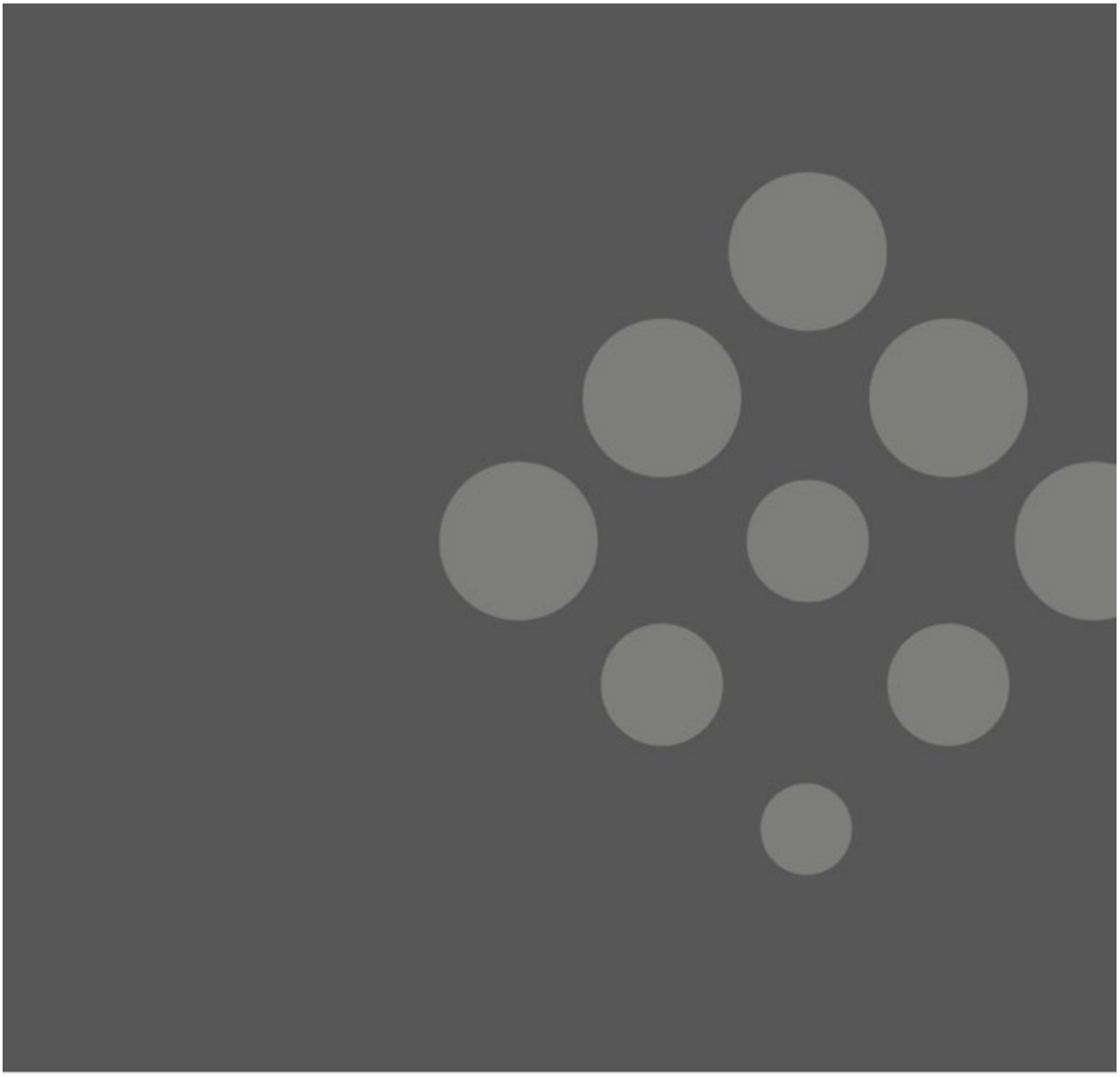


IIROC Cyber Governance Guide

January 31, 2020

IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

juno risk solutions

1. INTRODUCTION

The IIROC Cyber Program Governance Guide is intended to provide IIROC dealer members (**dealer member**) with explicit guidance on how best to implement, manage and advance a cybersecurity program. This document should be read in conjunction with the 2015 IIROC Cybersecurity Best Practices Guide as it incorporates and expands upon the information within that Guide. This Guide reflects the experience gained by both IIROC and dealer members in developing and implementing programs to counter cyber threats.

1.1 DOCUMENT STRUCTURE

The document is structured to provide dealer members with an understanding of the present state of the threat they face from cyber criminals, hostile foreign intelligence services and from its own employees and third-party business stakeholders. Dealer members are encouraged to remain vigilant to changes in the threat environment including new schemes employed to breach systems, exploit information, or access funds.

1.2 THE CHALLENGE

The best way to characterize the nature of the challenge faced by dealer members relative to cyber attackers is in the context of two competing business models. Dealer members in the securities industry rely on an ecosystem of clients, internal systems, staff and a range of third-party relationships to provide services to its clients and to generate revenue. The cyber criminals' business model requires the successful penetration of your business model in order to generate revenue. Typically, cyber-attacks are the work of organized criminals employing their own ecosystem of third-party partners: to provide access to malware and phishing-attacks-as-a-service, to move ransomware payments with cryptocurrency, and to find the next target. Paying these illicit service providers depends on the successful penetration of companies with access to funds. In much the way the drug trade evolved into an integrated multi-national business, organized crime has shifted to cyber-crime as a low-risk, high-value criminal business.

1.3 THE APPROACH

This report has been written to support a holistic view of cybersecurity and to expand on best practices for IIROC dealer members.

Section 2 examines the current threat operating environment for dealer members with a focus on human and cyber-oriented tradecraft.

Section 3 proceeds by providing guidance on the legal dimensions of sound cyber governance, and touches on the evolving and complex nature of the cyber insurance market.

Section 4 introduces the NIST Cybersecurity Framework and the idea that some safeguards should be given higher priority than others given a dealer member's capability, the nature of the threat and the business of financial services.

Section 5 provides a governance framework upon which to view potential NIST safeguards and to prioritize their implementation. The aim of this relative ranking is to provide dealer member leadership with a sense of the relative benefit of a specific security investment.

Section 6 advances a series of recommendations for security based on established best practices.

Sections 7 and **8** provide an overview of key considerations for cyber incident response. These discussions include the nature of triggering events, the relationship between a dealer member's internal resources and external vendors necessary for successful cyber incident response, and how best to align dealer member needs when engaging cyber insurance providers to establish sufficient coverage.

Lastly, **Section 9** addresses the importance of information sharing and breach reporting.

2. THREAT ENVIRONMENT

2.1 WHAT CONSTITUTES A THREAT?

IIROC dealer members are at risk from cyber threats. "Cyber threat" is a generic term that often fails to generate the understanding necessary to focus corrective action on the risks posed. It is recommended that dealer members begin with an ongoing effort to personify the threat specifically posed to their own business. Consider what valuable information or access your firm retains, how it can be exploited for criminal gain and who might be the type of criminal or other threat actor that may seek to exploit it. Once a view of who might seek access to your firm's systems and how they would exploit that access, it is an easier task to consider the firm's vulnerabilities and to prioritize their treatment.

A threat is composed of an actor with the *capability*, *intention* and the *opportunity* to cause damage. An actor requires all three of these characteristics to constitute a threat. This section discusses possible threat actors and how they can cause harm through the use of human and cyber-oriented tradecraft. The term tradecraft is used in the section to connote the means and methods employed by threat actors to gain access to systems and information. Cyber tradecraft continues to develop, and mimics advances in security controls. This section is intended to introduce the key concepts to help better consider the security control best practices offered in later sections.

2.2 THREAT ACTORS

This section will explore the many threat actors that constitute insider threats to IIROC and its dealer members. Experience has shown that illustrating the nature of the threat by referring to the experiences others assists in more effective security program design decisions.

Insider Threats

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."[1] Insider threats can manifest as security threats linked to either nation state or criminal espionage, or through the unauthorized disclosure of sensitive material.

Edward Snowden, a former National Security Agency contractor, stole millions of classified documents and perpetrated the largest and most damaging public release of classified material in U.S. history. The House Select Committee on Intelligence Report, released in redacted form in December 2016, highlights a pattern of behaviour by Snowden including false statements on employment documents, challenges to authority and conduct exceeding his authority that

[1] Carnegie Mellon University, *The CERT Insider Threat Centre*, 2017

clearly suggest in hindsight issues related to reliability.[2] The theft and release of classified material was another expression of these behavioral characteristics.

The U.S. Office of the Comptroller of the Currency reported to Congress in the fall of 2015 that a former employee downloaded in excess of 10,000 files onto two removable thumb drives and took them with him before he retired.[3] The U.S. Federal Deposit Insurance Corporation disclosed to Congress seven breaches that occurred as employees left the agency, taking with them sensitive data. The incidents potentially exposed the private information of nearly 160,000 Americans.[4]

Employees who have heightened privileges pose a particularly significant threat. Canadian Pacific Railway (CPR) was hit by an act of network sabotage by an employee who was terminated.[5] In late 2015, a computer system administrator, Christopher Grupe was suspended for 12 days for insubordination. Upon his return to work, CPR decided to terminate him but agreed to let him resign instead. While still having network access, Grupe used his active remote access credentials to remove admin-level access from other accounts, delete important files from the network and changed passwords so other employees could no longer access the network. He also deleted any logs showing what he had done. The damage was so extensive that the network had to be re-established.

An insider threat originates from either a staff member or an invited party who is cleared to access the facility, but who acts contrary to the norms and code of conduct of that institution. IIROC and its dealer members employ thousands of staff directly and engage a number of temporary contractors, students, and term employees. This creates a diverse and often transitory workforce with access to their facilities.

Organized Crime

Organized crime poses a serious long-term threat to Canada's institutions, society, economy, and to the quality of life of Canadians. Transnational organized criminal groups have achieved the same level of sophistication recently exhibited by only major nation state intelligence agencies. At present, cyber-crime offers low-risk, high-reward opportunities for those with the means to conceive of and execute criminal schemes. Fraud, identify theft, and extortion are three generic manifestations.

The marketplace for intelligence gathering and criminal exploitation of information has rapidly matured in recent years. The notion that protections are afforded to organizations simply because of the granular, unstructured and/or seemingly uninteresting nature of the data they hold makes their exploitation improbable, is false. Hackers for hire provide their services to

[2] U.S. House of Representatives, *"Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden"*, 2016

[3] The Wall Street Journal, "*U.S. Bank Regulator Notifies Congress of Major Data Security Breach*," October 28, 2016

[4] Ibid.

[5] U.S. DOJ, "*Former Employee of Transcontinental Railway Company Found Guilty of Damaging Ex-Employer's Computer Network*," October 10, 2017

criminals who have the knowledge of how to exploit internal information and the intention to launch schemes for financial gain.

Financially savvy criminals with knowledge of how to exploit proprietary information are known to use hackers in order to gain access to the information necessary to further their schemes. In 2014, 76 million commercial and seven million small business accounts were stolen from JP Morgan & Chase Co.[6] In an indictment charging three individuals, the Federal Bureau of Investigation described the co-conspirators looking to further a traditional pump-and-dump stock manipulation scheme and engaging a hacker to breach a number of financial institutions in order to get email addresses of potential targets touting its selected stocks. The scheme allegedly netted many millions of dollars for the conspirators.

Foreign and Corporate Espionage

In December 2018, David Vigneault, the Director of the Canadian Security Intelligence Service (CSIS), stated that the greatest threat to Canadian prosperity and national interest is foreign interference and espionage.[7] Mr. Vigneault stated that hostile foreign intelligence services, or people who are working with the tacit or explicit support of foreign states, actively gather political, economic, commercial, or military information through clandestine means in Canada.

Foreign states, in particular China and Russia, pose significant intelligence threats to Canadian government institutions and private industry. A recently published study of Chinese military collaboration with foreign universities highlights the use of academic research opportunities to collect sensitive research and to establish relationships with foreign research leaders.[8] Dozens of People's Liberation Army (PLA) scientists have obscured their military affiliations to travel to Five Eyes countries (Canada, Australia, New Zealand, UK and U.S.) and the European Union. In addition, the Chinese military have sponsored more than 2,500 scientists to travel to foreign universities over the past decade. Of the top ten universities outside of China chosen for PLA collaboration, University of Waterloo is 4th, University of Toronto and McGill University are 9th and 10th respectively.

In 2017, China's National People's Congress passed the National Intelligence Law which included language stating that it is the duty of all Chinese citizens to cooperate with state intelligence and security agencies.[9] The law sanctions the co-opting of officials in other Chinese government agencies and compelling cooperation from other PRC citizens. The implication is that Chinese government officials from ostensibly benign departments can also pose an intelligence collection threat.

---

[6] Wired, "*Four Indicted in Massive JP Morgan Chase Hack*," November 10, 2015

[7] Government of Canada, "*Remarks by Director David Vigneault at the Economic Club of Canada*" December 4, 2018

[8] Australian Strategic Policy Institute, "*Picking flowers, making honey.*" October 30, 2018

[9] Government of Canada, "*China's intelligence law and the country's future intelligence competitions*"

Social media is used by organized criminal groups and foreign intelligence services to identify individuals with access to relevant information. Extensive use of fake profiles to initially connect to and then communicate with targeted individuals is one tactic employed. German and French intelligence services have warned their citizens of the extensive use of LinkedIn by Chinese intelligence to identify individuals with access to information of interest to the Chinese government. Germany's domestic intelligence agency asserts that China has used LinkedIn to target at least 10,000 people.[10] The French government reported at least 4,000 leading French civil servants, scientists and senior executives were found to have been contacted by Chinese spies using LinkedIn.[11] Those targeted included 2,300 individuals in the public sector and 1,700 in French industry positions. The French Intelligence report indicated that those targeted included individuals from nearly every area of industry and government administration. They were approached online by Chinese spies who employed fake identities and identified themselves as headhunters for Chinese corporations, think-tank researchers or consultants for major companies. Typically, those targeted were then invited to all-expenses-paid trips to China for conferences or research symposia or offered paid work as consultants.

Hostile intelligence officers seek to identify, as potential information sources, individuals who are dealing with personal issues. A person's willingness to engage in espionage against an employer is often triggered by a personal crisis that has identifiable external pressures. In October 2012, Sub-Lieutenant Jeffery Paul Delisle pled guilty to spying for Russia from his position as a Royal Canadian Navy intelligence officer in a high-security facility in Halifax.[12] He had caught his wife cheating on him and was in financial distress. He reported these issues to his supervisor who dismissed it and failed to give him the appropriate organizational support. The Russian military intelligence service used Delisle for information from 2007 until 2012 when he was arrested. During that time, he was able to smuggle out vast amounts of highly classified information with a USB flash drive. The breach has been called one of the worst security breaches of Western intelligence services since the end of the Cold War. This case underscores the willingness of foreign intelligence services active in Canada to recruit Canadian government officials in positions of trust with access to information of interest to their nations.

2.3 Human-Oriented Tradecraft

Tradecraft describes "how" systems and access to people can be exploited to further criminal goals. The following tradecraft discussion is provided as context for the security controls section that follows. The objective is to sensitize readers to the ways systems and people can create security vulnerabilities.

[10] BBC News, "*German spy agency warns of Chinese LinkedIn espionage*" December 10, 2017
[11] Bloomberg, "*French Are Target of Widespread Spying by Chinese, Figaro Says*" October 23, 2018
[12] The Globe and Mail, "*Naval intelligence officer sold military secrets to Russia for $3,000 a month*" published October 10, 2012 , updated May 9, 2018

Extortion

- Extortion is the practice of obtaining something valuable through force or threat. As employees and executives lead increasingly connected lives online and with social media, there is an increased pool of information for threat actors to use against staff to provide sensitive information, access, and/or to influence decision-making.

Access control

- Perimeter access could be breached including both initial access to the facility and internal security controls between security zones. Proximity to networks has been used by criminals to gain surreptitious network access.

Visitor control

- In any professional environment, external visitors will be required to access the facility. Effective visitor control can increase the risk of unauthorized network access and provide clues in post incident analysis about involved parties.

Third-party contractors

- Contractors can present a series of security vulnerabilities. Contractors are typically present for a limited duration but are often given considerable access to sensitive information. Retaining control of information subsequent to their contracts can be a challenge particularly if the data is not maintained on internal systems.

Talent Spotting

- In seeking to find staff to exploit, threat actors first look to identify individuals who have access to information of relevance. These can be holders of specific positions or those who by way of their public persona provide evidence of that knowledge.

Elicitation

- Elicitation is a technique used to discreetly gather information. It is typically conversation with a specific purpose – to collect information that is not readily available and to do so without raising suspicion that facts are being sought. It is usually non-threatening, easy to disguise, deniable and effective.

2.4 Cyber-Oriented Tradecraft

Phishing

- Phishing is the fraudulent attempt to gain access to networks or data by disguising its purpose as a trustworthy entity in an electronic communication. Typically, the email will ask the individual to click on a link, which then installs malware on the computer, or asks the individual to provide login credentials. Phishing remains the single greatest vulnerability for most organizations as even a single successful phishing email can provide necessary network access.

Privilege Escalation

- Privilege escalation is the process of exploiting a design flaw or configuration oversight in an operating system, software application or other network

resource that enables the attacker to perform actions that they are not authorized to perform. Criminals who initially gain network access through phishing often then seek to escalate their network privileges to further exploit their initial foothold.

Inadvertent Data Loss

- Inadvertent data loss results from the accidental deletion of a file or program, misplacement of data from storage media, administrative errors or the inability to read unknown file formats. While the focus of this section has been on deliberate threats by criminals or spies, inadvertent errors by staff can also pose considerable danger.

Supply Chain Attack

- A supply chain attack is a cyber-attack that damages an organization by initially targeting less-secure elements of its network infrastructure. When reviewing security programs, it is essential to consider not simply those systems operated by the firm, but also the broader extended network that includes third-party providers.

Ransomware

- Ransomware is malicious code that blocks access to system files or data unless a ransom is paid. In many cases, the attacker may also threaten to publish the victim's data. Ransomware is extensive today with victims ranging from individual home computers to large government targets.

DDoS

- A Distributed Denial-of-Service (DDoS) attack is a cyber-attack where the attacker seeks to deny authorized users the ability to use networks or services by overwhelming the targeted machines with a flood of superfluous requests in order to overload the system and prevent legitimate requests from being serviced.

3. SECURITY POLICY & PROGRAM GOVERNANCE

3.1 LEADERSHIP AND FIDUCIARY RESPONSIBILITY

Under Canadian law, shareholders elect a board of directors (**board**) to oversee and manage the business and affairs of the corporation. Board members have a fiduciary duty to the corporation to demonstrate due care, act in good faith and maintain the skills necessary to exercise care, diligence and judgment over the business activities of the corporation. Specifically, regarding cybersecurity, board members must exercise oversight over the security program of the corporation.

Failure to demonstrate effective oversight over the firm's cybersecurity program can place the firm and its stakeholders in jeopardy and potentially expose board members to personal liability. In the event of a breach, the firm's board can anticipate being placed under scrutiny for their execution of the above duties.

Listed below are a number of steps that a board can implement to ensure that they are exercising their oversight responsibilities regarding cybersecurity and data breach matters:

- Ensure that board meetings regularly include discussions of the firm's cybersecurity readiness and data privacy issues.
- Maintain written records of board meetings including security tasks assigned and its status.
- Delegate control of cybersecurity measures and data protection activities to a board committee.
- Engage an audit of the corporation's cybersecurity systems and seek recommendations on prioritized improvements.
- Oversee management's cybersecurity program activities to include relevant policies, programs and alignment with applicable cybersecurity standards.
- Oversee management's efforts to establish a cyber incident response plan and supporting business continuity efforts to deal with cyber incidents and data breaches.
- Ensure the firm has access to cybersecurity program resources that can ensure the establishment and maintenance of a cybersecurity program and program governance.
- Ensure management's creation of an appropriately rigorous security culture that includes employee training and awareness.

3.2 KEY CYBERSECURITY PROGRAM ELEMENTS

Cybersecurity is not simply an information technology (IT) problem. Rather, it is a key element of any successful business activity. This issue should be proactively managed by the firm's leadership who has a responsibility to:

Maintain an Asset Inventory
Understand the firm's information assets and risks by ensuring that the firm's critical data and IT systems and assets are inventoried, and appropriate security is applied based upon its sensitivity. A privacy audit would gather details on the personal information that the firm gathers and its uses. A systems audit would provide comfort over the access and controls in place over critical systems.

Perform Risk Assessments
Data security law, regulations and standard contract obligations often use a reasonableness standard to judge protections applied. It is reasonable in the investment industry to conduct threat risk assessments (TRA) for a firm's critical systems. A TRA looks to define and prioritize critical systems and data, identify threats posed to the firm's information assets, identify potential vulnerabilities and the impact that breach would have upon the firm.

Develop and Maintain a Written Information Security Program
A written program will establish norms and behaviours expected of the firm's employees, contractors and key stakeholders. A well-documented program may assist a firm by:

- Prompting it to proactively and periodically assess risk and implement security measures to protect personal and other sensitive information
- Educating employees and other stakeholders about actions they need to take
- Communicating to staff and stakeholders the data security expectations of the firm
- Establishing the reasonable prudential steps that the firm expects its staff to take in order to protect personal and other sensitive information

Develop and Enforce Information Security Policy
This document lays the foundation for an effective information security program. Polices define behaviours expected of staff and contractors and articulate the steps expected of those with access to protect a firm's information assets. Absent an effective and accessible information security policy, it becomes difficult for a firm to shape behaviours that run counter to good practices. Topics in an information security policy include:

- Management expectations for both staff and contractors
- Data categories used to assign risk and protection levels
- Staff interaction with firm information assets, including access control and acceptable use
- How the firm protects and manages its information assets
- Cyber incident response
- Restrictions on engaging with external parties including vendors and clients
- Risk management and compliance programs

Training and Awareness

Employees and contractors are among the best defenses and greatest vulnerabilities for a firm's information security. Malicious and, much more often, accidental actions by staff are the single largest cause of data breaches. Building a culture of shared responsibility for security and providing ongoing focused training on how to avoid cyber risks are foundational to an effective security program. Employee training should:

- Explain the firm's security policy including the underlying rationale for the policy
- Communicate to staff their obligation to comply and their individual accountability for the information assets they access
- Provide employees with resources and expert help to avoid security risks
- Explain how to report security incidents
- Include more detailed training for those with access to more specialized systems and information that may pose a higher risk to the firm.

Manage Vendor Risks

Virtually all firms rely on third-party vendors for key elements of its business processes. There is increasing business pressure to automate processes and outsource key functions. Cyber criminals have used third-party service providers as attack vectors to reach their primary target. Given the known risks posed by third-party vendor relationships, there is an industry standard expectation that firms exercise diligent vendor oversight along with enforcement mechanisms in the event of non-performance, data breaches or significant security incidents.

When considering engaging any third-party service provider, firms should consider the following factors:

- Perform pre-engagement due diligence to determine if a potential vendor has existing security and privacy controls comparable to your own firm.
- Use standard contract terms that apply to all vendors that impose requirements to meet or exceed the firm's own practices. If your firm lacks the bargaining power to impose your standards upon a common vendor, request that the vendor identify where its existing standards differ from your firm's practices.
- Perform continuous oversight and enforcement through contractual audit privileges and reporting metrics that allow for an ongoing informed assessment of the risks posed to privacy and data security. Ensure that in cases where the business relationship ends, data is returned or reasonably destroyed with a certification of its destruction.

3.3 INSURANCE AGAINST CYBER-RELATED RISKS

The insurance market continues to evolve with respect to products relevant to cyber-related risks. While dealer members maintain Financial Institution Bonds (FIB) and commercial general liability insurance to cover losses related to business activities, most polices of this nature do not provide coverage for losses that can result from a data breach or other cyber incidents.

Cyber policies can vary and firms should be mindful of the types of risks they are exposed to and the type of coverage that would transfer that risk.

Depending on the policy, cyber insurance may cover both first-party costs stemming from a cyber breach or incident and provide third-party liability coverage.

First-party costs

First-party costs are a firm's own costs for investigating and mitigating the effects of a breach or incident and complying with relevant privacy laws and regulations. These costs are often incurred regardless of whether a third party such as a client or employee sues the firm for a breach of privacy or security. These include:

- Legal costs
- Breach notification costs
- Forensic investigation costs
- Credit/identity monitoring costs
- Call center costs
- Public relations costs
- Business interruption costs

Third-party claims

Cyber insurance also provides third-party liability coverage and will cover:

- defense costs
- settlements awarded to a third party
- insurable fine/fines imposed by a regulator following an investigation or regulatory proceeding

In addition to protecting against potential financial losses, cyber insurance can significantly assist a firm's level of responsiveness to incidents. Insurance companies provide policyholders with coaching and resources in the event that a potential incident is believed to be taking place. A "breach coach," who in most instances is a lawyer, acts as a trusted third-party advisor throughout the course of the incident. The breach coach also serves as a conduit between the firm and other third-party service providers like forensics investigators to protect the firm by claiming legal privilege over new and sensitive information.

Other insurance coverage

While these are expenses typical of a data breach incident, cyber insurance does not cover the full range of other potential losses that a firm may consider cyber-related. Take, for instance, the case where a computer system was breached to collect information that resulted in fraudulent instructions being sent to authorized employees to transfer funds out of the firm. While the penetration of the computer system to collect information and send the fraudulent instructions may be covered, the actual loss from the transfer of funds is not.[13]

[13] There may be limited coverage for such losses under a FIB policy depending on the extensions.

In addition to cyber coverage, firms should also consider whether it needs Directors' and Officers' (**D&O**) Liability coverage. In the event of loss arising from a cybersecurity incident, board members and executives may be exposed to individual liability. For example, stakeholders such as investors and clients may file lawsuits alleging that the board members and executives breached their fiduciary duty by not ensuring that cyber-related risks were adequately managed. A D&O policy may help cover the costs associated with such lawsuits.

Insurance carriers have different terms and limitations for their policies. Depending on the allegation and losses involved, it could be covered under different policies. Firms should carefully review the likely loss scenarios with its insurance brokers and the types of coverage it needs to ensure enough protection.

3.4 KEY LEGAL CONSIDERATIONS

A firm's leadership needs to ensure that they are both informed of and in compliance with applicable laws and regulatory schemes related to cybersecurity and the management of sensitive data. For example, IIROC dealer members are obligated to report cybersecurity incidents to IIROC pursuant to IIROC Rule 3703.[14] In Canada, other relevant laws include the following:

- the *Personal Information Protection and Electronic Documents Act* (PIPEDA), as amended by the *Digital Privacy Act*, which protects personal information and applies to private-sector organizations across Canada that collect, use or disclose personal information in the course of a commercial activity,
- provincial private-section privacy laws, which may apply to dealer members operating in those provinces instead of PIPEDA if those provincial privacy laws have been deemed substantially similar to PIPEDA,[15]
- financial sector-specific laws and regulations, which depending on the dealer member's business activities may include the *Bank Act*, the *Insurance Companies Act* and guidelines issued by the Office of the Superintendent of Financial Institutions,
- other laws and regulations designed to protect at-risk data, assets, business interests, trade secrets and business contracts

Firms that operate in jurisdictions outside of Canada may be subject to applicable laws and regulations in those jurisdictions related to its protection of critical data and reporting of material events that could affect that data. In Canada, other than provinces where the provincial privacy laws govern, PIPEDA sets out:

- umbrella protections for personal information

[14] The requirements related to reporting under the IIROC Rule are discussed in IIROC Notice 19-0194 with additional guidance in the form of frequently asked questions in IIROC Notice 19-0195.

[15] Three provinces have enacted private sector privacy laws which have been deemed by the Government of Canada to be "substantially similar" to PIPEDA – British Columbia, Alberts and Quebec.

- steps that firms should be taking to protect the information from inadvertent disclosure, and
- requirements for timely reporting of possible breaches.

PIPEDA is enforced by the Office of the Privacy Commissioner (OPC). PIPEDA requires firms to implement procedures and identify individuals responsible for responding to data breaches and other incidents that involve personal information. The OPC could view the failure by a firm to develop, implement, and maintain a cyber incident response plan as a failure to meet PIPEDA's reasonableness standard for security measures.

3.5 POLICIES & PROCEDURES

The security policy articulates the firm's objectives. Rather than guidance, policy establishes mandatory conduct.

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.
Creating a security policy requires management to document what controls are necessary to manage the risks they are willing to accept. A firm's leadership should be educated on security risks in order to develop an informed cybersecurity strategy.

Key elements of an information security policy should include:

- All information, systems, facilities, programs, data networks, and all users of technology in the organization (both internal and external), without exception
- Firmly defined information classification methodology along with content-specific definitions for those categories, 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)[16]

The implementation of a policy is not a single event, but rather an iterative process revisited as business models, relationships, and technology changes. Without such policies & procedures, there can be no effective governance of the cybersecurity program.

[16] "How to write an information security policy," CSO Online

4. OPERATING TIER FRAMEWORK

Firm leaders need a means to assess the preparedness of their firm relative to peers and the investment industry as a whole.

4.1 THE NIST CYBERSECURITY FRAMEWORK

Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing a nation's security, economy, and public safety and health at risk. The National Institute of Standards and Technology (NIST) was tasked with facilitating and supporting the development of cybersecurity risk frameworks to strengthen the resilience of these sectors. The NIST Cybersecurity Framework (**Framework**) focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risks as part of the organization's risk management processes.

The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improve its security and resilience.

It is applicable to organizations relying on technology, whether its cybersecurity focus is primarily on IT, industrial control systems, cyber-physical systems, or connected devices more generally, including the Internet of Things or IoT.[17] The Framework can assist organizations in addressing cybersecurity as it affects the privacy of clients, employees, and other parties.

The Framework consists of three parts:

- Framework Core:
  The Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure.

- Profiles:
  Profiles will help an organization align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. Elements of the Core provide detailed guidance for developing individual organizational profiles.

- Implementation Tiers (**Tier**):
  The Tiers are a mechanism for organizations to view and understand the characteristics of its approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

[17] The IoT can be described as an extension of the internet and other network connections to different sensors and devices — or "things" — affording even simple objects, such as lightbulbs, locks, and vents, a higher degree of computing and analytical capabilities.

The CSF provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today.

4.2 WHY RELY ON NIST?

There are a range of cyber control frameworks for dealer members to choose from. In addition to NIST, ISO 27001 and COBIT are also well-established, control-based frameworks. These standards can be easily mapped to the NIST CSF.

NIST's CSF was chosen as the guiding framework for this project because of its common language and systematic methodology for managing cybersecurity risk. The NIST CSF is accessible by executives and IT professionals alike, enabling end-to-end risk management communications across an organization. The list of organizations that rely on NIST is wide-ranging and includes hospitals, financial institutions, universities and colleges, as well as organizations supporting critical infrastructure. In addition to this publication, there is substantial literature available on the Internet if dealer members wish to dig deeper into the principles and individual security controls.

4.3 PHASED APPROACH

Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the NIST CSF will vary. This type of flexibility is important given the fluidity of the cyber threat landscape and the often-limited means devoted to cybersecurity management.

Dealer members should use a phased approach when implementing applicable safeguards based on an evaluation of their cybersecurity capability (i.e., NIST Tier 1, 2, 3, or 4), followed by a tailored assessment of applicable safeguards within the subcategories of each NIST Function (i.e., Identify – "ID", Protect – "PR", Detect – "DE", Respond – "RS", and Recover – "RC") based on the assessed capability.

In other words, the assessment can be used to prioritize expenditures to maximize the impact of each dollar spent based on a dealer member's capability to support the implementation of applicable safeguards.

It is important to note that Tiers do not represent maturity levels. Tiers are meant to support organizational decision-making to manage cybersecurity risk, as well as identify which dimensions of the organization are higher priority and could receive additional resources. Progression to higher Tiers is encouraged when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk.

4.4 APPRECIATING COST / DIFFICULTY / TIME FRAME

Organizations should identify and prioritize feasible and cost-effective improvements in the short-, medium- and long- term after considering its business requirements and material risks and making reasonable and informed cybersecurity decisions using its assessments. This will include an approximate evaluation of cost, difficulty and time frame for each specific selection of safeguards based on its NIST Tier.

4.5 PROFILE DESCRIPTIONS

A **Tier 1** organization is defined by the following:

- Organizational cybersecurity risk management practices are not formalized.
- Risk is managed in an ad hoc and sometimes reactive manner.
- Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business / mission requirements.
- There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established
- The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience of information gained from outside sources

- The organization may not have processes that enable cybersecurity information to be shared within the organization.
- An organization may not have the processes in place to participate in coordination or collaboration with other entities.

A **Tier 2** organization is defined by the following:

- Risk management practices are approved by management but may not be established as organizational-wide policy.
- Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established.
- Cybersecurity information is shared within the organization on an informal basis.
- Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization.
- Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.
- Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both.
- The organization collaborates with and receives some information from other entities and generates some of its own information but may not share information with others.
- The organization is aware of the cyber supply chain risks associated with the products and services it provides and uses but does not act consistently or formally upon those risks.

A **Tier 3** organization is defined by the following:

- The organization's risk management practices are formally approved and expressed as policy.
- Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- There is an organization-wide approach to manage cybersecurity risk.
- Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed.
- Consistent methods are in place to respond effectively to changes in risk.
- Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.
- The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.

A **Tier 4** organization is defined by the following:

- The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.
- Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.
- There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.
- Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on systems and networks.
- The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

5. OPERATIONAL PROGRAM IMPLEMENTATION GUIDANCE

Section 3 described the obligations firms face when dealing with cybersecurity. Section 4 introduced the concept of security tiers and the idea that structured program enhancements can collectively move a firm from one Tier upwards to the next. This section speaks to the firm-level steps necessary to implement an effective security program. The subsequent section addresses recommended best practices that are components of an effective security program.

Operational governance is about decision-making and communications, it and ensures that clear responsibilities for communications and accountability of processes and assets are assigned. Tailored policies, standards, controls and measures enabling staff and suppliers to understand and execute on their roles and responsibilities are developed to articulate the types of expected behaviours and what constitutes unacceptable behavior. Finally, a deliberate program review activity and compliance measurements provide feedback on the effectiveness of accountability, communications policies, controls and the governance program itself.

At its core, operational governance ensures the security plan to protect a firm's most valuable assets is deployed and sustained. The process to identify the key elements of this plan are described in the following graphic.

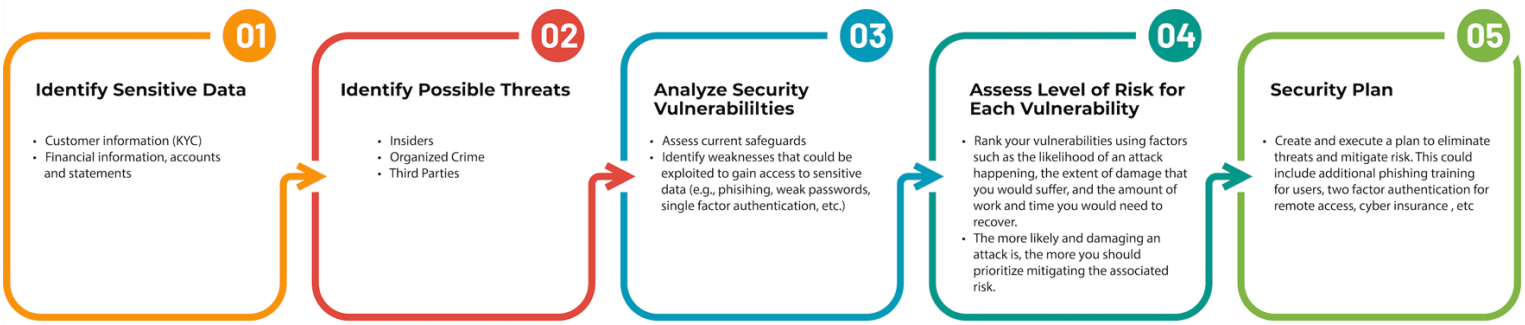


Figure 1: Operational Security Plan

Building a plan to secure your firm's assets requires a focus on the following **three fundamental goals**:[18]

- **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.

[18] GetCyberSafe Guide for Small and Medium Businesses

- **Availability**
  Maintain the availability of systems, services, and information when required by the business or its clients.

The plan and its focus on the key goals will enable a firm to deploy safeguards that accomplish key Cybersecurity Framework functions outlined below:[19]

1. Protect assets with the appropriate safeguards.
2. Detect intrusions, breaches, and unauthorized access.
3. Respond to a potential cybersecurity event.
4. Recover from a cybersecurity event by restoring normal operations and services.

5.1 DUE DILIGENCE & DUTY OF CARE

The creation and execution of a security plan will assist a firm in demonstrating due diligence to protect valuable assets and satisfy legal requirements as inherent in privacy laws.

Cyber operational governance focuses decision-making and communications on ensuring that the protections and controls being depended on (the security plan) are operating as expected on a day-to-day basis.

Good cyber governance crystallizes itself into tangible artifacts that can be reviewed and relied on including:

- **Policies**: that document management's intent to provide guidelines by which decisions can be made. A firm's incident response policy and plan would be an example, security awareness would be another.
- **Effectiveness measures**: defining measurements as a basis for understanding and controlling cyber processes. An example would be unpatched vulnerabilities.
- **Compliance**: specifying the documentation required to support the auditability of processes and decisions.

As capabilities mature, efforts and investments will become increasingly focused on cybersecurity hygiene and demonstrating duty of care. Operational governance will ensure a standard of reasonable care has been taken in protecting a firm's assets and information. The same responsibilities that leadership demonstrates for other aspects of the business are also applicable for cybersecurity, such as ensuring auditability of processes and outcomes.

Key documentation includes inventories of assets and services, third-party reviews, risk assessments and risk management policies, among others. These artifacts once developed and formalized should be reviewed and updated on a regular basis and ensure that acceptable levels of duty of care are demonstrated on a consistent and regular basis.

[19] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. 2014

5.2 PREPAREDNESS

A key aspect of due diligence is cyber preparedness and resiliency. A firm's investments in its cyber and security plan will reduce and mitigate the likelihood of a cyber incident and its impact but it cannot eliminate the probability of one taking place. Firms need to plan, develop and test capabilities to respond and recover from significant, and likely, cyber incidents and/or business interruptions.

How well a firm is able to respond to and recover from a bad day will be directly related to its level of preparedness. Preparedness of cyber and IT capabilities can be a key aspect of responding to an incident. Equally as important, and quite often more important, are communications, legal and leadership capabilities especially when responding to incidents that may involve the potential breach of personal and financial information.

Incident Response
An essential component of preparedness is a well-documented and understood Incident Response Plan. Components of this plan and how to optimize its utilization are described in section 6.15.

Backups
Copies of key data and information are one of the main components of an adequate resiliency and recovery plan. Backups of data can ensure business operations continue with minimal interruption depending on the circumstances. Backups can be especially useful in recovering from ransomware and hard-drive focused virus attacks. It is essential that backups are tested on a regular basis and that they are stored with appropriate protections and are easily accessible to ensure availability if required. Storage of at least one back-up off-site is also recommended.

Cyber Tabletop Exercises
A cyber tabletop exercise is an incident / disaster preparedness activity that takes participants through the process of dealing with a simulated disaster scenario. A tabletop is discussion-based and not only helps participants familiarize themselves with the response process, but also enables leadership to gauge the effectiveness of the firm's incident / emergency response capabilities. Key staff present during the exercise have the opportunity to not only become more comfortable with their own roles in disaster scenarios, but to see how the entire response will play out across the organization.

Leveraging an accelerated timeline, tabletop exercises walk through every aspect of the hypothetical scenario, from beginning to post-disaster efforts. They evaluate:

- internal resources,
- any external resources that may be called upon for assistance including, legal, breach coaches and / or cyber insurance companies, and
- identify what communications will be transmitted, to what audiences and how.

Exercise scenarios should test progress within the firm on cyber preparedness and plans developed to deal with likely scenarios. A critical component in assessing the potential impacts of an incident is determining if regulators need to be notified. This is particularly important in the case of potential breaches of personal and/or financial information.

The outcomes of tabletops exercise should inform future incident response and disaster recovery planning and determine new guidelines and practices the organization may need to implement. The exercise may identify gaps in knowledge from personnel, or security flaws that must be corrected. Typically exercises reinforce that though IT and security response and recovery capabilities are important, communications and decisions from the business, especially during the incident itself, are vital to how well an incident is responded to.

Tabletop exercises should be conducted regularly, i.e. three to four times annually. Scenarios can be derived by using recent events in the industry as examples. An exercise can last from 45 minutes to 2 hours depending on the complexity of the incident and number of participants.

Following the exercise, participants and facilitators may compile an after-action report, detailing any key findings or questions highlighted during the exercise.

Business Continuity Planning

A business continuity plan (BCP) is a document that describes how a business will continue business operations during an unplanned service disruption. This plan is more comprehensive than a disaster recovery plan which focuses strictly on restoring IT capabilities. A BCP focuses on outlining the actions needed to sustain business processes. It will contain contingencies, and in some cases, workarounds, processes, assets, human resources and business partners. By definition it covers every aspect of the business that might be affected. Key interruptions to be planned for firms would include:

- loss of offices for an extended period,
- the inability to access offices for more than a week,
- pandemic and/or public health crisis,
- the loss of key personnel,
- cyber incidents.

Plans may provide detailed strategies on how business operations can be maintained for both short-term and long-term outages. Plans typically contain a checklist that includes supplies and equipment, alternative site locations, remote working protocols. Plans also identify plan administrators and include contact information for key personnel, backup site providers, and emergency responders.

It is important to note that IIROC Rule 4710 through to 4714 requires all dealer member firms to maintain an updated BCP and to test it annually.

5.3 ASSESSING THREATS AND VULNERABILITIES [20]

Cyber criminals continue to take advantage of basic security vulnerabilities in computer systems. These include unpatched 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. 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 it onto production systems.
- ensure computer software/applications are updated with security patches regularly.

5.4 COMPREHENSIVE PROGRAM DEVELOPMENT

In developing the necessary policy framework and program elements, firms are encouraged to use systems thinking rather than considering point solutions or ad hoc security controls. Due diligence is demonstrated when the program formation addresses likely threats and vulnerabilities developed through a systematic approach. While external vendors can assist in describing the threat environment, it takes those within the firm with knowledge of the business activities and information holdings to shape the general threat environment to the specific firm environment.

Beyond the adoption of security controls, effective preparedness includes planning for and testing against likely threat scenarios to ensure that the firm's plans are sufficient to address potential business interruptions.

[20] The following provides an example of how recommendations in the best practices document will be cross-referenced with controls in the NIST Cybersecurity framework.

6. BEST PRACTICE RECOMMENDATIONS

Cybersecurity is a shared responsibility – people, processes, tools, protections and technologies work together to protect an organization's assets. The following safeguards should be considered when designing a cybersecurity plan. Implementation of the following safeguards that align with a firm's risk appetite will enable the design and deployment of a plan that best meets an organization's unique business needs and requirements.

The plan can also be used to demonstrate management's duty of care and provide comfort to third parties and regulators as required.

6.1 PERSONNEL SCREENING AND THE INSIDER THREAT

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

Data published by McKinsey & Company in 2018 indicated that an insider threat was present in 50 percent of cyber breaches. Of those almost 40 percent were malicious insiders with roughly 44 percent the result of either negligence or innocent co-opting by an external party of an employee. The implication for dealer members is that cyber security needs also to focus on the human element, particularly who is recruited and how their behavior changes while employed at the firm.[21]

Some of the risks posed from insider threats in the financial sector are:[22]

- Undesired disclosure of confidential client and account data
- Fraud & monetary loss
- Loss of intellectual property
- Disruption to critical infrastructure
- Regulatory repercussions
- Destabilization, disruption, and destruction of financial institutions' cyber-related information, applications, controls and protections
- Embarrassment, and public relations/reputational risk issues

According to the Carnegie Mellon CERT Insider Threat Center,[23] employees who pose the greatest insider threat risk are:

- 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,

[21] McKinsey & Company: The Human Element of Cyber Risk, 2018
[22] Bunn, C. (2013). A Focus on Insider Threats in Banking & Financial Institutions
[23] Ibid, 1

- employees moving to a competitor or starting a business who, for example, steal client lists or business plans to give themselves a competitive advantage, and
- employees who believe they own the intellectual property that they helped develop and take the intellectual property with them when they leave the organization.

The following are some recommendations to help manage the insider threat:[24]

- **Build a Multidisciplinary Team**
  Where feasible, organizations should have a dedicated team made up of Human Resources, Security, and Legal professionals to create policies, drive training, and monitor at-risk employees.
- **Understand Organizational Issues**
  Organizations should assess whether it is at greater risk due to certain inherent factors. For example, remote offices, suppliers, or subcontractors and differences in cultures, politics, or language could lead to potential conflicts.
- **Examine Pre-Employment Screening Processes**
  The information collected during this process 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**
  It is important to recognize that diligence cannot be limited to the hiring process. Staff members often will face external stressors that are difficult for them to deal with and that can present a challenge to their workplace performance.
- **Anticipate and manage negative workplace issues**
  Managers remaining vigilant to changes in workplace behavior and being willing to support the at-risk employee has proven to be an effective strategy to treat an emerging internal threat.
- **Enforce separation of duties and least privilege**
  Segregation of key duties and access restrictions can also assist in limiting the degree of opportunity that an insider has to cause damage. Periodic review of permissions and accesses to align with a policy of least privilege to achieve business requirements supports the overall goal of limiting the potential risk of an insider.

Dealer members can help to mitigate the damage that may arise from insider threats by recognizing the potential harm posed by current or departing employees.

[24] 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

Case Study (2018): Unauthorized Police Database Searches [25]
A temporary civilian employee, Erin Maranan had access to information classified by police as "highly restricted." Maranan conducted dozens of illegal police database searches during a 16-month spree between 2014 and 2015. Her queries gave her access to a catalogue of individuals within the police databases, including photos, physical descriptions, addresses, known associates and more. She could also see any links between those individuals and criminal investigations. Some of Maranan's searches were conducted to collect information on rival members of criminal organizations, while others were so-called "heat checks" — queries done on a gang's own members to see what police had on them. Although three of the people Maranan searched were later killed, the Crown did not establish Maranan knew how the information would be used, and it was not proved that the disclosure of information compromised ongoing investigations or resulted in harm to any particular person.

Maranan was sentenced to a year in jail and three years of probation after she pleaded guilty to breach of trust. Maranan's phone records showed she had a personal relationship with an alleged gang member whose name she queried 17 times. The information Maranan had access to was so highly restricted that even those investigating her did not have immediate clearance to see it.

6.2 PHYSICAL AND ENVIRONMENTAL SECURITY

The physical security of assets is a cybersecurity first line of defense. The effect of a stolen laptop or smartphone can be very disruptive to an organization. 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
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 interruption in energy supply that negatively impacts an information system.

The following are recommendations for physical and environmental security:

- The "clean desktop" principle should be followed, and employees should put away sensitive items before leaving their work area. A clean desk will keep sensitive

[25] The Toronto Star, "Civilian Toronto police employee jailed after conducting illegal database searches," June 2018

information out of the hands of personnel who do not have a legitimate reason for accessing this information including cleaning staff and security guards.
- An employee's access to a work area should be allowed only if they have a legitimate business requirement.
- Visitor management procedures should be established which ensure that guests are signed in and out and escorted at all times while in the office.
- Access to a computer's contents should be restricted by locking the screen when the user is away.
- Information system should be safeguarded against fluctuations in electricity or electrical power outages by ensuring that it is plugged into a UPS.
- Backups should be performed on a regular basis to safeguard information against a catastrophic event.

6.3 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. Financial institutions remain the constant target of cyber criminals who want to steal its intellectual property and confidential information because of the increasing use of online tools to communicate with stakeholders. PwC's 2018 *Global State of Information Security® Survey* suggests that businesses that have a security awareness program report significantly lower average financial losses from cybersecurity incidents.[26] It also points out that an effective security awareness program requires adequate funding.

Many organizations invest in technical controls to protect its computer systems and data. However, employees and insiders who are not vigilant greatly increase cybersecurity risks to the organization by opening suspicious emails or not protecting sensitive information stored on, or transmitted from, their computers. The *2019 Cyberthreat Defense Report Survey* reports that low security awareness among employees remains the greatest inhibitor to defending against cyberthreats.[27]

The following are recommendations for cybersecurity awareness and training:
- Implement policies covering the acceptable and 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 annually. 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 and

[26] PwC, 2018 Global State of Information Security Survey
[27] 2019 Cyber Threat Defense Report, CyberEdge Group LLC.

    - Appropriate sanctions will be taken against personnel who fail to comply with the cybersecurity awareness principles and security policies.
- Instruct employees
    - Not to open suspicious emails or click on suspicious links, regardless of the source.to validate non-standard and/or suspicious "requests" from coworkers or senior management, especially if it involves transfers of monies, purchases of gift cards, access to restricted information, etc.
    - Not to connect devices to the network, unless they have a legitimate business reason to do so, or are using pre-approved devices
    - To follow good password practices
    - On the dangers and safe use of external media (USB sticks and CDs)
- Continually educate and share mandated knowledge using videos or webinars.

Case Study (2017): Canadian Charged as International Hacker-for-Hire [28]
Russian intelligence officers ("FSB") directed criminal hackers, Canadian Karim Baratov, and others, to gain unauthorized access to the computers of companies providing webmail and internet-related services (Yahoo, Inc., Google, Inc. and others), to maintain unauthorized access to those computers, and to steal information from those computers.

Baratov's intended victims, included Russian government officials, such as senior political leaders and their counselors, a law enforcement official, and a prominent Kazakh banker, among others. Baratov and the co-conspirators undertook this conduct for the purpose of commercial advantage and private financial gain. Baratov would employ "spearphishing" messages, designed to trick unwitting recipients into providing access to their computers and accounts.

6.5 NETWORK SECURITY

An organization's constant connectivity to the Internet exposes it to a hostile environment of rapidly evolving threats – external and internal.

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: [29]

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

[28] United States of America v Baratov, 2017 ONSC 2212 (CanLII)
[29] Communications Security Establishment Canada. Baseline Security Requirements for Network Security Zones in the Government of Canada. 2007: 5

Cyber criminals search 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.

Adopting a defense-in-depth approach,[30] 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 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 multi-factor authentication[31] 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 required 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.

6.6 WIRELESS NETWORK SECURITY

Wireless connectivity has the advantage of increased mobility and productivity, but it also introduces a number of critical security risks and challenges. Wireless networks have made it exponentially easier for cyber criminals to penetrate organizations without physically stepping foot inside a building. Wireless signals typically broadcast outside a building's physical infrastructure and bypass traditional wired security perimeter safeguards such as firewalls and Intrusion Protection Systems.

Cyber criminals can gain unrestricted access to an organization's internal network by installing hidden, unauthorized wireless access points on the network. Disgruntled employees or other individuals with malicious intent disguising themselves as authorized contractors would typically be responsible for planting these devices.

The following are recommendations for wireless network security:

[30] A multi-layered defense, e.g. deploying two firewalls, setting up antivirus protections on servers as well as end user devices, etc.

[31] Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). NIST Computer Security Resource Center

- 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.
- disable wireless access on computer systems that do not have a legitimate business requirement via the computer's hardware setup which is available while the computer is booting and require a password for anyone attempting to enter the computer's hardware configuration.
- ensure that all traffic that flows across the wireless network is protected by advanced encryption, e.g. Advanced Encryption Standard (AES), and Wi-Fi access utilizes advanced authentication, e.g. Protected Access 2 (WPA2). [32]
- 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.
- disable wireless peripheral access of devices (such as Bluetooth), unless there is a legitimate business requirement.

6.7 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:[33]

- implement a remote access policy and train staff to adhere to it
- provide remote access only using secure VPN technologies
- configure the secure VPN so that split tunneling is not permitted
- monitor and log all remote access sessions
- require multi-factor authentication for all remote access sessions

Case Study (2019): Nation-State Actors Breached Two US Municipalities [34]
The FBI released a security alert to private industry partners in early 2020 about nation-state hackers breaching the networks of two US municipalities in 2019.

[32] For current recommendations for security protocols can be found at: https://www.us-cert.gov/ncas/tips/ST18-247
[33] Public Safety Canada. Industrial Control System (ICS) Cybersecurity: Recommended Best Practices. 2012
[34] ZDNet, "FBI: Nation-state actors have breached two US municipalities," January 16, 2020

The hacks took place after attackers used the CVE-2019-0604 vulnerability in Microsoft SharePoint servers. The FBI says that once attackers got a foothold on these networks, "malicious activities included exfiltration of user information, escalation of administrative privileges, and the dropping of webshells for remote/backdoor persistent access…Due to the sophistication of the compromise and Tactics, Techniques, and Procedures (TTPs) utilized, the FBI believes unidentified nation-state actors are involved in the compromise," the agency said in its security alert.

The attacks on US municipalities are not isolated cases, nor are they the first attacks where the CVE-2019-0604 SharePoint vulnerability has been used. Throughout 2019, this particular SharePoint vulnerability was one of the most exploited security flaws, by both financially motivated cybercriminals, but also nation-state-sponsored cyber-espionage groups.

The first attacks detected in the wild were discovered by Canadian Centre for Cyber Security in late April, when the agency sent out a security alert on the matter. The Saudi National Cyber Security Center (NCSC) confirmed a similar wave of attacks a week later, in early May.

6.8 ENDPOINT SECURITY

Employees accessing organization resources, the office or remotely should do so only using approved company-owned equipment.[35] In addition to the guidance outlined in section 6.9 *Information System Protection*, all users should follow the advice outlined below.[36]

- ensure that all updates run automatically so that the anti-malware solution is up to date and 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

6.9 INFORMATION SYSTEM PROECTION

[35] See section 6.10 *Bring Your Own Device (BYOD)* for a discussion of appropriate security measures if this policy has been adopted.
[36] Government of Canada. GetCyberSafe Guide for Small and Medium Businesses

The computer systems must be protected from attempts to hack it including computers that are used to access company resources remotely. 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.
- provide remote users access to company resources using a secure VPN and multi-factor authentication.

Several vendors sell all-in-one endpoint security solutions for personal, small business, and enterprise computer systems at affordable prices.

6.10 BRING YOUR OWN DEVICE

The *Bring Your Own Device* (BYOD) concept is a growing trend in business. It refers to the policy that allows employees to use personally-owned devices – including laptops, smartphones, and tablets –to access the company's applications and data. While there are real business benefits from BYOD in the workplace, it does carry significant risks. For example:

- losing a personal device that contains business information.
- installing malicious applications
- disclosing business information to unauthorized individuals, for example, if family members or friends also use the device
- possibly violating data privacy laws and regulations related to the employee, If improperly implemented

A firm should conduct a risk assessment and seek legal advice before deciding whether to allow BYOD and how to manage the associated risks. BYOD in the workplace has resulted in significant data breaches[37] so it is important that firms institute a comprehensive BYOD policy. At a minimum, the BYOD policy should cover: [38]

- 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)

[37] Trend Micro. Mobile Consumerization Trends & Perceptions: IT Executive and CEO Survey. 2012
[38] Fraud Advisory Panel. Bring your own device (BYOD) policies. 2014

- 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. There are 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).

6.11 MOBILE DEVICE MANAGEMENT

Mobile device management (MDM) is software that secures and enforces policies on smartphones, tablets and other endpoints. The goal of MDM is to optimize the functionality and security of mobile devices within an organization while simultaneously protecting the corporate network. It is an especially important protection for smart phones and tablets accessing e-mail and file-based cloud services.

Key services can provide:

- Device inventory and tracking;
- Application distribution, how mobile applications are provided to users and how they subscribe to their use; and
- Remote wipe, in the instance that a device is lost, stolen or as part of the off-boarding process.

Key policies to be configured for the devices include:

- Password enforcement: ensuring password rules are followed;
- Application whitelisting and blacklisting: explicitly controlling which applications can be used and should not be used;
- Data encryption enforcement: ensuring rules for encrypting information are adhered to;
- Dual authentication; ensuring multifactor authentication is enforced for accessing key services and information.

6.12 BACKUP AND RECOVERY

A backup plan is essential for any organization. Backups ensure that an organization can recover quickly by restoring lost or damaged files. Timely backups can be especially critical when recovering from malware attacks. For small and medium-sized businesses, 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. Copies of backups should be rotated with a copy stored outside of the office.

- **Cloud**
  Backup services can save files to cloud-based storage. Firms should review which jurisdictions data could be coming to ensure compliance with privacy regulations. Also, all backups should be encrypted.

6.13 USER ACCOUNT MANAGEMENT AND ACCESS CONTROL

Access controls determine how employees read email, access 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
- 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 it is changed every 90 days, and that the previous 15 passwords are not allowed to be used as a new password.
- require multi-factor authentication for privileged accounts or accounts that have access to sensitive data or computer systems. Multi-factor authentication can be achieved using smart cards with certificates, One Time Password (OTP) tokens, or biometrics.

6.14 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 and are typically more vulnerable to exploitation.

7. 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 accessibility of an organization's information assets.

Cyber incident management helps mitigate the risks associated with internal and external threats, and helps an organization ensure regulatory compliance where required. An organization must be prepared to handle incidents that may originate from a variety of sources.

7.1 KEY TERMS

The framework and definitions used in this document align with the Government of Canada Cyber Security Event Management Plan (released in 2018) and the U.S. National Institute of Standards and Technology Computer Security Incident Handling Guide (Special Publication 800-61, Revision 2, released in 2012).

- **Compromise**: This as a potential or actual cyber security breach of the confidentiality, integrity, or availability (CIA) of the enterprise's digital information or information technology (IT) assets.
- **Confidentiality**: Prevention of information from disclosure to unauthorized individuals.
- **Integrity**: Assurance for the accuracy, completeness, and authenticity of information and services.
- **Availability**: Ability to supply the operations, programs, and services of the enterprise.
- **Cyber Event**: Any event that is *potentially detrimental* to the Confidentiality, Integrity and/or Availability (CIA) of information or information technology assets, including cyber incidents, that are the products of threats and vulnerabilities.
- **Cyber Incident**: Any event(s) that have caused an *actual compromise* to the CIA of assets that are the products of threats and vulnerabilities.
- **Threat**: Any security event that is caused by a deliberate, accidental, or natural hazard threat agent that may potential compromise the enterprise's assets.
- **Vulnerability**: A weakness in the organization's controls to identify, protect, detect, respond, and recovery against a threat that increases the potential for, or impact of, a compromise.

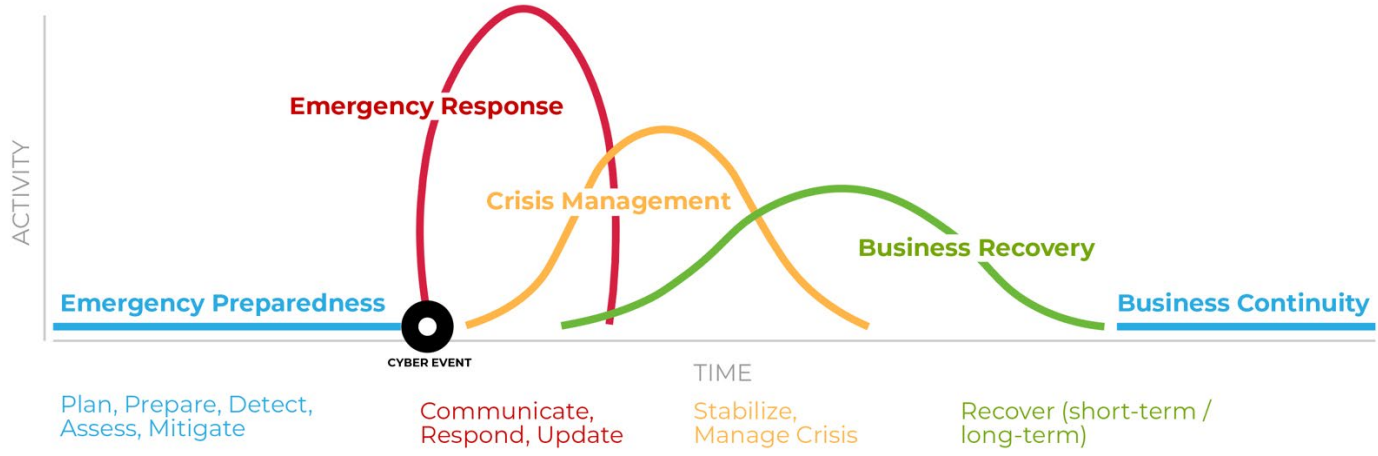
7.2 INCIDENT RESPONSE MODEL

The Cyber Incident Response Plan (CIRP) can be based on the proven Incident Command

System (ICS)[39] model. ICS establishes common terminology that allows diverse incident response and support organizations to work together across a wide variety of incident response functions and hazard scenarios.

The diagram below reflects the phases of incident management from the preparation phase through to the recovery phase. The singular focus at the outset of any cyber security event where a compromise of Confidentiality, Integrity or Availability (CIA) of the enterprise's information or IT systems has already occurred is depicted by the red curve, indicating that a tactical Cyber Response will occur before initiating the CIRP. In all cases, the Executive Emergency Oversight Team (EEOT) has authority to act within their scope of responsibilities to ensure the preservation of the firm's information and IT assets.

The CIRP, depicted by the yellow curve, shall be activated as soon as the primary objectives of the Cyber Response Plan have been met. The CIRP enables effective coordination of ongoing response and recovery tasks and communication to relevant stakeholders.



7.3 MODULAR ORGANIZATION

The CIRP organizational structure is scalable to the nature, scope and complexity of the events and incidents to be managed. Responsibility for the establishment and expansion of the CIRP modular organization ultimately rests with **Incident Commander**.

7.4 MANAGEMENT BY OBJECTIVES

Management by objectives is communicated throughout the entire CIRP organization and includes:

- Establishing incident response objectives
- Developing strategies based on incident response objectives

[39] The Incident Command System is a standard on site command and control system used to manage emergency incidents and planned events.

- Developing and issuing assignments, plans, procedures, and protocols
- Establishing specific, measurable tactics or tasks for various incident response functional activities, and directing efforts to accomplish them, in support of the defined strategies
- Documenting results to measure performance and facilitate corrective actions
- Establishing a response and reporting cadence by assigning operational periods for internal reporting

7.5 CYBER INCIDENT ACTION PLANNING

Centralized, coordinated Cyber Incident action planning should guide all response activities. The Cyber Incident Action Plan (CIAP) provides a concise, coherent means of capturing and communicating the overall incident response priorities, objectives, strategies, and tactics in the context of both operational and support activities.

Every cyber incident must have an action plan. However, not all cyber events require written plans. The need for written plans is the decision of the Incident Commander.

Most initial response operations are not captured with a formal CIAP. However, if an event is likely to extend beyond one operational period, become more complex, or involve external stakeholders, preparing a written CIAP will become increasingly important to maintain effective, efficient, and safe response operations. The CIAP further serves as a documented chronology of decisions and actions taken on the information available at the time.

7.6 MANAGEABLE SPAN OF CONTROL

Span of control is key to effective and efficient cyber security incident response. Supervisors must be able to adequately supervise and control their subordinates and communicate with and manage all resources under their supervision. The type of cyber incident, nature of the task, hazards and safety factors, and distances between personnel and resources all influence span-of-control considerations.

7.7 INCIDENT FACILITIES AND LOCATIONS

The Incident Commander will direct the identification and location of facilities based on the requirements of the situation. Typically, designated facilities include Cyber Incident Command Posts, Executive War Room, Rest Facilities, and others as required.

7.8 COMPREHENSIVE RESOURCE MANAGEMENT

Maintaining an accurate and up-to-date picture of resource utilization is a critical component of cyber incident response and emergency response, in large part to maintain awareness of and actively limit staff fatigue leading to burnout. Resources to be identified in this way include personnel, teams, equipment, supplies, and facilities available or potentially available for

assignment or allocation.

7.9 INTEGRATED COMMUNICATIONS

Cyber incident response voice and data communications are facilitated through the development and use of a common communications plan and interoperable communications processes and architectures.

An integrated communications approach links the operational and support units involved and is necessary to maintain common situational awareness and interaction. Preparedness planning should address the equipment, systems, and protocols necessary to achieve integrated voice and data communications.

7.10 ESTABLISHMENT AND TRANSFER OF COMMAND

The command function must be clearly established from the beginning of cyber incident operations and may be transferred in a prolonged cyber incident response situation. When command is transferred, the process must include a briefing that captures all essential information for continuing safe and effective operations.

7.11 CHAIN OF COMMAND

Chain of command refers to the orderly line of authority within the ranks of the Cyber Incident Response Team (CIRT) to clarify reporting relationships and eliminate the confusion caused by multiple or conflicting directives.

7.12 DISPATCH/DEPLOYMENT

Resources should respond only when requested or when dispatched by the appropriate authority. Resources not requested must refrain from spontaneous deployment to avoid overburdening the recipient and compounding accountability challenges.

7.13 INFORMATION AND INTELLIGENCE MANAGEMENT

The CIRT must establish a process for gathering, analyzing, assessing, sharing, and managing incident-related information and intelligence.

8. INCIDENT RESPONSE ORGANIZATION AND OPERATIONS

All cyber incidents involve similar response tasks. The problem(s) presented by the cyber incident must be identified and assessed, a plan to deal with the problem(s) developed and implemented, and the necessary resources acquired. The CIRP provides the structure for effectively managing the following common incident tasks:

- Providing leadership and developing an organizational structure to minimize the potential or actual impacts of a cyber incident
- Setting goals, objectives, strategies and tactics
- Developing plans and clearly communicating those plans to all involved
- Managing information and helping ensure that all internal and external stakeholders receive timely information concerning the cyber security incidents, threats, and vulnerabilities
- Tracking the status of the cyber incident from the initial escalation phase through to the de-escalation, resolution, and post-incident review
- Maintaining effective span of control and ordering additional resources as needed
- Documenting the cyber incident response decisions and activities

Effective response to significant incidents requires a division of labor to accomplish these tasks. The organization of the CIRP is built around five major management activities:

1. **Incident Command**
   Sets objectives and priorities and has overall responsibility at the incident.
2. **Business Operations**
   Conducts tactical operations to carry out the plan develops the tactical objectives, organization, and directs all resources.
3. **Planning**
   Develops the action plan to accomplish the objectives, collects and evaluates information. Maintains resource status.
4. **Logistics**
   Provides support to meet incident needs, provides resources and all other services needed to support the incident.
5. **Finance / Administration**
   Monitors costs related to incident, provides accounting, procurement, time recording, and cost analyses.

These five major management activities are the foundation upon which the CIRP organization develops.

8.1 The Five Primary Phases in The Planning Process:

Understand the Situation

The first phase includes gathering, recording, analyzing, and displaying

situation, resource, and incident-potential information in a manner that will facilitate:

- Targeted situational awareness of the magnitude, complexity, and potential impact of the incident
- Confirming the resources required to develop and implement the CIAP

Establish Incident Objectives and Strategy

The second phase focuses on formulating and prioritizing measurable incident response and identifying an appropriate strategy. The incident objectives and strategy must conform to the firm's legal obligations and management objectives. Reasonable alternative strategies that will accomplish overall incident objectives are identified, analyzed, and evaluated to determine the most appropriate strategy for the situation at hand. Evaluation criteria include public injury factors, estimated costs, and various regulatory, legal, and political considerations.

Develop the Plan

The third phase involves determining the tactical direction and the specific resources, reserves, and support requirements for implementing the selected strategies and tactics for the operational period. Before each meeting of the CIRT, each member of the response team is responsible for gathering information to support the proposed plan.

Prepare and Disseminate the Plan

The fourth phase involves preparing the plan in a format that is appropriate for the level of complexity of the incident. For the initial response, the format is a well-prepared outline for an oral briefing. For most incidents that will span multiple operational periods, the plan will be developed in writing according to procedures and captured in the standardized CIAP template.

Execute, Evaluate, and Revise the Plan

The planning process includes the requirement to execute and evaluate planned activities and check the accuracy of information to be used in planning for subsequent operational periods. The CIRT should regularly compare planned progress with actual progress. When deviations occur and when new information emerges, it should be included in the first step of the process used for modifying the current plan or developing the plan for the subsequent operational period.

9. INFORMATION SHARING AND BREACH REPORTING

9.1 PRIVACY BREACH NOTIFICATION

Incident response plans should include explicit guidance on how to deal with potential data breach incidents including notification to all applicable regulators. Refer to section 3.4 on key legal considerations.

9.2 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 and 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. Doubts about the integrity of one market participant can quickly shift to others and impact overall investor confidence. Finally, it can concern sensitive information, which can be potentially harmful for one organization, while being very useful to others.[40]

For Dealer Members, there are a variety of opportunities and forums for engaging in proactive information sharing. 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.

9.3 VENDOR/OUTSOURCING RISK MANAGEMENT

Reliance on third-party vendors for providing key services continues to be a significant strategy for many Firms. Dealer members outsourcing services inherit the security practices of those vendors into its own risk profile. Care must be taken to ensure that operations and risks are being fully transferred and managed by vendors.

The essential elements of a vendor or outsourcing risk management program include:

- Risk ranking vendors
- Developing clear policies which vendors are expected to adhere to
- Making conditions explicit within contracts
- Establishing a program to verify the performance of vendors

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 1 below).

[40] Luiijf, E. and Kernkamp, A. *Sharing Cybersecurity Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach*. March 2015

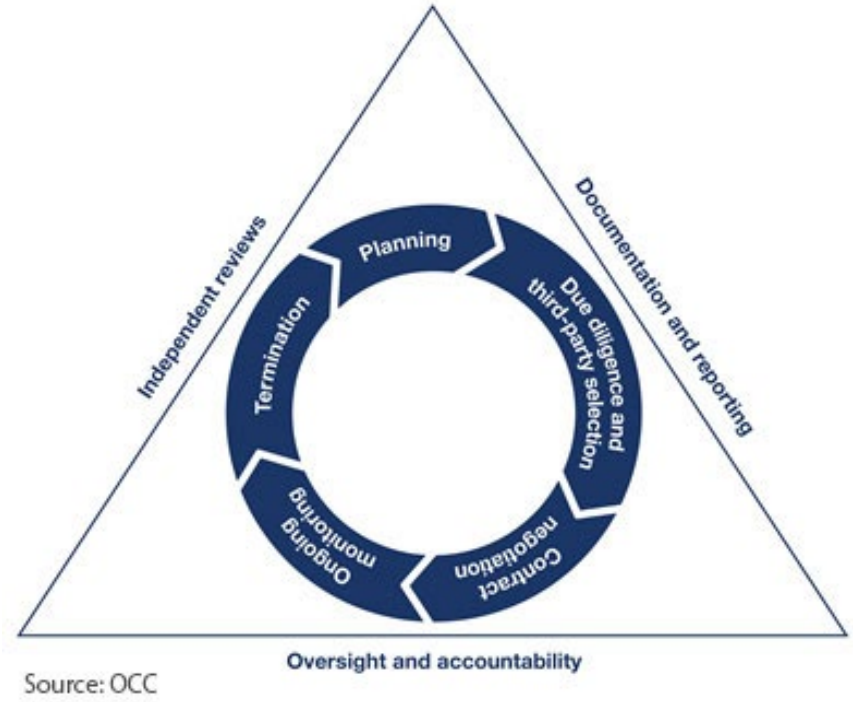


Figure 1 – Risk Management Life Cycle for Third Party Risk, Office of the Comptroller of the Currency (OCC)

Adequate vendor management commences with contracting. 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.

Firms should approach vendor risk management in a tiered fashion with the highest risk relationships managed first. Typically, these will be back office and front office vendors.

Vendor Stratification 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, Safe Harbor, etc.)
- Previous data or security breaches
- Extent of outsourcing performed by the vendor

- Performance history

Common Deficiencies with Third-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[41]
- Requests for documentation from potential vendors[42]
- Third party certifications such as ISO 27001, SOC 2, ISO 27017, ISO 27018
- Desk assessments to evaluate requested information
- On-site visits as appropriate by either in-house or contracted experts
- Penetration tests of potential vendors

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.

9.4 CLOUD COMPUTING

Cloud computing means storing and accessing data and programs over the Internet instead of on a local computer. [43] While there are many advantages to cloud computing, it carries with it risks that are similar to those associated with outsourcing to third-party vendors. In fact, many third-party vendors have been moving services to the cloud.

Cloud services for firms can range from back-up, archiving, file sharing and distribution, and much more. A cloud services provider'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 its 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 that: [44]

[41] See Appendix B in IIROC's Cybersecurity Best Practices Guide for a Sample Vendor Assessment Questionnaire.
[42] For examples of types of documentation, see Appendix B in IIROC's Cybersecurity Best Practices Guide for a Sample Vendor Assessment Questionnaire.
[43] Eric Griffith. April 2015. "What Is Cloud Computing?"
[44] ISACA. Security Considerations for Cloud Computing. 2012

- has a significant history in the cloud services industry who can provide solid business references
- clearly outlines its mitigating controls for handling risk – controls related to security, availability, processing integrity, confidentiality, and privacy
- has clear service level agreements especially in regard to:
    - Availability,
    - notification of potential incidents, and
    - responding to client tickets
- allows auditing and the verification of controls
- is certified or recognized by one or more security standards authorities
- has backup procedures, business continuity plans, and disaster recovery plans that meet your firm's requirements
- store and manage information in compliance with key privacy laws and regulatory rules, particularly in those jurisdictions where data is stored, and backed up
- facilitates the repatriation of business and client information back to your firm at the end of the contract.

9.5 MANAGED SERVICES PROVIDERS

Many organizations especially small and medium-size businesses outsource IT and security to a Managed Service Provider (MSP). These MSPs provide access to scarce expertise, enable 7/24 monitoring and provide additional response capabilities.

Services provided by MSPs can range from point solutions such as the management of firewalls, perimeter monitoring and end-point protection to full security services across all devices and information in an organization. Dealer members need to carefully consider what it wants to outsource. Answers to the following questions can help determine when to outsource security services and which providers best meet a specific firm's needs:

1. What are the respective responsibilities and accountabilities for protecting our firm's data? Are roles and responsibilities clearly defined with measures of accountability?
2. What is the onboarding process? What steps will be taken to provide the services being contracted and ensuring it is operating at the levels expected? How much time and effort is expected from our firm?
3. What level of access will our firm have to logging information of the security services and activities of security staff?
4. Who will be able to access our firm, and under that circumstances? What is the audit trail of staff and their access to our firm's data and the configuration of services we are being provided?
5. Where will our company's data come to rest? In what countries? Where will backups of our data come to rest as well?
6. What is your service level for availability of the services you are providing?

7. How strong and deep is your expertise? What certifications does your company have, as opposed to individual certifications of staff?
8. What level of client support can I expect?
9. What are your service levels for incident notification? What services are provided to support the investigation, containment and remediation of a potential incident?
10. What is the exit process from this relationship? What services will you provide our firm in the transition? What data can our firm repatriate? What data will be destroyed? What third-party verification will there be that all exit processes have been adequately followed?

9.6 COMPREHENSIVE OFFICE AND COLLABORATION TOOLS

There are companies that offer comprehensive sets of office and collaboration tools including email, documents, spreadsheets, presentations, team chats and meetings as well as file storage and management.

Comprehensive security solutions underlie and support the services being provided including:

- Perimeter protection, monitoring and alerting,
- Encryption of data at rest and in motion,
- Multifactor authentication,
- Compliance with a wide range of laws, regulations and certifications

Medium and higher and offerings typically provide greater security services and protections including data layer protection, privacy protections, eDiscovery and enhanced incident response capabilities. These offerings enable firms not only to outsource information technology operations, example supporting email, file servers, etc., but also security operations and management. Again, like MSPs, such companies centralize expertise from scarce resources in the marketplace.

Firms can outsource much of the operations, support and maintenance of these services, however, they cannot outsource operational and policy governance. In these models, security is a shared responsibility. Vendors provide the infrastructure and core services and firms are responsible for the configuration and operation of information, applications, devices and users. Firms retain responsibility for key operations including:

- The onboarding and off boarding of users
- Device management, in particular mobile device management
- User awareness and training
- Data classification and handling
- Encryption of information, especially at rest

9.7 GOVERNANCE OF HYBRID

Many firms are optimizing its operations and budgets by moving to a hybrid model with some information and services in the cloud and other information and services remaining on-premise or stored in third-party datacenters. The responsibilities for governance remain the same and processes for governing need to be implemented and executed. The focus in a hybrid solution is ensuring:

- Inter-operability of the information and processes on premise and in the cloud and ensuring that no operational or security risks are being introduced.
- Clear definition and accountabilities of roles and responsibilities within the firm for information, services and processes on premise and in the cloud.
- Integration of incident response and business continuity plans, processes and capabilities.