at rest and in transit
- Administrator Privilege Lockdown
- Vulnerability testing or penetration testing

Common Approaches to Evaluating Third Party Vendors Include:

- Questionnaires incorporated into RFPs
 - See Appendix B for a Sample Vendor Assessment Questionnaire.
- Requests for documentation from potential vendors
 - For examples of types of documentation, see Appendix B for a Sample Vendor Assessment Questionnaire.
- Desk assessments to evaluate requested information
- On-site visits as appropriate by either in-house or contacted experts
- Penetration tests of potential vendors

To be successful, vendor risk management should be an element of an enterprise risk management program with established, repeatable processes in place that are consistent for all areas within the firm.

Case Study - ‘Hacking for Shorting’ - 2010 to 2014

Over the course of five-years, from 2010 to 2014, overseas hackers working with traders in the United States stole non-public corporate information and made lucrative bets by accessing servers at PRNewswire Association LLC, Marketwired LP and Business Wire.

The suspects used spearphishing techniques, and inserted malicious programming code into applications or websites to gain access to databases of corporate news releases. They would then exploit the period between when news releases were uploaded by listed companies into newswires’ systems and when the services issued public announcements of the news.

The scheme was the largest known collaboration between hackers and traders, reaping at least \$30 million in illegal profits and underscoring the hidden danger of modern finance and the broader Web, in which any one compromised link in the larger chain can quietly endanger the system for years.

3.14.1 Cloud Computing

In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of on a computer hard drive.^{xxv} While there are many advantages to cloud-based computing, it carries with it risks that are similar to those associated with outsourcing to third-party vendors; however, unlike third-party vendors, a cloud vendor’s primary business is the storage of critical applications and sensitive data. As a result, security and data privacy are the top concerns of most firms considering their use. Firms should consider the risks and threats involved, in addition to the amount of risk that they are willing to accept. Risks include data or application unavailability, data loss, theft, and the unauthorized disclosure of sensitive information.

In addition to the risk mitigation guidance outlined in the Vendor Management section, firms considering the use of cloud services should look for a provider with the following characteristics:^{xxvi}

- A significant history in the cloud services industry who can provide solid business references
- The provider clearly outlines its mitigating controls for handling risk – controls related to security, availability, processing integrity, confidentiality, and privacy
- They allow auditing and the verification of controls
- They are certified or recognized by one or more security standards authorities
- Their backup procedures, business continuity plans, and disaster recovery plans meet your firm’s requirements

3.15 Cyber Policy

A cybersecurity program is defined by its underlying policy. The firm's security policy is the articulation of the organization's objectives agreed upon by management that establish those requirements that must be followed. Rather than guidance, **policy establishes mandatory conduct**.

Creating a security policy requires management to articulate what they believe is necessary and what risks they are willing to accept. Rather than merely "downloading" a security policy template, a best practice is to engage firm leadership in an education process regarding security risks in order to develop an informed consensus amongst firm leadership and with it, the authority upon which to develop and deliver the cybersecurity strategy.

Security policy, as opposed to cybersecurity policy, is a term deliberately used. Security comprises physical security, personnel security, cybersecurity, as well as supporting business continuity practices. While this guide is focused upon cybersecurity, effective cybersecurity cannot be achieved absent an integration of the other security disciplines.

Key elements of a policy include:

- Scope – all information, systems, facilities, programs, data networks, and all users of technology in the organization (both internal and external), without exception
- Information classification – should provide content-specific definitions, rather than more generic "confidential" or "restricted"
- Management goals for secure handling of information in each classification category
- Placement of the policy in the context of other management directives and supplementary documents
- References to supporting documents, including industry standards and guidelines
- Specific instruction on organization-wide security mandates (e.g. no sharing of passwords)
- Specific designation of established roles and responsibilities
- Consequences for non-compliance (e.g. up to and including dismissal or termination of contract)^{xxvii}

The implementation of a policy is not a single event, but rather an iterative process revisited as business models, relationships, and technology changes. **Absent policy, there can be no effective governance of the cybersecurity program as there can be no clear guidance upon which to make program decisions.**

Appendix A – Cybersecurity Incident Checklist

These following are the processes and procedures that need to be in place before, during, and after a cybersecurity incident^{xxviii}:

CYBERSECURITY INCIDENT CHECKLIST

BEFORE AN INCIDENT

- ☐ Create a prioritized list of information assets critical to the functioning of your organization.
- ☐ Identify the stakeholders responsible for each critical asset.
- ☐ Create an Incident Response Team, who will be responsible for all incidents (including individuals from legal, corporate communications, and HR).
- ☐ Ensure proper monitoring and tracking technologies are in place to protect your organization's information assets (such as firewalls, IPS, and anti-virus).
- ☐ Provide media training to the proper individual(s).
- ☐ Provide a company-wide process for employees, contractors, and third parties to report suspicious or suspected breach activities.
- ☐ Provide company-wide training on breach awareness, employee responsibility, and reporting processes.

[Continued on next page]

DURING AN INCIDENT

- ☐ Record the issues and open an incident report.
- ☐ Convene the Incident Response Team.
- ☐ Convene a teleconference with requisite stakeholders to discuss what must be done in order to restore operations.
- ☐ Convene a management teleconference with requisite stakeholders in order to provide situational awareness to executive management.
- ☐ Triage the current issues and communicate to executive management.
- ☐ Identify the initial cause of the incident and activate the specialists to respond to the current issues to restore operations.
- ☐ Retain any evidence and follow a strict chain of evidence to support any needed or anticipated legal action.
- ☐ Communicate to affected third parties, regulators, and media (if appropriate).

AFTER AN INCIDENT

- ☐ Update the incident report and review exactly what happened and at what times.
- ☐ Review how well the staff and management performed in during the incident.
- ☐ Determine whether or not the documented procedures were followed.
- ☐ Discuss any changes in process or technology that are needed to mitigate future incidents.
- ☐ Determine what information was needed sooner.
- ☐ Discuss whether any steps or actions taken might have inhibited the recovery.
- ☐ Determine which additional tools or resources are needed to detect, triage, analyze, and mitigate future incidents.
- ☐ Discuss what reporting requirements are needed (such as regulatory and customer).
- ☐ If possible, quantify the financial loss caused by the breach.

Appendix B – Sample Vendor Assessment

Adapted from the University of British Columbia's Third-Party Assessment Questionnaire^{xxix}.

The original copy is available at the following

address: <https://it.ubc.ca/sites/it.ubc.ca/files/3rd%20Party%20Outsourcing%20Information%20Security%20Assessment%20Questionnaire%20V1.4.xlsx>

Additional sources:

- ISACA's Vendor Management using COBIT 5^{xxx} and
- Cloud Security Alliance's Consensus Assessments Initiative Questionnaire V3.0.1^{xxxi}

Sample Vendor Assessment

Name of Company	
Email Address Phone Number Company's Website	
Date of assessment:	
Additional Documents Provided	<input type="checkbox"/> Network Diagram <input type="checkbox"/> Security Architecture <input type="checkbox"/> Security Assessment Results <input type="checkbox"/> Security Policies <input type="checkbox"/> SSAE16, ISO reports <input type="checkbox"/> Risk Management Policy <input type="checkbox"/> Vendor Management Policy <input type="checkbox"/> Change Management Plan <input type="checkbox"/> Backup and Restore Procedures <input type="checkbox"/> Record Retention Policy <input type="checkbox"/> Incident Management Plan <input type="checkbox"/> Business Continuity Plan <input type="checkbox"/> Disaster Recovery Plan <input type="checkbox"/> Risk Assessment Procedures <input type="checkbox"/> Other Relevant Documentation

Vendor Controls	Vendor Response Yes/No/Partially Implemented
1. Allows on-site security audit with 24 hours' notice.	
2. Will store all data in Canada.	
3. Maintains an audit log for the location of all confidential data.	
4. Will not access confidential data from outside of Canada.	
5. Can provide recent results of external Information Security assessments	
6. Maintains incident response procedures.	
7. Has a policy to protect client information against unauthorised access	
8. Has a policy that prohibits sharing of individual accounts and passwords.	
9. Has a policy that implements the need-to-know and separation-of-duties principles	
10. Implements multi-factor authentication in order to access client resources	
11. Performs background checks on all employees	
12. Provides customer support with escalation procedures.	
13. Has documented change control processes.	
14. Requires employees to attend regular security awareness and training sessions	
Security Architecture	Vendor Response Yes/No/Partially Implemented
1. Will provide a network topology diagram.	
2. Implements network firewall protection.	
3. Implements web application firewall protection.	
4. Implements host firewall protection.	
5. Provides network redundancy.	
6. Has Intrusion Prevention Systems technology implemented.	
7. Implements a three-tiered DMZ architecture for Internet-facing systems.	
8. Uses enterprise virus protection on all systems.	
9. Implements a patch management program	
10. Provides dedicated customer servers to segregate data from other customer data. If not, then how is this accomplished in a secure virtual or segmented configuration?	
11. Implements controls to restrict access to data from other customers.	
12. Remote access takes place over secure connections that employs multi-factor authentication	
13. The development, test, and production environments are separated physically or virtually	
14. Employs managed, secure access points on its wireless network.	

Information System Configuration	Vendor Response Yes/No/Partially Implemented
1. Implements encryption for confidential information at a strength of at least AES 128 bit and TLS 1.0	
2. Has password-protected screen savers that activate automatically to prevent unauthorised access to systems.	
3. Uses file integrity monitoring software on servers (such as tripwire, etc.).	
4. Uses passwords with at least 10 characters that have complexity requirements are must be changed every 90 days.	
5. Ensures that passwords are never stored in clear text	
6. Implements redundancy or high availability for critical functions.	
7. Does not use production data in development or test environments.	
8. Sets account lockout feature for successive failed logon attempts on all system's support computers.	
9. Prohibits split tunneling when connecting to customer networks.	
Access Controls	Vendor Response Yes/No/Partially Implemented
1. Immediately removes or modifies access when personnel terminate, transfer, or change job functions.	
2. Ensures that critical data, or systems, are accessible by at least two trusted and authorised individuals, in order to limit having a single point of service failure.	
3. Ensures that users have the authority to only read or modify those programs, or data, which are needed to perform their duties.	
Security Monitoring	Vendor Response Yes/No/Partially Implemented
1. Reviews access permissions for all server files, databases, application regularly	
2. Reviews and analyses after hour's system accesses regularly.	
3. Reviews system logs for failed logins, or failed access attempts regularly	
4. Reviews and removes dormant accounts on systems regularly.	
5. Reviews network and firewall logs regularly.	
6. Reviews wireless access logs at least regularly.	
7. Performs scanning for rogue access points regularly.	

Physical Security	Vendor Response Yes/No/Partially Implemented
1. Controls access to secure areas.	
2. Controls access to server rooms and follows the principles of least privilege and need-to-know.	
3. Safeguards in place (e.g., cipher locks, restricted access, room access log, card swipe access control)	
4. Shreds or incinerates printed confidential information.	
5. Escorts visitors in computer rooms or server areas.	
6. Implements environmental controls to mitigate the environmental threats to equipment.	
Contingency Planning	Vendor Response Yes/No/Partially Implemented
1. Has a written contingency plan for mission critical computing operations.	
2. Updates the contingency plan at least annually.	
3. Has written backup procedures and processes.	
4. Tests the integrity of backup media quarterly.	
5. Stores backup media in a secure manner and controls access.	
6. Maintains a documented and tested disaster recovery plan.	
7. Provides notification in the event of a breach	
8. Has the vendor experienced a cyber security breach in the past three to five years?	
9. If so, please outline what information was lost in the comments section?	
Vendor's Business Associates	Vendor Response Yes/No/Partially Implemented
1. Confidentiality agreements have been signed before proprietary and/or confidential information is disclosed to the vendor's business associates.	
2. Vendor's business associate contracts, or agreements, are in place and contain appropriate risk coverage for customer requirements.	
3. Vendor's business associates are aware of customer security policies and what is required of them.	
4. Vendor's business associate agreements document the agreed transfer of customer's data when the relationship terminates.	

Appendix C – Glossary

This section uses the Government of Canada’s *GetCyberSafe Guide for Small and Medium Business* as an authoritative source in order to provide the reader with an understanding of the key terms used in this document.

Assets: Any items belonging to or held by the business with some value (including information, in all forms and computer systems).

Attack: An attempt to gain unauthorized access to business or personal information, computer systems or networks for (normally) criminal purposes. A successful attack may result in a security breach or it may be generically classified as an “incident.”

Authentication: A security practice implemented (usually through software controls) to confirm the identity of an individual before granting them access to business services, computers or information.

Backup: The process of copying files to a secondary storage solution, so that those copies will be available if needed for a later restoration (e.g., following a computer crash).

Breach: A security breach is a gap in security that arises through negligence or deliberate attack. It may be counter to policy or the law, and it is often exploited to foster further harmful or criminal action.

Cyber: Relating to computers, software, communications systems and services used to access and interact with the Internet.

Encryption: Converting information into a code that can only be read by authorized persons who have been provided with the necessary (and usually unique) “key” and special software so that they can reverse the process (e.g., decryption) and use the information.

Firewall: A firewall is a type of security barrier placed between network environments. It may be a dedicated device or a composite of several components and techniques. Only authorized traffic, as defined by the local security policy, is allowed to pass.

Identity Theft: Copying another person’s personally identifying information (such as their name and Social Insurance Number) and then impersonating that person to perpetrate fraud or other criminal activity.

Malware: Malicious software created and distributed to cause harm. The most common instance of malware is a “virus.”

Patch: An update to or repair for any form of software that is applied without replacing the entire original program. Many patches are provided by software developers to address identified security vulnerabilities.

Password: A secret word or combination of characters that is used for authentication of the person that holds it.

Phishing: A specific kind of spam targeting one or more specific people while pretending to be a legitimate message, with the intent of defrauding the recipient(s).

Risk: Exposure to a negative outcome if a threat is realized.

Safeguard: A security process, physical mechanism or technical tool intended to counter specific threats. Sometimes also referred to as a control.

Server: A computer on a network that acts as a shared resource for other network-attached processors (storing and “serving” data and applications).

Spam: Email that has been sent without the permission or request of you or the employee it has been sent to.

Threat: Any potential event or action (deliberate or accidental) that represents a danger to the security of the business.

VPN: Virtual Private Network.

Vulnerability: A weakness in software, hardware, physical security or human practices that can be exploited to further a security attack.

Wi-Fi: A local area network (LAN) that uses radio signals to transmit and receive data over distances of a few hundred feet.

Appendix D - References

NIST Cybersecurity Framework, Version 1.0, 2014

CGI, “Cybersecurity in Modern Critical Infrastructure Environments,” 2014

ENISA, “Technical Guideline on Security Measures,” Version 2.0, 2014

Public Safety Canada, “Industrial Control System (ICS) Cyber Security: Recommended Best Practices,” 2012

xxxii xxxiii xxxiv xxxv

ⁱ NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*

ⁱⁱ Australian Signals Directorate. “Strategies to Mitigate Targeted Cyber Intrusions”. February 2014

ⁱⁱⁱ GetCyberSafe Guide for Small and Medium Businesses

^{iv} National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. 2014

^v Cyber-Ark (2012). “2012 Trust, Security & Passwords Survey”

^{vi} CERT Insider Threat Center, <http://www.cert.org/insider-threat/>

^{vii} Bunn, C. (2013). A Focus on Insider Threats in Banking & Financial Institutions

^{viii} Shaw, E.D. and Stock, H.V. (2011). Harley V. Stock, Ph.D. Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall

^{ix} Price Waterhouse Coopers. 2015 Global State of Information Security® Survey. 2015

^x CyberEdge Group. 2015 Cyberthreat Defense Report: North America & Europe. 2015

^{xi} The Council On CyberSecurity. The Critical Security Controls For Effective Cyber Defense. 2015: 27-32

^{xii} Communications Security Establishment Canada. Baseline Security Requirements for Network Security Zones in the Government of Canada. 2007: 5

^{xiii} Public Safety Canada. Industrial Control System (ICS) Cyber Security: Recommended Best Practices. 2012

^{xiv} Government of Canada. GetCyberSafe Guide for Small and Medium Businesses

<http://www.getcybersafe.gc.ca/cnt/rsrscs/pblctns/sml-bnss-gd/sml-bnss-gd-eng.pdf0>

^{xv} Trend Micro. Mobile Consumerization Trends & Perceptions: IT Executive and CEO Survey. 2012

^{xvi} Fraud Advisory Panel. Bring your own device (BYOD) policies. 2014

^{xvii} ISACA. Incident Management and Response. 2012

^{xviii} ISO/IEC. ISO 27035-2 (2nd Working Draft), Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management

^{xix} Government of South Australia. ISMF Guideline 12aCybersecurity Incident Reporting Scheme. 2014

^{xx} Experian Data Breach Resolution. Data Breach Response Guide. 2013

^{xxi} Luijff, E. and Kernkamp, A. Sharing Cyber Security Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach. March 2015

^{xxii} Goodwin, C. and Nicholas, J. P. (Microsoft). A Framework for Cybersecurity Information Sharing and Risk Reduction. 2015

^{xxiii} PwC 2013 Global State of Information Security Survey.

^{xxiv} Ibid.

^{xxv} What Is Cloud Computing?. Eric Griffith. <http://www.pcmag.com/article2/0,2817,2372163,00.asp>. April 2015

^{xxvi} ISACA. Security Considerations for Cloud Computing. 2012

^{xxvii} “How to write an information security policy,” CSO Online. Available at

<http://www.csoonline.com/article/2124114/strategic-planning-erm/how-to-write-an-information-security-policy.html>

^{xxviii} Hewlett-Packard. Executive breach response playbook: How to successfully navigate the enterprise through a serious data breach. 2015

^{xxix} University of British Columbia. Third-Party Assessment Questionnaire

<https://it.ubc.ca/sites/it.ubc.ca/files/3rd%20Party%20Outsourcing%20Information%20Security%20Assessment%20Questionnaire%20V1.4.xlsx>

^{xxx} ISACA. Vendor Management using COBIT 5. <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/VendorManagementDownload.aspx>

^{xxxi} Cloud Security Alliance. Consensus Assessments Initiative Questionnaire V3.0.1. <https://downloads.cloudsecurityalliance.org/initiatives/cai/caiq-v3.0.1.zip>

^{xxxii} <http://www.antifraudcentre-centreantifraude.ca/fraud-escroquerie/types/phishing-hameconnage/index-eng.htm#wirefraud>

^{xxxiii} <http://www.cbc.ca/news/technology/ashley-madison-data-dump-what-s-at-risk-and-for-whom-1.3199031>

^{xxxiv} <http://www.law360.com/articles/662840/sec-finra-officials-talks-cyberbreach-enforcement>

^{xxxv} <http://www.cbc.ca/news/canada/nova-scotia/cryptowall-virus-hits-some-mahone-bay-and-bridgewater-town-computers-1.3171424>

<http://www.cbc.ca/news/world/100m-cybercrime-ring-busted-by-u-s-led-team-of-investigators-1.2662871>