IIACACCVM
INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÈRES

11 King Street West, Suite 1600, Toronto ON M5H 4C7
T 416.364.2754 | F 416.364.4861

www.iiac.ca

IIAC Cybersecurity Guidebook

June 2015

In a matter of a few years, the issue of cyber crime has gone from being a rather limited IT issue to one which demands the attention of senior executives and board members.

The prevailing expert opinion is that eventually, all firms will be subject to some sort of cyber-incident. As cyber criminals have become more sophisticated, and attacks have become much more prevalent, the potential for serious financial, operational and reputational damage of a cyber attack is becoming recognized as a critical risk that must be managed at the highest levels of an organization.

Financial services firms, in particular, are targeted at high rates. This is due to a number of factors, including their direct and indirect access to financial assets, sensitive client information, information about potential and current transactions, and trading data and algorithms. In addition the profile and symbolic status of financial firms as institutions of power and capitalism make them a target for hacktivists.

The financial industry is particularly vulnerable to cybersecurity threats due in part to the fact that it is operations are extremely reliant on technology. In addition, there are many technological interconnections between firms, their employees, third party service providers, data vendors, marketplaces, and the vast number of other institutions that comprise the financial markets. The amount of data that is generated and shared between these entities can be extremely valuable, and every data entry point and system intersection provides a target for those seeking access.

The level and types of threats will vary among firms, depending on their size, business model and profile. Smaller firms should be aware that they are as much a target as larger firms. The 2015 Symatech Annual Internet Security Threat Report indicated that in 2014, 60% of all targeted attacks struck small and medium sized organizations.

As such, it is critical that all firms develop and maintain comprehensive cybersecurity plans to protect themselves, their clients, and the industry in general, from the damage that a cyber attack can inflict. Having a robust cybersecurity program will not eliminate all cyber risks or guarantee that the firm will not be a victim of a cyber incident. It will however, allow a firm to manage risks through an informed decision-making process. This is also known as cyber resilience.

The IIAC is committed to assisting our Members in their efforts to be cyber-resiliant. The Cybersecurity section of our website contains information, tools and links to resources intended to assist firms in developing and maintaining their cybersecurity plans. This paper is intended to give firms an overview of the elements of cybersecurity that they should consider when developing a strategy to deal with this threat.

Contents

Please note: These sections are hyperlinked. Simply click on any title and you will be taken directly to that section.

I. Overview of the Cybersecurity Threat

The increasing incidence, scope and impact of cyber crime has elevated this issue from the confines of the IT department to the offices of senior executives and boardrooms of businesses, governments and other organized enterprises. As the potential for serious financial, operational and reputational damage of a cyber attack have become apparent, cybersecurity is becoming recognized as a critical risk that must be managed at the highest levels of an organization.

Over the past several years, intrusions into companies' electronic systems have increased in frequency, sophistication, scope and impact. These breaches are also becoming more visible to the public, as high profile systems, data, and client information are affected. In particular, financial services firms are targeted at high rates, due to a number of factors, including their direct and indirect access to financial assets, sensitive client information, information about potential and current transactions, and trading data and algorithms. In addition the profile and symbolic status of financial firms as institutions of power and capitalism make them a target for hacktivists.

The financial industry is particularly vulnerable to cybersecurity threats due in part to the fact that it is operations are extremely reliant on technology. In addition, there are many technological interconnections between firms, their employees, third party service providers, data vendors, marketplaces, and the vast number of other institutions that comprise the financial markets. The amount of data that is generated and shared between these entities can be extremely valuable, and every data entry point and system intersection provides a target for those seeking access.

Threats can originate externally, from those seeking financial gain, or to make a political point or demonstrate their hacking prowess. As often, however, threats can come from internal sources such as employees or other parties that may have legitimate access to certain of the firms' systems.

The sophistication level of cyber attacks has increased significantly over the past number of years. The attacks are no longer restricted to a company's perimeter defence systems such as firewalls and other intrusion detection systems. Rather, the new cyber criminals are capable of detecting and exploiting vulnerabilities in the many layers of a company's networks.

The level and types of threats will vary among firms, depending on their size, business model and profile. Smaller firms should be aware that they are as much a target as larger firms. *"Although many smaller and medium sized companies have historically believed they were too insignificant to be a target, that perception is wrong. In fact, the majority of cyber attacks are levied against smaller organizations that have fewer security resources.* [1]

[1] NACD Cyber Risk Oversight Directors Handbook Series – Executive Summary

The 2015 Symatech Annual Internet Security Threat Report indicated that in 2014, 60% of all targeted attacks struck small and medium sized organizations.[2]

Cybersecurity plans must be tailored to address the specific risks and resources at each firm. There are, however, a number of common elements to the development and implementation of a cybersecurity plan that are common to all entities. The objective of this paper is to identify these commonalities and provide firms with resources to help them identify the steps they should take to reduce their vulnerabilities.

Having a robust cybersecurity program will not eliminate all cyber risks or guarantee that the firm will not be a victim of a cyber incident. It will however, allow a firm to manage risks through an informed decision-making process. This is also known as cyber resilience.

This paper does not provide exhaustive guidance on each cybersecurity issue discussed. As such, firms should use the information only as a basis from which to build a cybersecurity program, taking into account their particular business model, resources and management structure.

In providing this guidance, the IIAC has relied significantly on the excellent report issued by the Financial Industry Regulatory Association ("FINRA") in February 2015. (the "FINRA Report")[3] The key elements of a cybersecurity plan as articulated by FINRA are included in this guidance, and supplemented with examples, resources and regulatory considerations adapted for the Canadian investment industry.

a. Defining "Cybersecurity"

The FINRA Report defined "cybersecurity" as the protection of investor and firm information from compromise through the use—in whole or in part—of electronic digital media, (e.g., computers, mobile devices or Internet protocol-based telephony systems). "Compromise" refers to a loss of data confidentiality, integrity or availability.[4]

b. Threat Landscape

There are a number of cyber threats that exist, with different categories of perpetrators and motives. Four commonly identified cyber threat sources/motivations are:

1. Criminals – often groups or individuals that launch attacks for financial gain;
2. Hacktivists – this may be a group or individuals that launch campaigns to cause embarrassment or financial damage to targets;

---

[2] 2015 Symatech Annual Internet Security Threat Report – p.6
[3] FINRA Report on Cybersecurity Practices – February 2015
[4] FINRA Report on Cybersecurity Practices – February 2015 – p.3

3. Espionage – this is usually carried out by nation-states to gain intellectual property to enhance their own economies
4. War – a nation-state or terrorist group may undertake actions to damage and destroy targets.

In the financial industry, the primary threat is criminal, and secondarily, hacktivists. The targets within a firm are money, information, and/or critical systems. The sources can be external, but often, especially where the motivation is financial gain, firm insiders may be involved.

In developing cybersecurity programs, firms must understand the type and source of threats they will most likely attract based on their business model. From that basis, firms can then build systems and processes to best address these particular threats.

Back to Table of Contents

II. Key Elements in a Cybersecurity Program - Overview

The FINRA Report outlined certain key elements in developing and maintaining a robust cybersecurity program**.** This paper is structured using these elements, and providing further information and resources applicable to each topic**.**

The key elements of a cybersecurity program include[5]:

- **Governance and Risk Management** – Firms must establish a sound cybersecurity governance framework. This must be accompanied by board and senior level support and engagement .
- **Risk Assessment** – It is critical to understand the firm specific risks across the entire range of firm's activities. Firms must understand what is at risk – ie) the firm's assets, and how those assets can be accessed or compromised.
- **Technical Controls** – Managing the firm's technology is a key element in a cybersecurity program. The controls and technology employed will be highly dependent on the firm's business model and operational structure and processes.
- **Incident Response Planning** – Firms must have a tested and executable response plan that can be implemented when an incident is detected. Key elements of a plan include containment and mitigation, eradication and recovery, investigation, notification and a process for making customers whole.
- **Vendor Management** – Investment firms generally have a several relationships with various vendors and other entities that have access to sensitive firm or client information and/or firm systems. This is a key area of risk. Firms should undertake initial and ongoing due diligence that takes into account the potential risk of a breach in areas to which vendors have access.
- **Staff Training** – Given that staff provide a gateway into a firm's systems, it is critical that they be well trained to identify risks and undertake actions to prevent cyber attacks.
- **Cyber Intelligence and Information Sharing** – Cyber attacks may originate from sources, or be executed through means that are known to others who have been targeted, or through detection by experts in the field. In order to understand and respond to the most current threat landscape, firms should take advantage of intelligence sharing opportunities within and outside of the industry. This helps protect individual firms and the industry as a whole.

---

[5] Ibid p.3

- **Cyber Insurance** – In order to protect the assets of the firm and its clients, firms are encouraged to investigate and obtain the appropriate amount of insurance that will cover them in the event of a cyber attack.

Back to Table of Contents

III. Governance and Risk Management for Cybersecurity

An effective cybersecurity governance framework recognizes the importance of cybersecurity efforts and supports timely information flow and decision making to manage ongoing cybersecurity risks.

The following elements are essential to the development and ongoing effectiveness of a cybersecurity governance and risk management plan.[6]

a. Establishing a Cybersecurity Governance Framework

A cybersecurity governance framework is necessary to give senior management a means to understand, prioritize and manage the firm's specific risk exposure. The firm's risk exposure includes operational, legal, regulatory, reputational and environmental elements. Once the risks are identified, the firm can then determine their potential impact, and the strategy for managing the risk. Depending on the potential impact on the firm's reputation and bottom line, firms may choose to mitigate, transfer, avoid, or accept the risk.[7]

The framework should include specific information channels, policies and procedures, controls, and decision making frameworks for cybersecurity information. In order to ascertain the firm's cybersecurity status at any given time, firms must involve their IT department, but also ensure other departments including the business, risk management, compliance, and internal audit departments are included in the process. In addition, internal or external audit—should be involved in assessing the implementation and effectiveness of the firm's cybersecurity program.[8]

Cybersecurity information must constantly be collected and shared across business units. While it is usually the case that the IT department takes the lead in cybersecurity monitoring, some threats may be more likely to be detected by those in the business unit of the firm.

Relevant information should be presented to senior management (including the board) in a manner that allows those in decision making positions to understand and act on information in a timely and informed manner.

b. Board and Senior Management Involvement

It is essential that executive and board level management are involved in cybersecurity management. Senior level understanding and support is critical to ensure cybersecurity efforts are not relegated to the background, and receive appropriate resources and attention to

---

[6] Ibid p.6
[7] National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity- Version 1 – p.5
[8] FINRA Report on Cybersecurity Practices – February 2015 – p.6

ensure that the firm is on top of issues that could have a significant negative effect on every element of a firm's operations.

In 2014, the National Association of Corporate Directors (NACD) addressed the role of the board on cybersecurity in a publication, Cyber-Risk Oversight. In that publication, the NACD—in collaboration with the American International Group and the Internet Security Alliance—cited five cybersecurity principles for boards.[9] The principles state:

i. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
ii. Directors should understand the legal implication of cyber risks as they relate to their company's specific circumstances. For example, high profile attacks my spawn lawsuits, including shareholder derivative suits, alleging the organization's board neglected its fiduciary duty by failing to take sufficient steps to confirm the adequacy of the company's protection against breaches of its data.
iii. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
iv. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.

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

c. The Role of Frameworks and Standards

There are a number of relevant industry frameworks and standards that firms should use to evaluate their cybersecurity readiness and develop a cybersecurity plan. There are several benefits from using an established framework. Most importantly, they provide a tested and endorsed approach to help firms structure their approach to cybersecurity. They can provide a template for a program, or identify gaps in a firm's existing plan. Firms may use multiple frameworks to ensure different elements of their program are covered in an appropriate manner.

The frameworks also assist firms in establishing a common vocabulary around cybersecurity. This helps to ensure that there is precision in communication and fewer opportunities for

[9] NACD Cyber Risk Oversight Directors Handbook Series – p.3

misunderstandings within the firm, and with third parties on an ongoing basis and in critical situations where clear communication is essential.

Some of the most frequently utilized frameworks include:

i. National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 (the "NIST Framework" or "Framework");
    a. NIST, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, Revision 4 (there are a number of other NIST documents that address topics related to information and cybersecurity);
ii. The SANS Critical Security Controls for Effective Cyber Defense (the "SANS Top 20");
iii. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Information Technology 27001 and 27002 framework (collectively, ISO 27001/27002);
iv. ISACA's7 Control Objectives for Information and Related Technology (COBIT) 5;
v. Payment Card Industry (PCI) Data Security Standard (DSS).

In Canada, the Office of the Superintendent of Financial Institutions (OSFI) published a Cybersecurity Self Assessment Guidance[10] more directly targeted at Canadian financial institutions. The OSFI Guidance sets out desirable properties and characteristics of cybersecurity practices against which to measure a firm's current state of preparedness, and provide justification for their status.

The NIST Framework

The NIST was published in February 2014. It is the predominant framework referenced in respect of cybersecurity. NIST also references globally recognized standards for cybersecurity, allowing it to be used by international organizations.

The NIST Framework consists of three parts, the Framework Core, the Framework Profiles and the Framework Implementation Tiers. It provides a thorough, yet flexible risk-based approach for understanding where an organization stands in terms of its cybersecurity activities and where it would like to be to ensure that it is able to achieve its cybersecurity risk management priorities as defined by organizational goals, legal and regulatory requirements, and industry best practices.[11]

[10] OSFI Cyber Secuity Self-Assessment Guidance
[11] FINRA Report on Cybersecurity Practices – February 2015 – p.9

The SANS Top 20

The "SANS Top 20" provides a more tactical view of 20 cybersecurity risk controls that address some of the most common and significant cybersecurity threats. The Controls prioritize and focus on a smaller number of actionable controls with high-payoff; aiming for a "must do first" philosophy and serve as the basis for immediate high-value action. [12]
The SANS Top 20 focuses "first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works" - security controls where products, processes, architectures and services are in use that have demonstrated real world effectiveness."[13]

For each Critical Security Control, the SANS Top 20 describes the importance of the control, then lists actions that organizations are taking to implement , automate and measure effectiveness of the control. The SANS Top 20 also provides specific procedures and tools as well as metrics and tests to enable implementation and assess effectiveness.

d. Metrics

In order to assess the effectiveness of a cybersecurity program, measurement is critical. Firms should develop, implement and monitor metrics to accurately measure the performance of key elements of its cybersecurity program. Along with the metrics, firms must set the appropriate performance thresholds that would achieve the desired results. Metrics should be reviewed for relevancy on an ongoing basis, and where necessary updated to reflect current business and environmental circumstances.

The creation of, and tracking of metrics must be integrated into the cybersecurity governance structure. Firms must develop processes to communicate information about how and if the firm is meeting its objectives to all relevant parties, including management and staff of the business units affected and responsible for cybersecurity functions.

Back to Table of Contents

[12] SANS Institute – Critical Security Controls Webpage
[13] Ibid

IV. Cybersecurity Risk Assessment

A cybersecurity risk assessment is a critical step in the development of a cybersecurity plan. In conducting a cybersecurity risk assessment, firms identify and analyze potential dangers or risks to a firm's business that could arise through its information technology systems.[14]

For example, in the case of broker-dealers, risks include the compromise of customer or firm confidential information, the misuse of customer funds or securities resulting in potential financial losses for the firm or its clients, and the theft of proprietary trading algorithms, as well as adverse reputational impacts for the firm.[15]

In conducting a risk assessment firms should consider what would be the disruption to their business in the event of a cyber attack, and how it would affect their business operations, revenue and reputation.

a. Asset Inventories and Critical Assets

In order to conduct a proper and thorough risk assessment, firms must undertake an asset inventory. The value of the assets should be examined not only from the firm's perspective, but from the perspective of potential cyber criminals, who may be acting for financial or other reasons. This is important, as the targeted assets may differ, depending whether the motivation of the cyber criminal is to obtain funds, information or disrupt firm systems.

Firms must understand what assets they have, and where they are located, in order to protect them. Assets can then be categorized by their importance to the firm's business, which determines the steps they should take to protect them.

Critical assets should be identified as those requiring the highest degree of priority and protection. In order to determine whether an asset is a critical asset, firms must examine its importance to the firm's business model (such as trading systems, client information, corporate finance information) as well as any regulations relating the protection of that asset.

For example, client information is an asset that is subject to a number of regulatory regimes, including IIROC rules and Privacy legislation. Personal information breaches can also result in civil liability, which is potentially very costly. As such, databases and other repositories of client information should be classified as critical assets, and the effort and resources allocated to protecting this asset should reflect their importance.

[14] FINRA Report on Cybersecurity Practices – February 2015 – p.14
[15] Ibid

b. Establishing and Maintaining a Risk Assessment Program

Risk assessment is not a one-time exercise. Firms must constantly assess internal and external vulnerabilities and adjust their plans accordingly. As such, firms must develop an ongoing risk assessment program to ensure the firm's cybersecurity plans protect its current assets from current threats. In setting up a risk assessment program, firms should consider the NIST Framework, which sets out six sets of risk assessment activities or outcomes:[16]

i. identify and document asset vulnerabilities;
ii. review threat and vulnerability information from information sharing forums and sources;
iii. identify and document internal and external threats;
iv. identify potential business impacts and likelihoods;
v. use threats, vulnerabilities, likelihoods and impacts to determine risk; and
vi. identify and prioritize risk responses.

The controls can take several forms:[17]

i. Preventive—these are controls to stop or prevent harm from taking place in the first place; these include, for example, anti-malware, anti-virus software and privilege management tools.
ii. Detective—these are controls a firm uses to identify potential threats that may have occurred, for example, through the detection of data leakage or email content analysis.
iii. Corrective—these are controls that restore a system or process back to the state prior to the detrimental occurrence, for example, a business recovery process that could restore a system to its original state after a system outage.
iv. Event predictive—these are controls that would predict a detrimental event happening, such as notification that a specific type of hack has been occurring at similar firms.

Examples of areas in which a firm may add or make changes to its controls to reduce cyber threat exposure include: [18]

i. Data storage at vendors
ii. Privilege management
iii. Vendor access control

[16] NIST Framework (ID:RA – p22-23)
[17] FINRA Report on Cybersecurity Practices – February 2015 – p.13
[18] Ibid p.13

iv. Employee training
v. WiFi protection
vi. Web/URL filtering
vii. Data encryption
viii. Email content filtering
ix. Staff skillset matching
x. Employee access control
xi. Customer access control
xii. Vendor access controls
xiii. Patch and software updates
xiv. Hand-held device protection
xv. Software development life cycle processes

c. Assessing Threats and Vulnerabilities

There are a number of different ways a firm can assess its threats and vulnerabilities. It is important to understand that cyber threats are not purely external. One of the most common sources of cybersecurity breaches originates from internal system users, such as staff or third party vendors. These cyber threats can be the result of a deliberate act intended to exploit the firm's system, or an unintended breach through an action that allows an intruder to gain access to the firm's systems. (such as clicking on a link that introduces malware into the system)

A number of websites provide information about current threats, and peer-to-peer information sharing can assist firms in identifying threats specific to their industry. In addition entities such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) combine environmental scanning with information sharing to keep firms up to date about the latest threats and how to combat them.

One commonly used approach to conducting a risk assessment is the Common Vulnerability Scoring System (CVSS) to assess vulnerabilities in applications. CVSS is an industry open standard for assessing the severity of vulnerabilities and prioritizing their remediation. The results of these reviews are used as inputs to the firm's risk assessment program and would drive risk ratings of various critical assets.[19]

It is important that firms affiliated with other financial organizations such as banks, take an enterprise wide approach to cybersecurity. The assessment must include all of the business units, such as the banking, insurance, mutual fund, and broker dealer functions, as well as any other divisions. Given the number of interconnections between the entities, taking a silo approach to cybersecurity will not be effective.

[19] Ibid p.14

In large and geographically spread out organizations, threat analysis can become disjointed, and dispersed among several functions, physical locations and systems. This can present challenges in collecting and analyzing information in a systematic manner to identify and act on risks in a timely and effective manner. Firms must develop internal information sharing processes to ensure potentially important information is not lost or orphaned.

All firms, regardless of size, must have clear processes to escalate concerns identified in the risk assessment to the appropriate level of management. The significance of the risk should be calibrated to the level of management approval that is required to determine whether it will be addressed or accepted as a business risk with no direct action taken to mitigate it.

Back to Table of Contents

V. Technical Controls

The specific technology and controls underpinning a firm's cybersecurity program will be determined in large part by the nature of the firm and its business model. There are a myriad of tools, processes and methodologies available. Firms must take the time to investigate the ones that would provide the best fit for their organization.

The NIST Framework and the SANS Top 20 contain guidance to assist firms in choosing the controls appropriate for their firm's risk profile and tolerance.

One of the ways in which firms protect their data is by using a defence-in-depth strategy. This strategy employs framework that layers security controls throughout a firm's systems. [20] In order to access the desired information, users must present the proper credentials or access codes at various levels. This guards against single point failures in any specific technology or control.

Three key areas to be addressed by technical controls include: identity and access management, encryption and penetration tests.

a. Identity and Access Management (IAM)

A critical element in establishing a cybersecurity plan is to identify users' access to the firm's systems, and implement appropriate controls and limitations on that access. Firms must understand which internal and external parties such as vendors and clients have direct or indirect access to their systems, the scope of that access, and whether that scope is necessary and appropriate for that particular party. An access inventory should be undertaken on a scheduled basis, and upon triggering events, such as changes in job functions, terminations, vendor changes and where a client relationship is terminated.

The increased use of mobile devices by clients, employees and third parties must be considered as it creates complexities around access control, and vulnerabilities out of the control of the firm.

FINRA has indicated that it has noted problems at firms where insiders have gained unauthorized access to firm systems and information.[21]

This can happen when employees are:

i. granted inappropriate access upon hiring;

[20] Ibid p.16
[21] Ibid p.17

ii. allowed to carryover or accumulate privileges as they move from job to job within a company;
iii. are allowed to expand their access without a compelling business need for that access; or
iv. have their credentials stolen and misused.

The FINRA report establishes three important principles that should underlie policies, processes and technical measures.[22]

i. Policy of Least Privilege (POLP) is the concept that the minimum entitlements necessary to accomplish a business objective should be granted to any one individual.
ii. Separation of Duties (SoD) is the concept that actions affecting sensitive assets should require the collaboration of multiple independent roles to succeed. Independence is essential to making implementation of SoD effective. If separation of duties is based on roles that can influence one another, the value of the practice is significantly diminished.
iii. Entitlement Transparency is the concept that it should be easy to know who has access to what at all times. [23]

b. Authorization Schemes

In order for the IAM program to be effective, the process for granting authorization to the appropriate persons and roles must also have a structure and controls that maintains the integrity of the program.

To this end, firms should consider granting access through a centrally controlled function. If entitlements are granted in a dispersed manner, controls such as those enforcing separation of duties or monitoring for and terminating unneeded entitlements can become substantially more complex and expensive. In addition, it can become is extremely difficult to maintain a full inventory of possible entitlement sources and to confirm that all granted entitlements appropriate.[24]

In granting access, firms should review the business justification for each entitlement granted and requirements for access to sensitive information should be challenged. Business necessity rather than convenience should drive access to sensitive data and systems.[25]

---

[22] Ibid p.17
[23] Ibid p.18
[24] Ibid p.18
[25] Ibid p.18

Where possible, firms should ensure that for each role with access to sensitive data there is at least one other control that prevents (or at a minimum detects) misuse or abuse of that entitlement.

Firms should establish controls to detect misuse of sensitive entitlements. For example, there may be nothing unusual about a member of a properly entitled role accessing the confidential records of a customer; however, a member of that role accessing 10,000 customer records within a one hour period may indeed be unusual. Firms should seek to define business rules that differentiate between normal and abnormal use of sensitive entitlements and to create monitoring controls to rapidly detect and investigate abnormal behavior.[26]

It is critical that when employees no longer require access to systems, that the entitlement should be terminated. Firms should enact procedural mechanisms to review access in light of role assignments to ensure ongoing access is appropriate.

c. Encryption

Encryption is a critically important effective practice in a firm's cybersecurity control arsenal. Encryption provides the obvious benefit of protecting the confidentiality of data by ensuring that only approved users (users who hold the decryption key) can view the data. Encryption is a control applied to the data itself. If all of the higher-layer controls fail resulting in exposure of data, encryption can protect that data from being read or altered.[27] The application of encryption should be considered with respect to both workstations and servers. In addition, data-at-rest (stored data) and data in-transit over untrusted networks should also be encrypted.[28]

It should be noted that data storage in storage in the cloud does not increase or decrease the risk of unauthorized access. As such, sensitive data stored in the cloud should be encrypted before placing it in the cloud. In order to further mitigate risks, the firm should control the encryption controls rather than using such controls provided by the cloud provider.

d. Third-party Penetration Testing

In order for firms to understand their vulnerabilities from a cyber attacker's perspective, it is useful to undertake Penetration Testing (also known as "Pen Testing"). A Pen Test, is an attack on a computer system that mimics a real-world cyber attack. Pen Tests can be targeted to access specific systems, or conducted on a more general basis to find vulnerabilities in a firm's systems in general. The NIST Framework, SANS Top 20 and OSFI Self Assessment Guide, all recommend firms regularly conduct Pen Tests.

---

[26] Ibid p.19
[27] Ibid p.20
[28] Ibid p.20

A Pen Test target may be a white or glass box test (where all background and system information is provided) or a black box test (where only basic or now information is provided except the company name. There are also several variations in between, often known as grey box tests. The relative merits of these approaches depend on the testing objective. Black box testing simulates an attack from someone who is unfamiliar with the system. White box testing simulates what might happen during an "inside job" or after a "leak" of sensitive information, where the attacker has access to source code, network layouts, and possibly even some passwords.[29]

Firms will also have to decide whether they test against production or non production systems. Although testing against production systems is ideal from a security perspective as it leaves no question as to whether production controls are consistent with an alternate testing environment, it may present risks to the firm's data. As such, it may be necessary to perform testing with the system offline and to provide a facility for capturing the production state prior to the test and restoring after the test.[30]

Firms may elect to undertake testing in manner where only a small number of the firm's personnel are aware of the test. A secret test demonstrates how well the firm's monitoring and detection systems operate, and also tests the firm's incident response function.

Back to Table of Contents

[29] http://www.redsphereglobal.com/content/penetration-testing
[30] FINRA Report on Cybersecurity Practices – February 2015 – p.22

VI. Incident Response Planning

Given the reality that despite significant resources being allocated to preventing cyber attacks, firms continue to be attacked, much of the spending is being transitioned from prevention to incident response and recovery. All firms should have an incident response plan (IRP) that provides management and staff with a list of tasks and issues to consider in the event of a cybersecurity event. The purpose of the IRP is to limit the damage that the event may have on the firm's systems, clients and reputation. A properly designed IRP will also reduce the time and cost of recovering data and resuming operations.

An IRP is essentially a playbook that details who, according to their role, should take actions, what their responsibilities are, and to the extent possible, exactly what actions they should undertake.

Although some large firms may have a designated team created to manage cybersecurity incidents, most firms do not have the in-house expertise to identify the source of the breach, the scope and severity, and what systems might be compromised on a timely and comprehensive basis. As such, many firms will have to rely on a combination of staff and third party providers to manage the technical, specialized and multifaceted procedures that must be launched in the event of a cybersecurity incident.

Although it is impossible and inefficient to try to anticipate every possible cyber incident that may occur, in drafting an IRP, a firm should identify the types of incidents, attacks or breaches that they are most likely to be subject to, based on their risk assessment, and on-going information gathering about the current threats in the environment.

a. Elements of an Incident Response Plan[31]

i. Investigation and Analysis

The incident response team should work quickly to analyze and validate each incident, following a pre-defined process, documenting each step taken. When the team believes that an incident has occurred, it should rapidly perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited). The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident. [32]

---

[31] FINRA Report on Cybersecurity Practices – February 2015 – p.24
[32] NIST Computer Incident Handling Guide p29

ii. Containment and Mitigation

Containment is important before an incident overwhelms resources or increases damage.[33] The containment decisions to shut down a system, disconnect it from a network or disable certain functions should be planned in advance for different types of attacks, so that they can be implemented quickly and efficiently.[34] Containment strategies will vary based on the type of incident. For example, the strategy for containing an email-borne malware infection is quite different from that of a network-based attack. Organizations should create separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision-making. Some of the criteria for determining the appropriate strategy include: [35]

1. Potential damage to and theft of resources
2. Need for evidence preservation
3. Service availability (e.g., network connectivity, services provided to external parties)
4. Time and resources needed to implement the strategy
5. Effectiveness of the strategy (e.g., partial containment, full containment)
6. Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

iii. Eradication and Recovery

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected assets within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery. [36]

In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords and tightening network perimeter security. Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner.[37]

---

[33] Ibid p.34
[34] Ibid p.35
[35] Ibid p.35
[36] Ibid p. 37
[37] Ibid p.37

iv. Investigation

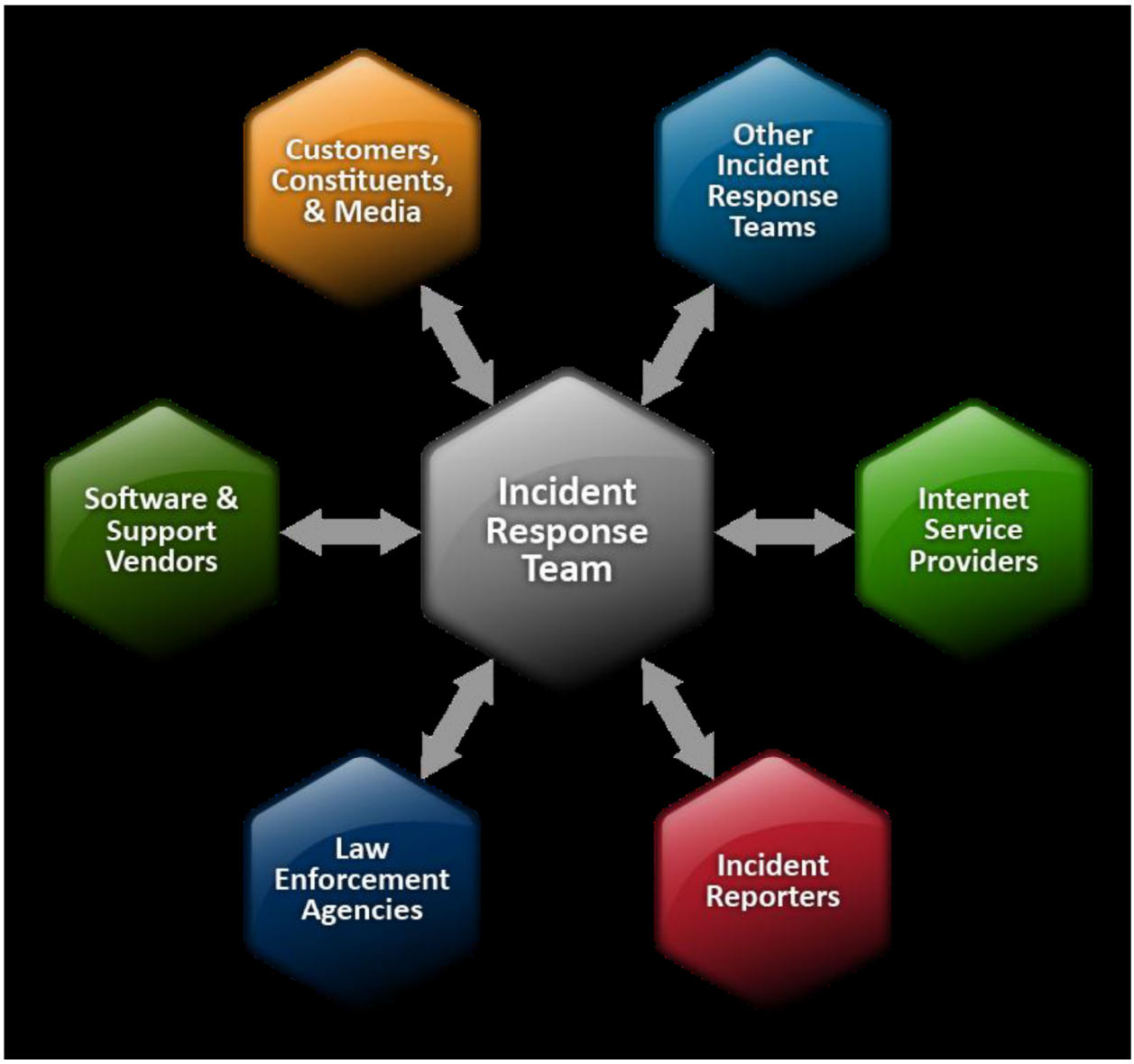
When a cybersecurity incident occurs, firms are expected to conduct a timely investigation of the incident to determine the extent of data or monetary loss and identify root causes. To be prepared for an effective investigation, firms should identify all log information to be recorded and maintained and develop a log retention policy. [38]

v. Notification

The incident response plan should identify the parties to be notified, as well as what information should be reported and when. Identifying the varying requirements in the response plan will aid a firm's ability to provide notifications in a full, accurate and timely fashion. [39]

[38] FINRA Report on Cybersecurity Practices – February 2015 – p.24
[39] Ibid

NIST (NIST Computer Incident Handling Guide provides a graphic of notification targets.)



vi. Post Incident Analysis

A key element of incident response is a post-incident review and analysis with the objective to learn and improve, so that they can respond more effectively to new threats as they emerge. Firms should hold a "lessons learned" meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident.[40]

[40] NIST Computer Incident Handling Guide p.37

Questions to be answered in the meeting include:

1. Exactly what happened, and at what times?
2. How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
3. What information was needed sooner?
4. Were any steps or actions taken that might have inhibited the recovery?
5. What would the staff and management do differently the next time a similar incident occurs?
6. How could information sharing with other organizations have been improved?
7. What corrective actions can prevent similar incidents in the future?
8. What precursors or indicators should be watched for in the future to detect similar incidents?
9. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?[41]

vii. Making Clients Whole

Incidents where clients lose money or have their personal information compromised can lead to loss of investor confidence in broker-dealers. To help address this, firms should:

1. provide free credit monitoring services to customers whose information has been compromised; and
2. reimburse clients who have lost money through direct attacks—*e.g.*, through an account takeover—or through a cyber-enabled attack, such as a phishing attack that leads to a fraudulent wire transfer. [42]

Back to Table of Contents

[41] Ibid
[42] FINRA Report on Cybersecurity Practices – February 2015 – p.25

VII. Vendor Management

a. Initial Due Diligence

The investment industry relies heavily on third party vendors to provide a variety of services. Given the interconnection of systems and reciprocal access to data, these relationships pose a significant risk to individual firms and across the industry. Firms can be put at risk through misuse of access by the vendor or one of its employees, or if the vendor itself is subject to a cyber attack which exploits the vendor's systems to access firm data and / or systems. In order to protect themselves from such risks, firms must have a vendor management program.

The cornerstone of a vendor management program is a risk based due diligence process that is undertaken on new and existing vendors. In evaluating a vendor, firms should ascertain whether the vendor's cybersecurity controls adequately meet the firm's standards. An imbalance in the integrity of the controls creates a vulnerability for the entity with the higher standard.

When conducting the due diligence on the vendor, firms must consider the sensitivity of the data and the systems to which the vendor will have access, and calibrate its review and requirements accordingly. Firms may have to include a variety of staff (eg: IT, business units, legal, compliance and risk management) and perhaps third party experts in conducting due diligence on prospective vendors, particularly when that vendor has significant access to sensitive data and /or systems.

Vendor due diligence should form part of the governance and risk assessment program, as if it were an internal system. Where a vendor's systems do not meet the firm's standards, firms should ensure that the appropriate level of management is informed pursuant to the governance and risk assessment process, so that decisions can be made to accept, mitigate or reject the risk posed by the vendor.

Some of the vendor's controls that should be examined include:[43]

- limits on data access by vendor employees;
- virus protection;
- encryption of data while at rest or in transit;
- controls in place concerning subcontractors;
- system patch management;
- ethical hacking of online systems;
- change management processes;
- program coding methodologies; and

[43] FINRA Report on Cybersecurity Practices – February 2015 – p.26

- business recovery practices.

b. Contractual Provisions

In order to ensure that the firm has established and ongoing rights in respect of its cybersecurity concerns relating to the vendor, it is important that appropriate provisions are included in vendor contracts. Such provisions will articulate the vendor's obligations and the firm's rights, and the actions that can be taken should concerns arise over matters of significant concern.

The FINRA report noted that standard contract language covered the following topics:[44]

i. Non-disclosure agreements/confidentiality agreements: This language outlines confidential material, knowledge or information that the parties exchange, such as customer PII or company trade secrets. The parties agree not to share further or disclose information obtained under the contract.
ii. Data storage, retention and delivery: This language describes how firm data should be stored and transmitted while on a vendor's system. This may include encryption requirements, requirements as to the type and location of servers used, and business recovery practices.
iii. Breach notification responsibilities: This language addresses the manner and timing of the vendor's notification to the data owner of a security breach and the requirements as to who is responsible for notifying customers along with any related costs. Contract language also would include the definition of a breach as it relates to the data or systems involved.
iv. Right-to-audit clauses: This language gives the data owner the ability to perform physical audits of the vendor's data storage facility and related controls. These clauses also might outline the vendor's responsibility for having a third-party test of the vendor's controls.
v. Vendor employee access limitations: This language defines which vendor employees have access to firm data. Typically this language also documents the approval process for granting this access, *e.g.*, who at the firm would approve employee access to restricted data.
vi. Use of subcontractors: This language outlines any subcontractors that the vendor will use and that would have access to firm data. It also addresses the controls that the vendor would require at any subcontractor, for instance regarding employee data

[44] Ibid p.28

access or data encryption. Typically, controls expected to be present at the vendor would also be required at the subcontractor.

vii. Vendor obligations upon contract termination: This language addresses requirements regarding the destruction or return of any data stored at the vendor's physical locations, including how quickly any data would be disposed of. It also includes language related to removing employee access to the data.

c. Ongoing Due Diligence

In order to ensure the firm is protected on a continual basis, it is important to conduct on-going due diligence of vendor's controls and processes, to determine if they remain robust , relevant and in line with the firm's standards. The ongoing due diligence may not be as intensive as the initial due diligence process, and may involve questionnaires or review of the vendor's third party security reports if applicable.

d. Terminating the Vendor Relationship

It is critical that when a relationship with a vendor is terminated, the firm take action to protect and retrieve the data to which the vendor had access. In addition, all points of access to firm's systems should be terminated. The return of data and removal of access should be clearly documented, by the firm and the vendor, with confirmations issued when data is deleted from the vendor's systems. In addition, governance procedures should continue in effect until all necessary steps are completed.

Back to Table of Contents

VIII. Staff Training

The role of staff training in the implementation of a cybersecurity program is critical. Employee errors and inattention to detail can derail even the most technically robust cybersecurity plan. Frequent employee mistakes include the inadvertent downloading of malware or response to a phishing attack. The danger is compounded when employees are able to access systems remotely from different computers, such as home systems that are used by other individuals

Both the NIST Framework and the SANS Top 20 emphasize the importance of training all users so that they understand the data at risk, the firm exposure, and steps they can take to mitigate risks. Training should be relevant to the tasks performed by the employee, and as such, the focus for IT staff should include different elements than that for other employees.
Some of the key training topics are include:[45]

General Training
Recognizing Risks
Social Engineering Schemes and Phishing
Handling Confidential Information
Password Protection
Escalation Policies
Physical Security
Mobile Security

IT Management Targeted
Application Lifecycles
Application Security
Privilege Management
Emerging Technology Issues
Software Vulnerabilities

Given that clients may have direct or indirect access to firm systems, it may be useful to provide education and information to clients. Information can be conveyed at client meetings, through the firm's website, or via messages sent to clients when they log in to access their account through the firm's access portal. Examples of customer-specific resources include recommendations for creating secure passwords and indications of social engineering attacks.[46] The IIAC series of 101 documents on the IIAC website may also be helpful in educating clients.

Firms should conduct training upon hiring of new employees, and on an ongoing basis. There may be triggering events to ongoing training, based on a schedule, or when an employee changes status and may have access to new data or different systems. In addition, firms

[45] Ibid p.31
[46] Ibid p 32

should ensure employees notified in a timely manner when new cyber threats emerge so that they can be vigilant in terms of the particular elements of that threat.

Back to Table of Contents

IX. Cyber Intelligence and Information Sharing

Given the exponential increase in the number and complexity of cyber threats, it is impractical to expect most firms to have the in-house capability to keep abreast of the current and relevant threats and develop individual strategies to guard against them.

There are a number of information sharing and analysis centres (ISACs) to which firms can subscribe that assist in gathering the relevant intelligence and developing defences to protect firm's business. Not only do ISACs help keep individual firms safe, they benefit the entire industry, as participating firms report emerging incidents and issues, allowing others to be warned and experts to develop defensive strategies on a timely basis.

In respect of the financial services sector, FS-ISAC is constantly gathering reliable and timely information from financial services providers, commercial security firms, federal/national, state and local government agencies, law enforcement and other trusted resources. It then quickly disseminates physical and cyber threat alerts and other critical information to its member firms. The FS-ISAC also provides an anonymous information sharing capability across the entire financial services industry. Upon receiving a submission, industry experts verify and analyze the threat and identify any recommended solutions before alerting FS-ISAC members. This assures that member firms receive the latest tried-and-true procedures and best practices for guarding against known and emerging security threats. [47]

A number of other government agencies, software and data vendors and law enforcement agencies also provide cyber threat intelligence. See below for a list of some of these agencies.

Vendors can provide a range of cybersecurity services, including threat intelligence analysis as well as software and network vulnerability analysis. Vendors can also undertake testing to identify existing issues and potential problems at a level that would be difficult for firms to achieve without dedicated expertise.

Back to Table of Contents

[47] FS-ISAC Webpage (About Us)

X. Cyber Insurance

Cyber insurance can be used to transfer the risks that have not been adequately addressed or mitigated in a firm's cybersecurity plan, and as such reduce the risk that a cyber incident will materially affect the firm's financial integrity.

Firms should consider if this type of insurance is an appropriate component of their risk management program. The cost of premiums on a cybersecurity insurance policy can vary, depending upon factors such as the type of confidential information on hand and the level of cybersecurity risk that a business faces. In determining whether to include cyber insurance as a part of a firm's cybersecurity plan, a number of questions are relevant.

- Which events are insurable
- Do the firm's risk management approaches adequately cover the financial risks associated with cybersecurity events
- What coverage will a new or enhanced cyber insurance policy provide and what will it cost? [48]

Cyber liability policies can provide both first-party and third-party coverage. First-party coverage protects firms against losses sustained by the firm, such as damage to the firm's company's data files. Third-party coverage protects firms against lawsuits filed by parties who claim the firm has injured them in some way. There is no "standard" cyber liability policy and the coverage offered by insurers may differ. Examples of events covered by typical policies are described below. [49]

a. First Party Coverage

The first-party coverage provided by cyber liability policies typically include various types of property and crime insurance. They also cover certain types of expenses, such as those incurred for crisis management. Examples of first-party coverage include:

i. Loss or Damage to Electronic Data- This covers losses caused by damage, theft, disruption, corruption etc. of firm data or data belonging to someone else that is stored on the firm's computer system, if the loss is caused by accidental damage, an operational error, hacker attack, virus, denial of service attack or other cause. It includes the costs to restore or recover lost data, costs to prevent further damage, and the cost of outside experts or consultants firms must hire to preserve or reconstruct their data.

---

[48] FINRA Report on Cybersecurity Practices – February 2015 – p.37

[49] http://businessinsure.about.com/od/errorsandomissionsliability/fl/Whats-Covered-Under-A-Cyber-Liability-Policy.htm

ii. Loss of Income and/or Extra Expenses - This covers loss of income and extra expenses incurred to avoid or minimize a shutdown of business after a firm's computer system fails due to one of the covered causes

iii. Cyber Extortion Losses – This type of coverage applies when a hacker or cyber thief breaks into the computer system and threatens to damage firm's data, introduce a virus, or shut down the system unless the firm pays a sum of money. The perpetrator may also subject computers system to a denial of service attack or threaten to release confidential data unless the firm pays the sum demanded. Extortion coverage typically applies to expenses incurred with the insurer's consent due to the extortion demand, as well as the money paid to the extortionist.

iv. Notification Costs- This covers the cost of notifying the parties whose data has been affected by the breach as required by government statutes or regulations. It may include the cost of hiring an attorney to determine what the firm is obligated to do under applicable laws and regulations. It also covers the cost of providing credit protection services for those affected by the breach.

v. Damage to the Firm's Reputation-This covers costs for marketing and public relations to protect the company's reputation and avoid bad publicity following a data breach.

b. Third-party Liability Coverage

Most cyber policies cover more than one type of liability. Coverage generally applies to damages claimed against firms as a result of errors and omissions it allegedly committed in creating, sending, receiving or storing electronic data. While policies typically cover the cost of defending against covered claims, these costs are likely subject to the policy limit. Types of third-party liability coverage include:

i. Network Security Liability – This covers lawsuits due to a data breach or to the inability of others to access data on the firm's computer system. Coverage may apply if the data breach or inability to access the system is due to a denial of service attack, a virus, malware or unauthorized access and/or use of the system by a hacker or rogue employee. Policies may cover lawsuits alleging that the firm failed to adequately protect data belonging to customers, clients, employees or other parties.

ii. Network Privacy Liability –This covers lawsuits based on allegations that the firm failed to properly protect sensitive data, stored on its computer system, which belongs to customers, clients and other parties. Some policies cover liability arising from the release of private data (such as social security numbers) belonging to a firm's employees.

iii. Electronic Media Liability- This covers lawsuits for acts like libel, slander, defamation, copyright infringement, invasion of privacy or domain name infringement. Generally, these acts are covered only if they result from publication of a firm's electronic data on the Internet.

Given that the market for cyber insurance is relatively new, it is evolving rapidly and subject to increasing competition, so firms are advised to undertake due diligence to ensure they are getting the appropriate coverage for their needs at the best price.

Back to Table of Contents

XI. Conclusion

Cybersecurity is a key risk that has moved from an IT concern to the boardroom. The nature of the threat is such that it can have a devastating impact on the firm, and can affect its clients and parties with which it interacts if it is not managed appropriately.

Cybersecurity should be included in firms' strategic plan, and its governance framework. It must be monitored and specifically addressed on an ongoing basis, as firms' business evolve and external threats continually seek new targets and adapt to existing defenses.
The information in this paper is intended to assist firms in ascertaining what they need to do to develop a cybersecurity program tailored to their particular needs. There are many other resources with specific information and guidance that can assist firms in developing and implementing cybersecurity programs that take into account their particular circumstances. Firms will need to work with their internal experts and in many cases, with third parties to ensure the risks to their business is appropriately addressed.

Much attention has been focused on advanced threats that firms face, and those certainly pose significant dangers. However, most successful attacks take advantage of fairly basic control weaknesses. While firms need to stay on guard, they can also take some comfort from this.[50]

The IIAC is committed to assisting our Members in their efforts to be cyber-resiliant. The Cybersecurity section of our website (iiac.ca) contains further information, tools and links to provide firms with additional resources to develop and maintain their cybersecurity plans.

Back to Table of Contents

[50] FINRA Report on Cybersecurity Practices – February 2015 – p.38

The IIAC: Representing Canada's Investment Professionals

The Investment Industry Association of Canada (IIAC) is the national association representing the investment industry's position on securities regulation, public policy and industry issues on behalf of our **148 IIROC-regulated investment dealer Member firms** in the Canadian securities industry. These dealer firms are the key intermediaries in Canadian capital markets, accounting for the vast majority of financial advisory services, securities trading and underwriting in public and private markets for governments and corporations. The IIAC provides leadership for the Canadian securities industry with a commitment to a vibrant, prosperous investment industry driven by strong and efficient capital markets.

For more information, please visit **iiac.ca**.

Toronto – Head Office

11 King Street West
Suite 1600
Toronto, ON M5H 4C7
416.364.2754

Montreal

1, Place Ville Marie
Suite 2001
Montreal, QC H3B 2C4
514.843.8950

Vancouver

701 West Georgia Street, Suite 1500
Vancouver, BC V7Y 1C6
604.637.1676