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

juno RISK SOLUTIONS

Cyber Incident Management Planning Guide

For IIROC Dealer Members

Table of Contents

1 Executive Summary

This Cyber Incident Management Planning Guide is designed to assist IIROC members in the effective preparation of internal cyber-incident response plans. In line with the 2015 IIROC Cybersecurity Best Practices Guide, the document presents a set of voluntary cybersecurity strategies, guidelines, and tools for small and mid-sized IIROC Dealer Members. These can be used to help develop a cybersecurity incident response capability and to respond effectively to incidents.

This Guide is not intended to function as a working response plan. Rather, each Dealer Member should develop internal plans as part of their cybersecurity strategy that prepares them in advance for the risks they are most likely to face.

Section 1 provides members with a brief background on cybersecurity and key industry standard references.

Section 2 provides members with an overview of the incident lifecycle, planning concepts, and key tools upon which to base incident response plans.

Section 3 speaks to the critical issue of engagement outside of the firm. This engagement should include both mandatory reporting as dictated by the type of cyber-incident being experienced, as well as voluntary reporting with key external parties. These parties can include regulators and clients, as well as partners, external vendors, and the government, each of whom can bring essential elements of support when responding to a cyber-incident.

Appendix A includes key recommendations for implementing a cybersecurity incident response capability, and is modeled after NIST's *Computer Security Incident Handling Guide*. **Appendix B** includes a 10-step guide, which outlines how to respond to a cybersecurity incident when your organization is not prepared.

Cyber-incident response planning is an activity that must be part of a comprehensive cybersecurity strategy. Incident response planning should be prioritized based on the types of risks the firm is most likely to face, in addition to those that have the potential for the greatest impact upon the firm, its relationships, and its reputation. This guide provides the means with which to begin that planning process.

This Guide describes common practices and suggestions which may not be relevant or appropriate in every case. It is not intended as a minimum or maximum standard of what constitutes an appropriate cyber-incidence response plan for IIROC Dealer Members. Effective cyber-incidence response planning involves a contextual analysis in the circumstances of each Dealer Member.

This guide is not intended to create new legal or regulatory obligations or modify existing ones, including existing IIROC requirements. The information in this Guide is provided for general information purposes only and is not guaranteed to be accurate or complete, nor does it constitute

legal or other professional advice. Dealer Members seeking further guidance should consult a cybersecurity professional for specific advice about their cybersecurity program and its constituent incident response plans.

1.1 Background

The cyber threat landscape in the financial sector is constantly changing, with new threats surfacing every day.

The best practice hardening of defences at many larger financial institutions has pushed malicious actors to adapt and modify their targets and attack vectors. As a result, smaller organizations can and have been targeted – both for immediate financial gain, and as a means of access into larger organizations' infrastructure. Any institution that has public facing (or Internet facing) operations should consider itself at risk of a cyber breach.

It is therefore critical that all organizations – regardless of size – harden their cyber defences in proportion to the sensitivity of their information assets.

1.1.1 Objectives

This guide on cyber incident management has been designed for small and mid-sized IIROC Dealer Members to enhance their preparedness to deal with a cyber incident. Larger entities are invited to cross-reference their existing incident management protocols with this plan, and to understand the processes their smaller peers will be implementing in crisis response.

This document is not intended to constitute a cyber risk assessment for individual institutions. The recommendations incorporate the contributions of a representative sampling of IIROC's membership. Dealer Members seeking further guidance should consult a cybersecurity professional for a full review of their cybersecurity program, and its constituent incident response plans.

1.1.2 Context

Cybersecurity incidents or events related to Dealer Member information systems can have a significant impact on the delivery of financial services. The ability to respond to cybersecurity incidents in a consistent, coordinated, and timely manner is essential.

This guide draws on cybersecurity principles from the publications listed below:

Standard Number	Title
ISO/IEC 27035:2011	• Information technology – Security techniques – Information security incident management
ISO/IEC 27035-1	• Principles Of Incident Management (Draft)
ISO/IEC 27035-2	• Guidelines To Plan And Prepare For Incident Response (Draft)
ISO/IEC 27035-3	• Guidelines For Incident Response Operations
NIST Special Publication 800-61 Revision 2	• Computer Security Incident Handling Guide
Government of Canada	• Information Technology Incident Management Plan

2 An Overview of Cybersecurity Incident Management

Planning and preparing for a cybersecurity incident can be challenging for many organizations. When a cybersecurity incident occurs, an organization is required to take immediate action in order to mitigate threats to the confidentiality, integrity, and availability of its information assets. This requires effective deployment of resources and established communication strategies.

Targeted organizations face an uphill battle against cyber criminals who, given enough time and money, can breach the most sophisticated system defenses. Potential threat actors include insiders who act with malicious intent, trusted insiders whose acts cause damage by mistake, and attacks from cyber criminals.

Dealer Members should take reasonable measures to respond appropriately in the event of a cybersecurity incident. Poorly-executed incident response has the potential to cause an organization significant financial losses, ruin its reputation, and perhaps even drive it out of business altogether.[i]

Some of the primary objectives of cybersecurity incident management include the following:

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

2.1 Key Terms

The definitions below are based on the International Standard for Information Security Incident Management (ISO/IEC 27035).[ii]

Cybersecurity Event

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

Cybersecurity Incident

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

Cybersecurity Incidents make up a small proportion of Events.

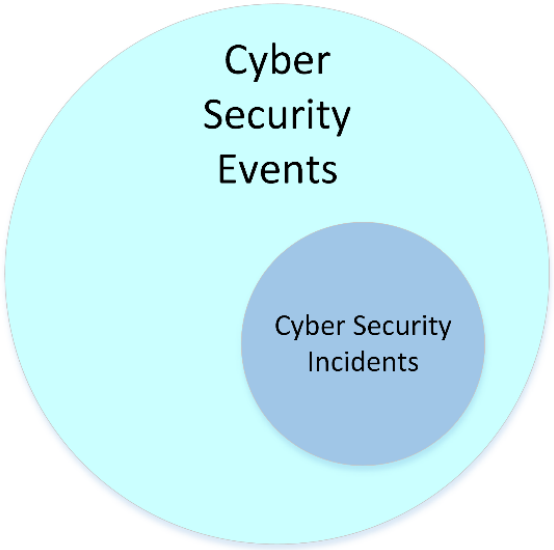


Figure 1 - Cybersecurity Events vs. Cybersecurity Incidents [iii]

Cybersecurity Incident Management

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

Incident Response

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

Incident Response Team (IRT)

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

2.2 The Cybersecurity Incident Chain

Figure 2 outlines the steps in the ISO 27035 Cybersecurity Incident Chain.

Figure 2 - The Cybersecurity Incident Chain

Diagram adapted from ISO/IEC 27035: Information Technology – Information Security Incident Management

2.3 Stakeholders

Primary Stakeholders	Secondary Stakeholders	Other Stakeholders
• Clients • Other Dealer Members (introducers or carriers) • Dealer Members' vendors • IIROC	• Specialized security organizations (e.g. Canadian Cyber Incident Response Centre - CCIRC) • Privacy Commissions • Voluntary information sharing organizations	• The Media • Federal/Regional Law Enforcement

2.4 Cybersecurity Incident Checklist

Table 1 below lists the processes and procedures that need to be in place before, during, and after a cybersecurity incident[iv]:

CYBERSECURITY INCIDENT CHECKLIST

BEFORE AN INCIDENT

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

[Continued on next page]

DURING AN INCIDENT

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

AFTER AN INCIDENT

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

Table 1 - Cybersecurity Incident Management Checklist

2.5 Five Phases of Cybersecurity Incident Management

The five phases of cybersecurity incident management are outlined in Figure 3.

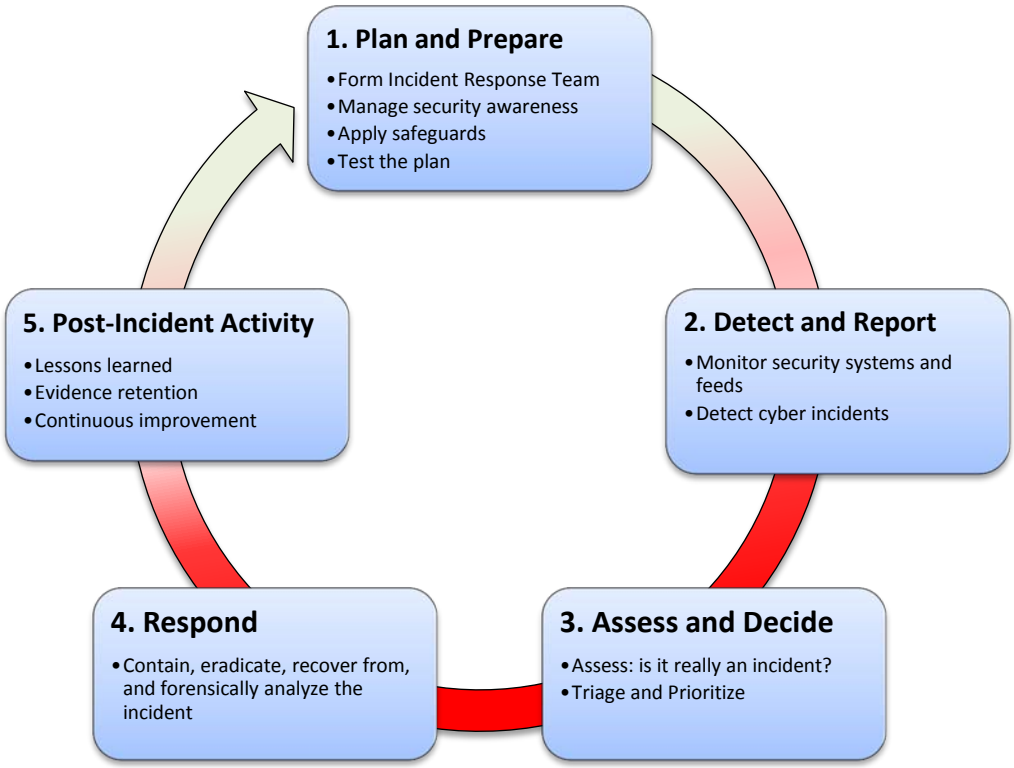
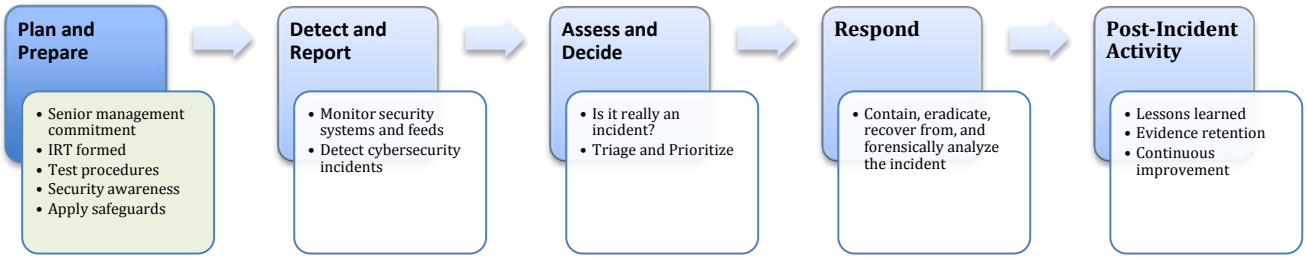


Figure 3 - 5 Key Elements of Cybersecurity Incident Management

2.5.1 Plan and Prepare



Plan and Prepare a cybersecurity incident management plan so that your organization is prepared for a cybersecurity incident when one arises.

When preparing for a cybersecurity incident, stakeholders should consider conducting the following **Key Activities**:

- Obtain support from senior management for the cybersecurity incident management plan.
- Establish a formal cybersecurity incident response capability to respond quickly and effectively when computer security defenses are breached.[v]
- Establish a policy governing cybersecurity incident management that: describes which types of events should be considered incidents; establishes the organizational structure for incident response; defines roles and responsibilities; and, lists reporting requirements.[vi]
- Develop incident response procedures. The incident response procedures provide detailed steps for responding to an incident. The procedures should cover all the phases of the incident response process, and should be based on the cybersecurity incident management policy and plan.[vii]
- Establish policies and guidelines for internal and external cooperation and information sharing.
- Know the information assets that you are responsible for protecting. Your data should be categorized according to its level of business criticality and sensitivity. Details that are collected should also include details about: who owns the information asset, where it is stored, and the controls that are in place to safeguard it. The controls themselves should also be monitored. *The most important thing to understand is what the potential impact of losing the information asset might be.*
- Implement controls to safeguard your organization's information assets. Possible controls include firewalls, patch management, and vulnerability assessments.
- Create an Incident Response Team (IRT).
- Conduct training for team members.
- Develop a communications plan and awareness training for the entire organization.
- Provide easy reporting mechanisms.
- Deploy endpoint security controls (e.g. anti-malware scanners) on information systems. Ensure that anti-malware scanners, and other endpoint controls, have their databases updated frequently. Subscription-based security services such as anti-malware software typically must be renewed on a yearly basis. Once you let the subscription lapse, your information systems will immediately become vulnerable to cyber threats.

- Establish relationships with law enforcement agencies and other external Incident Response Teams.
- Perform evaluations, such as tabletop exercises, of the incident response capability.

The cybersecurity event and incident flow diagram below provides a high-level overview of how cybersecurity incidents are handled.

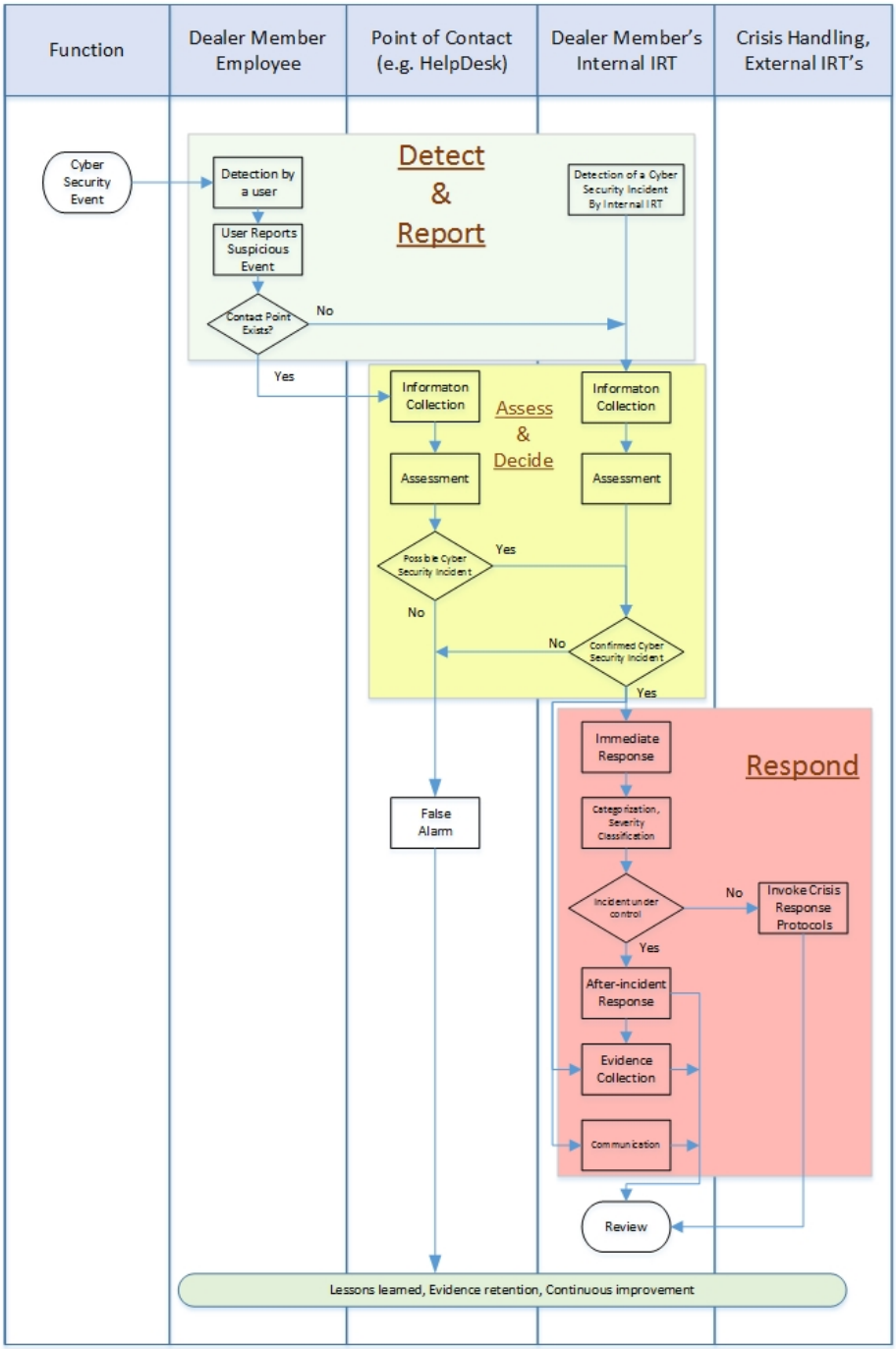
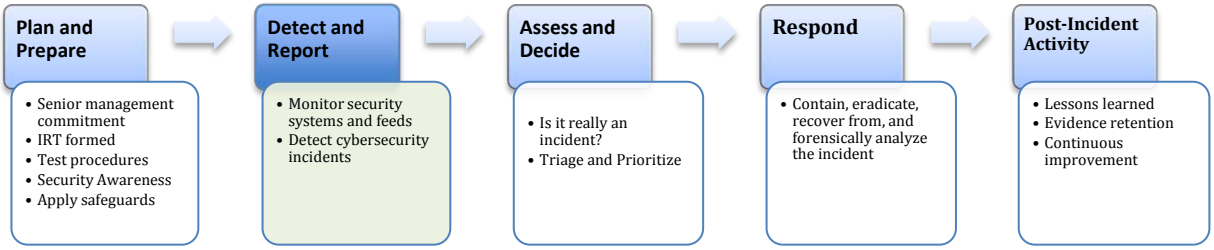


Figure 4 - Cybersecurity event and incident flow diagram[viii]

2.5.2 Detect and Report



This phase involves the continuous monitoring of information sources, the detection of a cybersecurity event, and the collection and recording of information associated with the event.

Key Activities include the following:

- Monitor user reports of anomalous activities
- Monitor alerts from internal security systems
- Monitor information shared from peer organizations, vendors, and organizations who specialize in cybersecurity incidents such as the Canadian Cyber Incident Response Centre (CCIRC) or the Financial Services – Information Sharing and Analysis Center (FS-ISAC)
- Monitor alerts from external information sources such as national incident response teams, law enforcement, etc.
- Look for signs of anomalous activities within systems or the network
- Gather relevant information
- Continue monitoring and detection
- Escalate anomalous reports to the Incident Response Team

2.5.2.1 Possible Causes of a Cybersecurity Incident

The possible causes of a cybersecurity incident include the following:

- Attempts to gain unauthorized access to a system or its data
- Attempts to disrupt an organization's service delivery
- Unauthorized access to information systems
- Unauthorized changes to information systems
- Infection with malware
- A trusted insider with malicious intent
- E-mail with malicious content
- Use of removable media such as an infected USB flash drive
- A user browsing to a web site that takes advantage of a weakness in the browser itself
- The theft or loss of an information system such as a laptop or smartphone

2.5.2.2 Signs of a Possible Information System Compromise

Signs that an information system may have been compromised include the following:

- Accounts or passwords are no longer working
- The company website contains unauthorized changes
- The system has run out of disk space or memory
- It can no longer connect to the network
- It crashes constantly or reboots unexpectedly
- The web browser no longer functions as expected
- Contacts from an email address book are receiving SPAM from that email address
- Endpoint security controls, such as a virus scanner, are no longer functioning
- Endpoint security controls, such as a virus scanner, inform you that an attempt has been made to compromise the information system itself
- Information system logs show suspicious activity

2.5.2.3 What to Report and What Not to Report to an Incident Response Team

It is important that all users know when they should report suspicious activities to their Incident Response Team and when not to. Users should be instructed to contact the help desk or the Incident Response Team directly if they believe an incident may have occurred.

Table 2 below outlines examples of when to report suspicious activity to the Incident Response Team.

The following are examples of events that **should be relayed** to an Incident Response Team:

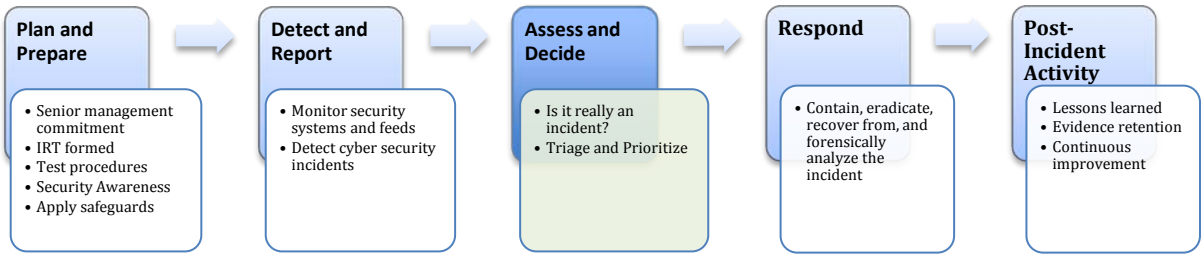
- Suspicious emails with attachments or links
- Data breaches
- Theft or loss of your organization's electronic devices (e.g. laptops and smartphones)
- Critical information systems infected with viruses or other malicious software
- Denial of Service attacks
- Suspicious or unauthorized network activity
- The failure of Dealer Member systems, services, or networks
- The defacement or compromise of your organization's online presence

The following are examples of events that **do not have to be reported** to the Incident Response Team, but should be reported to the help desk.

- Single cases of virus activity that are easily remediated and that do not impact an organization's critical systems
- Short-term outages of non-critical services
- Single cases of standard spam emails without any malicious links or attachments
- Users in breach of organizational specific Internet-related policies or guidelines

Table 2 - What Should be Reported to the Incident Response Team

2.5.3 Assess and Decide



This phase involves assessing cybersecurity *events* and deciding whether or not an actual cybersecurity *incident* has occurred.

The assessment phase begins when there are indications that a cybersecurity event has occurred. Members of the Incident Response Team and help desk can perform the initial assessment. The teams will use already-established criteria, such as those found in Table 2, to determine whether or not the event is actually an incident. Once they have decided that a cybersecurity incident has occurred, the organization needs to determine the impact on the confidentiality, integrity, and availability of the affected information asset.

Cybersecurity Incidents make up a small proportion of Events.

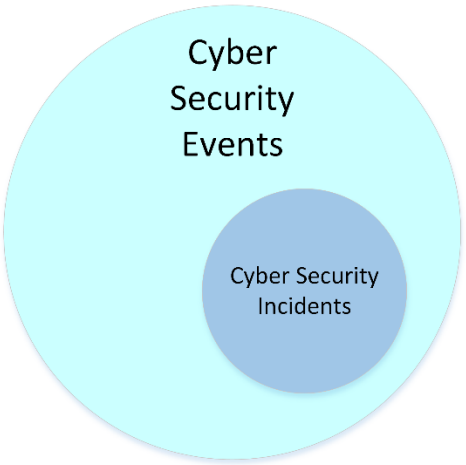
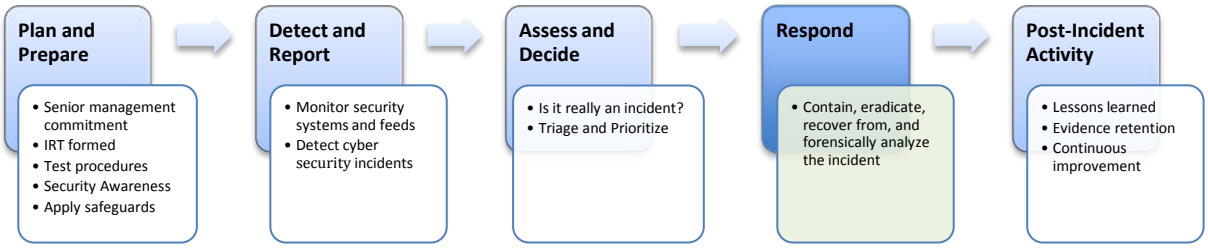


Figure 5 –The Relationship Between Cybersecurity Incidents & Cybersecurity Events[ix]

Activities include the following:

- Assign a person who will be responsible for the event
- Determine whether an event is actually a cybersecurity incident or a false alarm
- If a cybersecurity incident has occurred, then escalation to the Incident Response Team is required
- Find out what information, system, or network is impacted
- Find out what the impact is in terms of confidentiality, integrity, and availability
- Notify the appropriate officials
- Find out if your business partners are being affected

2.5.4 Respond



Respond to incidents: for example by containing them, investigating them, and resolving them.

Activities include the following:

- Assign internal resources and identify external resources in order to respond to the incident
- Contain the problem, for example, by shutting down the system or disconnecting it from the network
- Eradicate the malicious components of the incident, for example, by deleting malware or disabling a breached user account
- Recover from the incident by restoring systems to normal operation and fixing the vulnerabilities to prevent similar incidents
- If necessary, conduct a forensic analysis of the incident

➔ **See Appendix A for communication, reporting, and escalation procedures to be utilized during crisis response**

2.5.4.1 Four Classes of Cybersecurity Incident Response

The purpose of the response phase is to mitigate the impact of threats and vulnerabilities to the affected information system and restore it to normal operations. There are four classes of responses required for a cybersecurity incident:[x]

TECHNICAL RESPONSE

The technical response is designed to focus on the actions the technical staff takes to analyze and resolve an event or incident. Technical staff includes the IT groups required to assist with remediation of the event or incident. This phase can involve several groups or departments within the IT organization to coordinate and provide technical actions to contain, resolve, or mitigate incidents, as well as providing the actions needed to repair and recover, if necessary, affected systems or data.

MANAGEMENT RESPONSE

The management response highlights activities that require some type of management intervention, notification, interaction, escalation, or approval as part of any response. It may include coordinating with corporate communications as it relates to any human resources, public relations, financial accounting, audits, and compliance issues.

Communications Response

These are activities that require some measure of communications to the corporation and internal and external constituents. Corporate communications should always be consulted prior to any communications being released. In many cases, management will direct the release of breach information.

Legal Response

The legal response, if required, would work with outside regulators, third parties, and other parties. In addition, legal input would be required for any external communications, to ensure that such communication is in accordance with company policy and supports any statutory or regulatory requirements.

2.5.4.2 Four Cybersecurity Incident Response Levels for Small and Mid-sized Dealer Members

Whereas the previous section outlined the different types of responses a Dealer Member might undertake, this section discusses the different incident response states or *response levels*. Response states can range from normal day-to-day operations, when a cyber incident is not taking place, to a full-blown cyber incident that impacts many Dealer Members. These response levels will dictate the level of coordination required in response to a given cybersecurity event. Activities include escalation triggers and levels, stakeholder participation, and reporting.

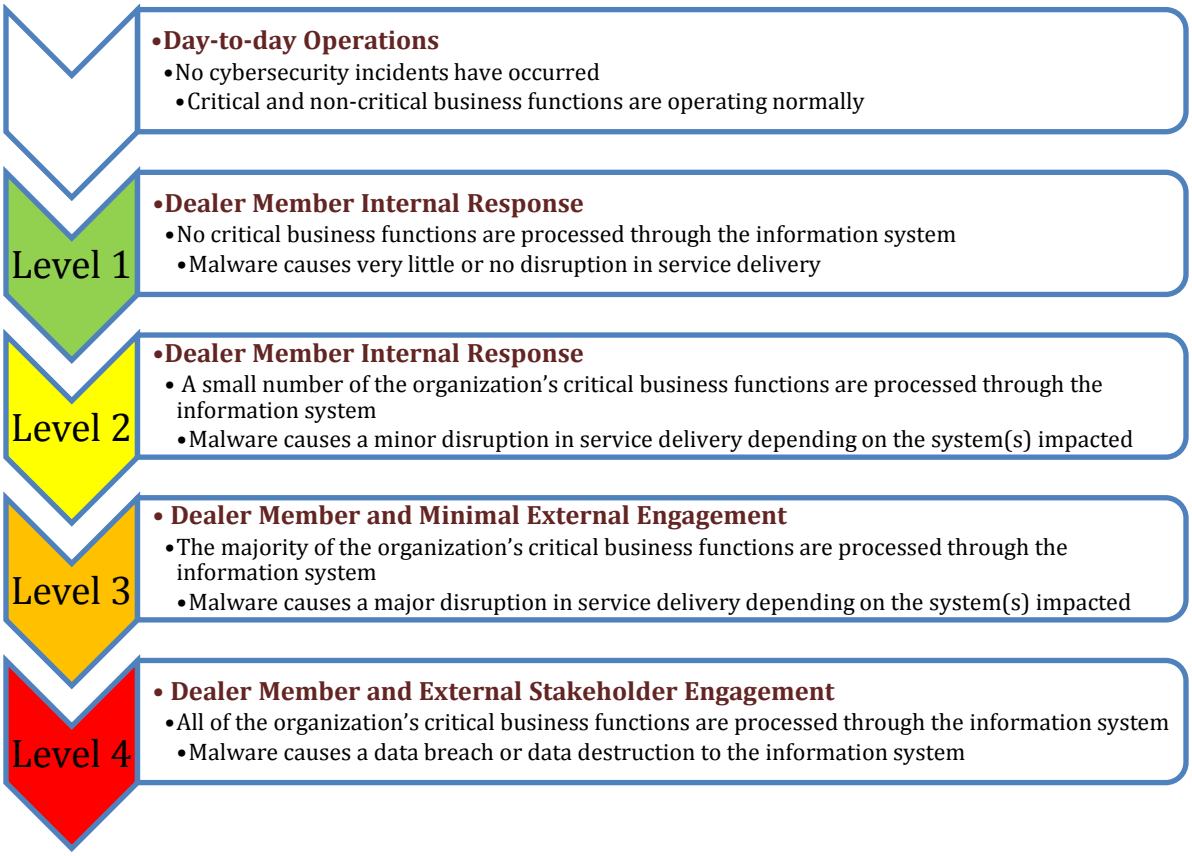


Figure 6 - Response Levels for Small and Mid-Sized IIROC Dealer Members

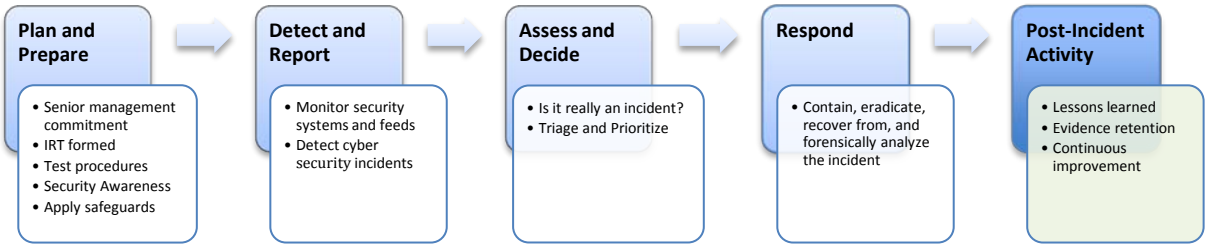
Response Level 1 – Very Little or No Disruption in Service Delivery
This level represents typical, day-to-day operations. Attempts at infecting a non-critical information system may be occurring; however, endpoint controls such as a virus scanner prevent this from happening and remove the threat. If a non-critical system becomes infected, the organization's help desk can remove the threat and restore the system to normal operations. No escalation is required to the Dealer Member's Incident Response Team.

Response Level 2 – Minor Disruption in Service Delivery
This level represents a heightened state of alertness for the Dealer Member. Many non-critical and a few critical information systems may be infected with malware. Escalation to the Dealer Member's Incident Response Team will be required in order to help assess the situation and mitigate the impact of the exposure. If the Incident Response Team and relevant stakeholders decide that there has been no impact on the organization's critical business functions, then they might respond by implementing an emergency malware scanner update or by invoking the emergency patch management process.

Response Level 3 – Major Disruption in Service Delivery
This level indicates that the immediate attention of the Dealer Member's Incident Response Team is required. Critical information systems of the Dealer Member may be compromised by malware. Escalation to this level will trigger a centralized, coordinated response by stakeholders within the Dealer Member's organization. External stakeholders such as vendors who specialize in incident response, law enforcement, and Canadian Cyber Incident Response Centre (CCIRC) might be engaged. Responses may range from having all Dealer Members implement emergency patch updates, to disconnecting the impacted Dealer Member's systems from the Internet.

Response Level 4 – Catastrophic Cybersecurity Incidents
This level is reserved for severe or catastrophic cybersecurity incidents. The Dealer Member's infrastructure may have been destroyed along with critical information system data. Incidents at this level will require the engagement of external stakeholders, such as IIROC, the Canadian Cyber Incident Response Centre, law enforcement, specialized vendors, peer regulatory organizations, and relevant government agencies.

2.5.5 Post-Incident Activity



The Post-incident phase involves activities such as learning from the incident and making changes that improve security and processes.

Activities include the following:

- Identify the lessons learned from the cybersecurity incident
- Identify and make improvements to the organization's security architecture
- Review how effectively the incident response plan was executed during the cybersecurity incident

This is one of the most important parts of cybersecurity incident response. It is very helpful in improving security measures, and the cybersecurity incident handling process itself. It 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.

3 Information Sharing

3.1 Sharing Information with Outside Parties

Information sharing with external parties has proven to be one of the most effective strategies for cyber defense. Predicated on the concept that one institution's security incident is another institution's early warning, sharing of cyber threat intelligence can significantly increase the velocity of response preparation.

Prior to reaching out for assistance or reporting to external parties, it is critical that firms understand both obligations for reporting and requirements for protecting sensitive information.

Key Information Sharing Planning Considerations include:

- Why – Understanding the purpose of the intended exchange
- What – Determining specifically what information will be shared/at what level of detail
- Who – Selecting which parties to share information with
- When – Deciding at what point to initiate an exchange
- How – Selecting both the method of exchange and the protections to be followed

Key Actors in Cybersecurity Information Planning[xi]

The following categories of partner will support engagement strategy planning and may be considered part of an information chain in the event of a cyber incident:

Government – in Canada, the Canadian Cyber Incident Response Centre (CCIRC) is the primary interface between the government and the private sector for incident response. CCIRC provides a range of reporting products to Canadian companies. Early reporting of cyber incidents to CCIRC can provide an excellent early source of intelligence.

Private Critical Infrastructure – Other members of the Canadian financial industry can support incident response with intelligence related to their experience with similar problems. Unless the incident is an issue of first impression, effective external engagement will generate intelligence.

Business Enterprises – Other companies external to the financial sector may have valuable experiences with related threats. Every company shares an interest in protecting its networks and critical information.

IT Companies – firms creating IT products have an interest in protecting their products and their clients. They often share information on vulnerabilities in their products and services so that security firms can create more effective defenses. Engagement with vendors of targeted products can accelerate product lifecycles.

IT Security Firms – these resources can be both a core element of incident response, but also sources of information for responding to threats.

Security Researchers – these researchers are in the academic, business, and voluntary collaborative areas supporting collective cybersecurity. They are both a source of intelligence and potential partners in incident response. Understanding who these resources are can be an effective pre-event activity.

3.2 Sharing Agreements and Breach Reporting Requirements

Information sharing should be driven by a combination of concerns regarding voluntary permissive sharing to achieve institutional objectives, and mandatory breach notification guided by legal obligations. Those obligations are unique to each firm, and are guided by the markets in which the firms operate, and the types of information that has been breached.

In those cases when permissive information sharing with external parties is contemplated, prior efforts to put in place protections in advance of an incident, such as mutual non-disclosure agreements and similar contract terms, can serve to clearly establish the ground-rules for exchange.

3.2.1 Privacy Breach Notification

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

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

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

3.2.2 Information Sharing

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

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

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

3.3 Information Sharing Techniques

Information can be shared in a variety of ways depending upon the sophistication of the information sharing relationship and the intentions of the parties. In advance of a cyber incident, firms should consider the parties with whom they would likely share information, and the nature of the approach. Information sharing techniques include:

- Ad hoc person-to-person
- Machine-to-machine using structured threat intelligence protocols
- Formalized structured exchanges, based on agreed upon protocols and reporting thresholds

Existing exchange forums such as those hosted by FS-ISAC or CCIRC facilitate anonymous exchanges of incident and threat data amongst participants. Less formal exchanges across groups of firms, or amongst IIROC members, should be defined in advance of an incident. This will ensure that the affected firm receives value for the exchange, with the confidence that the shared information will be protected.

4 Appendices

Appendix A: Key Recommendations for Implementing a Cybersecurity Incident Response Capability

NIST's *Computer Security Incident Handling Guide* makes the following key recommendations for implementing a cybersecurity incident response capability:

- **Acquire tools and resources that may be of value during incident handling.** The enterprise team will be more efficient at handling incidents if various tools and resources are already available to them. Examples include: contact lists, encryption software, network diagrams, backup devices, digital forensic software, and port lists.
- **Prevent incidents from occurring by ensuring that networks, systems, and applications are sufficiently secure.** Performing periodic risk assessments and reducing the identified risks to an acceptable level are effective measures to reduce the number of incidents. Awareness of security policies and procedures by users, IT staff, and management is also very important.
- **Identify precursors and indicators through alerts generated by security software.** Intrusion detection and prevention systems, antivirus software, and file integrity checking software are valuable for detecting signs of incidents. Each type of software may detect incidents that the other types of software cannot, so the use of several types of computer security software is highly recommended. Third-party monitoring services can also be helpful.
- **Establish mechanisms for outside parties to report incidents.** Outside parties may want to report incidents to the organization – for example, they may believe that one of the organization's users is attacking them. Organizations should publish a phone number and email address that outside parties can use to report such incidents.
- **Require a baseline level of logging and auditing on all systems, and a higher baseline level on all critical systems.** Logs from operating systems, services, and applications frequently provide value during incident analysis, particularly if auditing was enabled. The logs can provide information such as which accounts were accessed, and what actions were performed.
- **Profile networks and systems.** Profiling measures the characteristics of expected activity levels so that changes in patterns can be more easily identified. If the profiling process is automated, deviations from expected activity levels can be detected and reported to administrators quickly, leading to faster detection of incidents and operational issues.
- **Understand the normal behaviours of networks, systems, and applications.** Team members who understand normal behaviour should be able to recognize abnormal behaviour more easily. This knowledge can best be gained by reviewing log entries and security alerts; the handlers should become familiar with the typical data, and can investigate the unusual entries to gain more knowledge.

- **Create a log retention policy.** Information regarding an incident may be recorded in several places. Creating and implementing a log retention policy that specifies how long log data should be maintained may be extremely helpful in analysis, because older log entries may show reconnaissance activity or previous instances of similar attacks.
- **Perform event correlation.** Evidence of an incident may be captured in several logs. Correlating events among multiple sources can be invaluable in collecting all the available information for an incident and validating whether the incident occurred.
- **Keep all host clocks synchronized.** If the devices reporting events have inconsistent clock settings, event correlation will be more complicated. Clock discrepancies may also cause issues from an evidentiary standpoint.
- **Maintain and use a knowledge base of information.** Handlers need to reference information quickly during incident analysis; a centralized knowledge base provides a consistent, maintainable source of information. The knowledge base should include general information, such as data on precursors and indicators of previous incidents.
- **Start recording all information as soon as the team suspects that an incident has occurred.** Every step taken, from the time the incident was detected to its final resolution, should be documented and time stamped. Information of this nature can serve as evidence in a court of law if legal prosecution is pursued. Recording the steps performed can also lead to a more efficient, systematic, and less error-prone handling of the problem.
- **Safeguard incident data.** It often contains sensitive information regarding such things as vulnerabilities, security breaches, and users that may have performed inappropriate actions. The team should ensure that access to incident data is restricted properly, both logically and physically.
- **Prioritize handling of the incidents based on the relevant factors.** Because of resource limitations, incidents should not be handled on a first-come, first-served basis. Instead, organizations should establish written guidelines that outline how quickly the team must respond to the incident and what actions should be performed, based on relevant factors such as the functional and information impact of the incident, and the likely recoverability from the incident. This saves time for the incident handlers and provides a justification to management and system owners for their actions. Organizations should also establish an escalation process for those instances when the team does not respond to an incident within the designated time.
- **Include provisions regarding incident reporting in the organization's incident response policy.** Organizations should specify which incidents must be reported, when they must be reported, and to whom. The parties most commonly notified are the CIO, head of information security, local information security officer, other incident response teams within the organization, and system owners.
- **Establish strategies and procedures for containing incidents.** It is important to contain incidents quickly and effectively to limit their business impact. Organizations should

define acceptable risks in containing incidents, and develop strategies and procedures accordingly. Containment strategies should vary based on the type of incident.

- **Follow established procedures for evidence gathering and handling.** The team should clearly document how all evidence has been preserved. Evidence should be accounted for at all times. The team should meet with legal staff and law enforcement agencies to discuss evidence handling, and then develop procedures based on those discussions.
- **Capture volatile data from systems as evidence.** This includes lists of network connections, processes, login sessions, open files, network interface configurations, and the contents of memory. Running carefully chosen commands from trusted media can collect the necessary information without damaging the system's evidence.
- **Have a forensics professional obtain system snapshots through full forensic disk images, not file system backups.** Most small and mid-sized Dealer Members will not have the in-house resources capable of conducting a forensic examination of a compromised information system. It is important to establish a relationship with a local vendor of computer forensics services before a cyber incident occurs. When choosing a forensics services vendor it is important to select one that is staffed with personnel who have a forensics certification or designation. The follow is a sample list of forensics certifications:
  - Certified Computer Examiner
  - Computer Hacking Forensic Investigator
  - Certified Forensic Computer Examiner
- **Hold lessons learned meetings after major incidents.** Lessons learned meetings are extremely helpful in improving security measures and the incident handling process itself.

Appendix B: What to Do When a Cybersecurity Incident Occurs and You Are Not Prepared

When a computer security incident occurs and you do not have an incident response plan in place, follow these ten steps:[xiii]

Step 1 – *Remain calm*
Communication and coordination become difficult. Your composure can help others avoid making critical errors.

Step 2 – *Take good notes*
"Cybersecurity Incident Identification." As you take notes, keep in mind that your notes may become evidence in court. Make sure you answer the five W's: Who, What, When, Where, Why, and How. A hand-held tape recorder can be a valuable tool.

Step 3 – *Notify the right people and get help*
Begin by notifying your security coordinator and your manager. Ask that a co-worker be assigned to help coordinate the incident response process. Get a copy of the corporate phonebook and keep it with you.

Step 4 – *Enforce a need-to-know policy*
Tell the details of the incident to the minimum number of people possible. Remind them, where appropriate, that they are trusted individuals and that your organization is counting on their discretion. Avoid speculation except when it is required to decide what to do.

Step 5 – *Use out-of-band communications*
If the computers have been compromised, avoid using them for incident handling discussions. Use telephones and faxes instead. Do not send information about the incident by electronic mail. The information may be intercepted by the attacker and used to worsen the situation. If a computer must be used, encrypt all incident-handling email.

Step 6 – *Contain the problem*
Take the necessary steps to keep the problem from getting worse. This might mean removing the system from the network.

Step 7 – *Make a backup*
Make a backup of the affected system(s) as soon as is practicable. Use new, unused media. If possible make a binary, or bit-by-bit backup.

Step 8 – *Get rid of the problem*
Identify what went wrong if you can. Take steps to correct the deficiencies that allowed the problem to occur.

Step 9 – *Get back in business*
After checking your backups to ensure they are not compromised, restore your system from backups, and monitor the system closely to determine whether it can resume its tasks. Monitor the system closely for the next few weeks to ensure it is not compromised again.

Step 10 – *Leverage lessons learned*
Learn from this experience, so you will not be caught unprepared the next time an incident occurs.

5 References

[i] ISACA. Incident Management and Response. 2012
[ii] ISO/IEC. ISO 27035-2 (2nd Working Draft), Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management
[iii] Government of South Australia. ISMF Guideline 12aCybersecurity Incident Reporting Scheme. 2014
[iv] Hewlett-Packard. Executive breach response playbook: How to successfully navigate the enterprise through a serious data breach. 2015
[v] NIST. Computer Security Incident Handling Guide. 2012
[vi] NIST. Computer Security Incident Handling Guide. 2012
[vii] NIST. Computer Security Incident Handling Guide. 2012
[viii] ISO/IEC. ISO 27035-1 (2nd Working Draft), Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management
[ix] Government of South Australia. ISMF Guideline 12aCybersecurity Incident Reporting Scheme. 2014
[x] Hewlett-Packard. Executive breach response playbook: How to successfully navigate the enterprise through a serious data breach. 2015
[xi] Cristin Goodwin and J. Paul Nicholas. "A framework for cybersecurity information and risk reduction," Microsoft, 2015.
[xii] Luiijf, E. and Kernkamp, A. Sharing Cyber Security Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach. March 2015
[xiii] Northcutt, Steven. COMPUTER SECURITY INCIDENT HANDLING: An Action Plan for Dealing with Intrusions, Cyber-Theft, and Other Security-Related Events. 2003