Cyber Risk Management

A Guide for Healthcare Administrators and Risk Managers

HIROC

November 2017

Healthcare Insurance Reciprocal of Canada

www.hiroc.com

Head Office
4711 Yonge St, Suite 1600
Toronto, Ontario M2N 6K8
Tel: 416.733.2773
Toll Free: 1.800.465.7357
riskmanagement@hiroc.com

Western Region
1200 Rothesay St.
Winnipeg, Manitoba R2G 1T7
Tel: 204.943.4125
Toll Free: 1.800.442.7751
westernregion@hiroc.com

Table of Contents

1 Introduction

The reality is that cyber security can no longer be ignored or treated separately, as it can, and will, present ongoing and evolving risks that endanger both patient safety and financial stability within health care organizations.

(Magee, 2017, p. 2)

Cyber security incidents in the healthcare environment can have serious and devastating consequences. They can lead to one or more losses including service interruptions, operational losses, patient safety issues, reputational losses, privacy breaches, potential civil actions or class action lawsuits, regulatory investigations/fines and financial losses.

Recognizing the vital role critical systems play in patient care, we are slowly expanding from a focus on protecting patient data to the broader goal of protecting the ability to care for patients.

Unfortunately, security infrastructure built with state-of-the-art technology is not enough to protect an organization. A trick played on a single employee can pose a greater threat to the healthcare organization than a team of skillful hackers. There are many factors that go into managing the losses associated with cyber threats and the most important one is resilience. Resilience can be achieved through building organization-wide cyber intelligence, expertise, partnerships and a culture of security with appropriate information technology (IT) solutions.

Purpose of the Guide

There are many reasons healthcare organizations and independent practitioners face challenges when considering and/or implementing a comprehensive cyber security or cyber risk management program:

- Lack of priority given to cyber risk management;
- Lack of access to information security expertise;
- Lack of human and financial resources to implement cyber risk management solutions;
- Continuously evolving technology;
- Increased rate of adoption and reliance on information technology solutions by users; and
- Vast numbers and types of healthcare users – everyone from staff to volunteers and contractors – interact with information systems, networks and devices.

The purpose of this Guide is to provide practical cyber incident prevention and post-incident risk management strategies and recommendations to help minimize the occurrence or impact of cyber-related losses. Our focus is on risk management – identification, management and mitigation of risks – and how to use the various tools and resources to build awareness and cyber resilience.

The Guide is organized into six key sections:

We have included common findings from HIROC claims as well as other Canadian and international healthcare-based case examples.

The recommendations in this Guide are designed to facilitate adoption by healthcare organizations of all sizes and types (e.g. hospitals, long-term care organizations, midwifery practice groups, administrative service providers, family health teams). HIROC recognizes that it may not be feasible or practical for organizations to adopt all of the recommendations in the Guide.

This Guide complements cyber risk management resources and information security frameworks available across the industry and is not intended to cover all information technology-related risks.

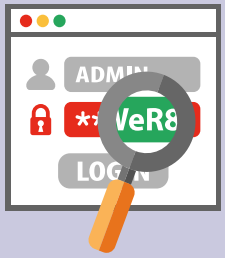
2 The Cyber Threat Landscape in Healthcare

> ***Commentators have said that there are only two kinds of organizations – those that have been hacked and know it, and those that have been hacked and don't know it yet.***
>
> (Freedman, 2017, p. 1)

Change is the only norm in the cyber landscape. Cyber security threats are an evolving area of risk in healthcare with the potential for catastrophic outcomes. HIROC's claims experience and recent outbreaks of ransomware are signs that Canadian healthcare organizations and providers are as vulnerable to cyber threats as private sector organizations.

Here is what a cyber intrusion into a healthcare organization can look like:

Hacking



Cyber criminals often target systems, websites and networks for various purposes such as theft of information or financial gain.

Case example: A healthcare organization's careers' section of their website was hacked into and modified to include malicious code. This resulted in job applicants being redirected to a site where they were asked to pay money to process their job applications. The healthcare organization's website was outsourced to a small vendor and the vendor did not notice that the codes were compromised.

Outcome: Several potential job applicants paid the funds and followed up with the healthcare organization about their application. The website was taken down for a few days to rectify the situation. The healthcare organization published a note on their website about the scam and disclosed the incident to the public.

Malware outbreaks

Malware, or malicious software, includes computer viruses, worms, trojan horses and spyware. They can infect computer systems, servers and workstations and can spread through networks, causing various degrees of harm to an IT infrastructure.

Case example: A hospital was subjected to a malware attack that spread quickly throughout the organization. The malware caused a varying degree of corruption to the operating systems. The affected servers hosted clinical and corporate applications. An investigation of the incident revealed the malware was designed to exploit a vulnerability that was found in Windows XP and 2003. These versions of Windows had not been supported by Microsoft since 2014/2015.

Outcome: The hospital experienced a temporary loss of systems and the network. Some servers and systems were not recoverable and had to be replaced with new equipment.

Ransomware attack

Ransomware is a malicious software that encrypts and prevents access to files, directories and systems until the demanded ransom is paid.

Case example: A healthcare organization was subjected to a ransomware attack and lost control of critical systems and one of their networks. Users were locked out of the system and a screen appeared on the monitor demanding $1000 USD in Bitcoins. The ransomware was disguised as a Microsoft Word attachment of an incoming e-mail with the file name 'invoice'. One of the employees who received the e-mail assumed that it was a legitimate invoice from a vendor and opened the attached document.

Outcome: The IT team attempted to restore the system from the backups with the help of a data recovery firm, however, the systems were not recoverable. During this time, systems were down and some patient care activities had to be diverted to other sites or rescheduled. In the end, the organization paid the ransom in order to receive the decryption key and regain access to their systems.

Alert! Paying ransom is discouraged by provincial/territorial authorities and the Canadian Cyber Incident Response Centre (CCIRC) as it does not guarantee the decryption keys will work or the organization will not be vulnerable to an attack by the cyber criminals again. It only encourages and guarantees criminals can benefit from these activities.

Social engineering/phishing attack

Cyber criminals use this type of attack to trick users into providing pertinent information such as their user ID and password or to click on a malicious link.

Case example: A phishing e-mail was sent to a finance staff member at a hospital who had access to the organization's electronic banking. The e-mail was disguised to look like an e-mail from their regular bank with a request for the staff member to perform certain activities online. He followed the link in the e-mail which directed him to a website that was designed to look like their bank's website. He then proceeded to input the log-in credentials to complete the requested activity.

Outcome: A month later, finance staff noticed a few questionable transactions processed over the weekend. Investigation revealed that they experienced a phishing attack with the perpetrators processing multiple transactions totaling $200,000. The transactions were not recoverable.

Phishing is a well-known social engineering attack technique. It involves an attempt to obtain sensitive information such as usernames, passwords, and credit card details. The target is usually tricked into divulging information because the request is disguised as coming from a trustworthy source such as a bank, government, etc.

3 Accountability Rests With the Board and Senior Management

Just as in financial operations and other areas of enterprise risk management, when it comes to cyber security, the board of directors has "risk oversight" responsibility but does not actually operationally manage cyber security risk.

(Magee, 2017, p. 4)

An important aspect of cyber resiliency is establishing and consistently strengthening a culture of cyber risk management throughout the organization. Cyber risk management is *not* an information technology (IT) issue alone and should be addressed as part of organization's integrated risk management/enterprise risk management (IRM/ERM) program. Board oversight and corresponding senior management accountability are critical foundational components to developing a culture of cyber risk management that effectively supports an overarching cyber risk framework.

Board oversight should at a minimum:

- Ensure cyber risk is part of the IRM program;
- Assign senior management accountability for cyber security and clearly delineate who will ensure the implementation of controls and mitigation strategies throughout the organization;
- Receive regular updates from senior management on the progress and effectiveness of cyber risk management strategies;
- Undertake training, education and research to increase cyber literacy and understand challenges and risks faced by the organization;
- Engage external experts regularly for updates and benchmarking;
- Participate in informed discussions with management about cyber security;
- Undertake self-assessments to gauge the cyber security posture of the organization.

Senior management should at a minimum:

- Be accountable for operationalizing cyber risk management activities that are mandated by the board;
- Serve as an overarching enforcement/escalation body for the organization's cyber risk management undertakings;
- Provide regular progress updates to the responsible board committee;
- Ensure accountability/responsibility for cyber security is cascaded throughout the organization from IT operational leads to all department/program/area managers and leaders;
- Have crucial conversations and make decisions around the cyber security incident response plan (e.g. should we pay the ransom or should we invest up front in sound system recovery solutions);
- Keep vendors, partners and stakeholders fully informed of your organization's cyber security strategy.

4 Cyber Security Incident and Loss Prevention Strategies

Even the most sophisticated security technologies can be rendered ineffective if people don't use them properly. Increasingly, the hacker community is reverting to tricking employees to gain illegal access to corporate assets.

(Public Safety Canada, 2016, p. 9)

Cyber security *incident prevention strategies* focus on information security breach/ incident prevention activities, while cyber security *loss prevention strategies* are intended to reduce the loss experienced as a result of a cyber security incident. In general, cyber security incident and loss prevention strategies are managed through a comprehensive cyber risk management program.

Build resilience through cyber security awareness and training

State-of-the-art technology will not completely protect organizations and providers from intentional or unintentional harmful actions of an end user with access to systems, networks, devices and equipment. One of the most effective cyber security strategies is having a strong awareness and training program.

Here are some ways you can do that:

- Provide mandatory basic cyber security training and current situational awareness training to all end users. This can be provided at new employee orientation or during regularly scheduled intervals throughout the year.
- Extend mandatory refresher training to all employees, contractors, students, volunteers, independent practitioners and third parties.
- Develop and deploy customized training targeted at various functional areas (e.g. IT, finance, clinical areas).
- Train employees to recognize malicious e-mails, links and e-mail attachments.
- Send mock social engineering e-mails to identify vulnerable users.
- Test cyber breach response plans by running table top exercises or drills that involve board members, senior management, program leads and frontline employees.
- Post signage around the premises and blog messages and FAQs on the intranet; hold an annual cyber security awareness week or month.
- Ensure end users are able to recognize potential security issues and know how to report system anomalies and suspicious activities to the organization's designated cyber security team.

Understanding the "current state"

Prior to implementing prevention strategies, healthcare organizations need to determine their current state with respect to assets, security controls, threats and vulnerabilities. Examples of assets include but are not limited to:

a. data/information and their classifications (e.g. personal health information, confidential internal information, regular public information) so that appropriate security protections may be applied based on the classification;

b. applications and software used by the organization along with their purposes; and

c. systems, networks and hardware that support the infrastructure.

Note: The asset assessment should also identify if each asset is supported internally or by a third party (e.g. vendor, health information network provider, etc.).

HIROC recommends taking an inventory of the following:

1. **Assets that need protection from cyber threats**.

2. **Who has access to or uses the systems, technology and data or information** – Can include staff, contractors, independent practitioners, students, volunteers, vendors and suppliers. Users can be an organization's asset as well as a source of threat.

3. **Potential threats or risks to the assets** – Determine potential cyber threats or risks by asset type (e.g. patch updates not done on time can lead to security vulnerabilities).

4. **Currently deployed information security strategies** – These would include physical, administrative and technical information security practices currently employed to protect the identified assets against potential threats or risks.

5. **Cyber industry trends** – Work with your internal cyber expert or external partners to identify information security standards that are recommended versus required.

6. **Potential risks** – Understand how your vulnerabilities can be exploited and identify your risks. Determine which risks are defendable and which risks are not defendable. Identifying defendable and non-defendable risks, existing controls and gaps will further strengthen your organization's ability to manage those risks. These risks can then be managed appropriately at various levels within the organization and reported up to the board.

7. **Existing mitigation strategies and gaps** – Identify current mitigation strategies and map against the assets that they have been designed to ensure the mitigation strategies are appropriate for each asset.

Once the above is completed, you're ready to do an assessment (using internal expertise or a third party) on the potential security threats and current controls to identify gaps. Organizations can use internal expertise or third parties to undertake vulnerability assessments.

Essential information technology processes and solutions

Not all healthcare organizations have access to the budget or the resources needed to employ state-of-the-art technology. Key IT strategies are briefly discussed in this section.

System updates and patch management

Timely review and deployment of system updates and patches is one of the important tasks entrusted to IT services. This process contains several steps including testing, analyzing results, and scheduling and deploying updates to all systems, networks, workstations and devices, which may take a number of days or weeks to complete.

Resource challenges and competing priorities mean that many healthcare organizations struggle to follow a timely system update and patch management process. But, not doing so has been shown to have detrimental effects on an organization. Cyber attackers are able to create and deploy malicious programs that exploit known system vulnerabilities.

Taking a proactive approach means assessing your current security update and patch management process to see if there are any potential areas for improvement. Dedicating the necessary time and resources now could save you money and hours of grief repairing potential damage in the future.

Proper password practices

Traditionally, healthcare organizations have dedicated a lot of time to setting up password rules that are complex and cumbersome for regular users of systems. The National Institute of Standards and Technology (NIST) recommends that organizations should consider usability when setting up a user authentication framework (NIST SP 800-63B).

Summarized below are key recommendations around password practices:

- The minimum length of a password recommended by the NIST is 8 characters
- Encourage allowing users to create passwords that are meaningful phrases and memorable
- Allow passwords as lengthy as the user wants using characters they like, including spaces
- Do not allow users to store hints that are easily accessible by an unauthorized user
- Verify the password against a list of known compromised, commonly used or expected passwords
- Passwords should be stored in a way that they cannot be vulnerable to attacks (e.g. salted and hashed using a suitable one-way key derivation function)
- Use of randomized complex or arbitrary passwords is not recommended
- Use of recycled passwords should be discouraged
- Adopt a strong password policy and procedure, including no sharing of passwords, passwords with at least 3 different types of characters, lock-out after set number of failed authentication or log in attempts, and a password expiry policy
- Follow a stringent process for shared accounts with the person responsible for the account who manages access according to defined/outlined and approval criteria.

Always engage your information security officer and/or privacy officer when setting up or updating your password structures.

Multi-factor authentication

Multi-factor authentication is a security feature that allows users to present two or more credentials to prove their identity to a device, system or network in order to gain access.

To be considered multi-factor authentication, credentials should fall into at least two or more of the following categories:

- Something you know: password, Personal Identification Number (PIN) or secret question/answer;
- Something you have: an access card, authentication application, key or token; or
- Something you are: fingerprint, voice or iris scan.

For example, the use of a password alone to authenticate access to a device, system or network is considered one factor authentication. The use of a password and authentication application in combination is considered two factor authentication, and stronger protection than one factor authentication. The use of a password, authentication application and fingerprint in combination is considered stronger than two factor authentication (NIST SP 800-63-2).

If feasible, consider implementing dual factor authentication for remote access.

Alert! The following limitations and parameters should be noted. Using a password and a PIN for a single log-in attempt is not considered multi-factor authentication, unless the PIN number is randomly generated and given to the user at a point in time through an authentication application on a mobile phone or text message.

Privileged accounts

Administrative access to desktops, laptops, applications, networks, etc. should not be given to regular users. Users that require administrative access should only use these privileged accounts when absolutely necessary. The principle of least privilege should always be followed when providing administrative access to users. The list of users with administrative access should be regularly reviewed, validated and approved by the senior manager accountable for information security.

Detecting cyber security incidents early on

Self-detection of cyber incidents is not easy and most Canadian healthcare organizations do not have the necessary resources required to install, monitor and manage technical monitoring tools such as intrusion detection and intrusion prevention systems (IDS and IPS). For that reason, we suggest working with internal and external IT experts to determine acceptable detection methods that can be most suitably employed at your organization based on the size and type of organization, risks to assets and resource availability.

Other key controls and mitigation strategies

Following are additional key controls and mitigation strategies for your consideration:

- E-mail and web browser protections to identify and prevent spam emails, malicious attachments, executable files and malicious websites from getting to the end user
- Appropriate firewall, antivirus/antimalware solutions to protect systems and networks
- Disabling the Microsoft Office macros as they often contain hidden malicious codes
- Necessary processes to collect, retain and assess system and network logs to identify potential issues early on (e.g. access logs, system activity logs, error logs, etc.)
- Appropriate encryption and cryptography solutions to protect transmission of sensitive data/information, including personal health information, personal information, etc.
- Privacy impact assessment (PIA) and/or threat and risk assessment (TRA) reviews when implementing new or changed processes, systems or other technology solutions that will handle personal information or personal health information. PIA and TRA are risk management tools used to identify risks associated with existing or new information systems, processes, programs, etc. This is a continuous process and should be reviewed regularly as changes are made to processes, systems and technology
- If feasible, annual penetration tests and vulnerability assessments are undertaken through a third party vendor. This can help facilitate identification and management of vulnerabilities.

For many organizations, the most challenging part of the incident response process is accurately detecting and assessing possible cyber security incidents – determining whether an incident has occurred and, if so, the type, extent, and magnitude of the program.

(Creasey, 2013, p. 32)

Protecting the premises

Strong physical security is important to protect against unauthorized access to your organization's information systems and technology assets including data centres, backup storage and computers/laptops with sensitive information, servers, etc. Access to physical locations housing these sensitive systems should be restricted to authorized employees only. Access to such areas should be closely monitored and access logs should be regularly reviewed. It may be beneficial to monitor access through video surveillance. The lead responsible for physical security of the premises should review the list of employees and roles semi-annually to ensure only the authorized individuals (e.g. employees, vendors, contractors) have access to sensitive areas. A stringent termination process should also be followed to ensure that the terminated individual's access is removed and ID cards are taken away.

> *Cybersecurity risk management programs should emphasize addressing vulnerabilities which may permit the unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient, and may result in patient harm.*
>
> (Food and Drug Administration (FDA), 2016, p. 13)

Medical devices and cyber security

As medical devices become increasingly sophisticated in their technology and more integrated with the healthcare organization's other devices, systems and networks to facilitate patient care, the risks of cyber security incidents increase.

Failing to protect and safeguard medical devices from cyber security incidents can have detrimental effects on patient safety. Here are some important risk management recommendations around cyber security of medical devices:

- Take inventory of all medical devices that are in use or may potentially be in use and note relevant information such as their connectivity to the network, Wi-Fi status, software version, date of last update, etc.

- Monitor all medical device notifications and recalls that are applicable from trusted sources and governing bodies; take action on alerts and recalls in a timely manner.
- Review updates and patches issued by manufacturers and apply them to affected devices in a timely manner.
- Monitor and report on medical device-related incidents to facilitate early identification of potential vulnerabilities that can be exploited by cyber criminals.
- Identify vulnerable medical devices with outdated software versions and consider disconnecting and/or disabling them from the networks and the internet.
- Encrypt all communications between medical devices and other systems and devices connected through unsecure Wi-Fi or networks (e.g. radio frequency communication).
- Monitor cyber security information sources (e.g. Canadian Cyber Incident Response Centre) to identify vulnerabilities early on.

Medical Device Case example: Johnson & Johnson (J&J) Insulin Pumps

In the fall of 2016, J&J released a cyber security warning on their Animas OneTouch Ping insulin pumps. The insulin pump is sold with a wireless remote that controls the insulin dosage delivered by the pump. The pump can be worn under the patient's clothing. Wireless communications between the pump and the remote are not encrypted.

Risk factor: According to J&J, "a person could potentially gain unauthorized access to the pump through its unencrypted radio frequency communication system" (Animas, 2016, p. 1). Communications can easily be hacked and the pump can be forced to deliver unsafe insulin doses or injections, which can lead to devastating patient safety outcomes.

Outcome: J&J notified approximately 114,000 patients who used the device in the United States and Canada. Although J&J believed that the risk of cyber attack was low, they provided steps that patients can take to minimize the risks (e.g. limit the maximum insulin dose, discontinue using wireless remote control). J&J is working to ensure that other products do not have the same vulnerability.

Vendor management and third party risks

Anyone who has access to your systems, infrastructure and key data could be a source of compromise. You must have strategies in place to minimize the risks posed by vendors, partners and third party providers.

Consider taking these proactive steps:

- Ensure the vendor's security practices are strong and meet acceptable information/cyber security standards (e.g. NIST, ISO 27001, SOC 2)
- Contractually obligate the vendor to continue to maintain accepted security standards and to provide at their expense an applicable security report or evidence prepared by an independent, reputable firm each term (for a specified consecutive defined period). This will help you assess your vendor's commitment to security standards on a regular basis
- Contractually require the vendor to notify you of all security breaches and data breaches within a specified time period from the occurrence date
- Ensure the vendor's breach response plans are inclusive and meet the acceptable standards for healthcare organizations
- Contractually require the vendor to comply with all privacy legislation/regulations
- Contractually negotiate the right to conduct an on-site visit and conduct other inspections such as review of log files, policies/procedures, etc. to confirm security controls. This right is more likely to be exercised with small vendors who do not meet required cyber security standards
- Where feasible, periodically or annually evaluate vendor agreements to ensure they are appropriate and relevant.

Cloud service providers

The widespread use of cloud services is raising questions about the risks associated with third party-managed cloud services. They pose a legitimate risk if a service provider is non-compliant with legislated and regulated privacy and security requirements.

HIROC encourages healthcare organizations to consult with IT professionals and legal services to assess privacy and security risks – consider the location of data centres and jurisdiction, unauthorized use and processing of data by the cloud service provider and inappropriate disclosure of information.

From a privacy standpoint, the location(s) of data centres should be considered before moving personal health information to a cloud service provider.

Before even starting a service relationship with a cloud service provider, you need to do your due diligence to evaluate and confirm the security measures that are being taken. Ask to speak to reference customers that are peer Canadian organizations and verify the following evidence:

- SOC 2/ISO 27001:2013/ISO 27018/SAE16 or similar audit or certification reports;
- completed self-assessments (e.g. PIA, TRA, Cloud Service Alliance Consensus Assessment Initiative Questionnaire).

At minimum, here are some questions to ask a potential cloud services provider:
• How would the cloud service provider detect, contain and remediate cyber breaches?
• How is the data stored, transferred and processed?
• Is the data stored on servers outside of Canada and, if so, where?
• How will you be able to repatriate data if the cloud service provider goes out of business, is acquired, or is absorbed?
• If the cloud service provider is taken over by another provider, who has rights to the data? What are the terms and conditions?
• What protections (encryption, access control, etc.) are in place to protect the information?
• What is the data destruction schedule and process?
• Are backups of the system or data conducted? If so, understand where the backups are stored, how often the backups are generated and destruction details.
• Does the service provider support single tenant architecture? If only multi-tenant architecture is supported, how will the organization's data be protected against unauthorized access?
• What sort of data migration support will be provided if the healthcare organization wants to migrate to another cloud provider or internal system?
• What type of auditing and logging capabilities are in place and how can they be accessed by the healthcare organization of the cloud service provider?
• What cyber and privacy breach incident management protocols are in place? Understand the breach notification process and timeframe; healthcare organizations should be notified of breaches as soon as reasonably possible.

Finally, review service contracts and service level agreements (SLAs) to verify compliance with applicable regulations and the organization's privacy and security standards/practices. One check is never enough – make it a habit to review SLAs regularly to monitor the service provider's compliance with commitments and requirements.

> *Despite the opportunities for improved operational efficiencies and services, and for reduced overhead and other costs, cloud computing introduces its own privacy, security and compliance risks that must be addressed.*
>
> (Information and Privacy Commissioner of Ontario, 2016, p. 5)

Select and follow a standard cyber security framework

As a healthcare organization, you can greatly minimize your risk of a cyber exposure by staying on top of existing knowledge and standards. If feasible, you should consider selecting and following a cyber/information security framework.

There are definite advantages to doing this – adopting an industry standard security framework ensures that guidelines are appropriately followed and cyber risks are identified, tracked and managed in a systematic and standardized manner.

Available cyber security frameworks and resources:

- International Organization for Standardization, ISO/IEC 27001: 2013 and ISO/IEC 27002 – Information Security Management Systems Standards
- The Centre for Internet Security (CIS) Critical Security Controls, SANS, 2016
- Fundamentals of Cyber Security for Canada's Critical Infrastructure Community, Public Safety Canada, 2016
- National Institute of Standards and Technology, U.S. Department of Commerce, Cybersecurity Framework, 2016
- Common Security Framework (CSF), Healthcare Information Trust Alliance (HITRUST), 2014
- Cyber Resilience Review (CRR), United States Computer Emergency Readiness Team (US-CERT), 2016

5 Cyber Security Incident Response and Business Continuity Plan

Avoiding a cyber crisis often comes down to properly managing a cyber incident before, during, and after it unfolds.

(Deloitte, 2016, p. 2)

With cyber security incidents becoming a common occurrence in the Canadian healthcare environment, having a well-established and verified cyber security incident response plan has become an utmost necessity. Not only will this plan minimize the losses associated with cyber security incidents, but its defined steps and checklists will keep you focused during a stressful event.

An effective and comprehensive cyber security incident response plan should have the key elements highlighted below:

1 Who is on your Incident Response Team

The plan must identify the multi-disciplinary cyber security Incident Response Team members, including key internal and external stakeholders:

- an incident response facilitator/lead
- senior management representative
- information systems and security experts
- legal, privacy, human resources, communications and patient representatives.

Depending on resource availability, partner with external organizations and vendors to identify experts who may become part of the Incident Response Team. Ensure the team members' after-hours contact information is kept up-to-date.

If cyber security incident response activities require client-solicitor protection, then consider involving external legal firms. Client-solicitor protection may not apply to basic facts of the incident, however, the investigation and associated sensitive information may be protected. **Upon learning of an incident, we urge you to contact HIROC early on for the appropriate legal assistance**.

2 Backups and restoration

Backups are an essential component of business continuity and system recovery. In fact, other than user awareness and training, well-thought-out backups have proven to be the strongest cyber security incident recovery strategy against prevalent malware and ransomware attacks. At minimum, ensure daily backups of all critical systems are taken and maintained offline and offsite to protect them from a potential breach. Healthcare organizations should also periodically test restoring the data from the backups to validate the backup/restoration process and ensure integrity of the data.

3 Clearly articulate your system downtime policy

The goal of a system(s) downtime protocol is to minimize operational loss and ensure continuity of patient care. Ensure system downtime procedures are clearly articulated in associated policy and checklists and are communicated to all healthcare staff, including students, volunteers, contractors, independent practitioners and residents. HIROC recommends extensive testing of the system downtime protocol involving frontline staff to identify potential gaps and facilitate improvements to the plan. Playbooks with a compilation of associated protocols, policies and best practice guidelines for each risk can be created to help with downtime activities for each team. The playbooks should be reviewed and updated regularly.

4 Create a Communications Plan

Communication following a cyber security incident is crucial to ensure continuity of operations and containment of the harmful situation. The usual modes of communication might be out of service and so the plan should outline alternate vehicles for communicating with the team. The plan should also include a notification protocol for the frontline staff who are on-site and off duty, senior leaders, board members, patients/family members and the community.

Vendor contact information should be a component of your Communications Plan.

Prepare a media response kit and establish a designated individual/team who will be prepared to speak to the media. Senior leaders and board members should also be appropriately trained on media engagement in the event they are called on to issue a response or talk to the media directly.

Monitor social media for negative press and harmful activities so the organization can respond appropriately.

5 Identify legal obligations

Data loss is a common occurrence of cyber security incidents. If data is lost, a privacy breach protocol needs to be commenced by the privacy breach response team. The organization's privacy breach protocol should identify provincial/territorial and federal legislation and regulations governing the various data stored in systems. The type of data and the governing legislation will determine what type of data breach notifications should be put in place within the mandated or reasonable timeframe (e.g. notification to patients, regulatory bodies, and the applicable privacy commissioner's office).

6 Review your insurance policy

Not all financial losses associated with cyber incidents are covered under general liability or property policies. Certain situations would need a separate cyber risk policy to provide coverage. As a good risk management practice, HIROC encourages healthcare organizations to undertake a review of the available coverages and limits to ensure they are appropriate and adequate. Part of this review would include discussions with your insurance provider or broker.

Alert! HIROC recommends having early notification and claims reporting procedures in place to inform your insurance provider of any cyber incidents or losses. Early notification can go a long way to resolving the incident in a cost-effective manner.

6 Immediate Management of Cyber Security Incidents

Engage your insurer early on to secure coverage, resources, expertise and support.

(HIROC)

Regardless of how meticulously an organization may have planned for a cyber security incident, panic strikes upon discovery of an incident. The following types of activities should take place immediately following the discovery of an incident (i.e. within the first 48 hours):

1. Commence implementation of the cyber security incident response plan:
   - Contact the incident response team members and ensure everyone knows their responsibilities
   - Ensure appropriate staff members outside of the response team are notified of the incident.

2. Take appropriate steps to detect, identify, contain, and eradicate the situation:
   - Detect the actual incident using self-detection strategies or external analysis
   - Identify the affected systems, applications, networks, servers, devices, etc.
   - Try to isolate and contain the incident by disconnecting the affected systems from the applicable network immediately;
   - Initiate strategies to protect the unaffected systems, applications, networks, etc.
   - Learn as much as possible about the incident, attack vector, and root cause. If possible and appropriate, eradicate the situation (e.g. by removing the malicious virus or malware, addressing the vulnerability of breach);
   - Engage external partners and experts as required (e.g. insurer, cyber expert, forensic incident investigator, law enforcement, etc.)

3. Document all facts, findings, activities and outcomes from incident detection onwards.

4. Maintain continuous communications with all involved and affected parties, including frontline staff, independent practitioners, management, partners, board members, and patients/family members.

5 Activate your communications team and communications plan; carefully monitor and manage social media activities and media releases.

6 Engage your insurer early on to secure coverage, resources, expertise and support.

7 Begin system recovery activities by evaluating the incident to determine the recoverability of the affected system(s), application(s), and network(s). Test the recovery plan by restoring a small portion of the affected system(s) and adjust the recovery plan as needed. If successful, implement recovery activities according to the developed plan.

8 If you decide to protect the details of the investigation of the cyber security incident, involve external legal counsel early on. Prior to engaging external legal counsel, check with your insurer to confirm coverage.

7 Post-Cyber Security Incident Recovery and Management

HIROC recommends healthcare organizations consider reporting verified and confirmed criminal activities to law enforcement agencies in order to protect the healthcare system as a whole.

(HIROC)

Once the immediate threat has been eliminated or mitigated, the focus shifts from responding to the cyber security incident to protecting and recovering normal operations. Sufficient attention and resources should also be directed on follow-up cyber security activities with a minimal lapse in time. This will involve:

- Investigating the cyber security incident thoroughly by undertaking a look-back and forensic review to understand the magnitude of the breach or incident;
- Instigating the organization's privacy breach protocol if a privacy breach was discovered. The privacy breach protocol will require notification to affected parties, including notification to the applicable privacy commissioner;
- Identifying and understanding the root cause of the cyber security incident;
- Quantifying the financial losses and operational losses;
- Understanding the implications related to reputation;
- Conducting a post-incident review and any necessary adjustments to the cyber security incident response plan based on first-hand experience and analysis of the event;
- Briefing senior management and board members about the incident and follow-up actions;
- Reporting on the incident and lessons learned to healthcare providers.

Why reporting is critical

Fear of reputational loss and associated stigma attached to the incident can occasionally result in the victims of cyber security incidents not reporting the incident to authorities. They may also fear secondary attacks if they publicize the initial incident. It is vitally important the affected healthcare organization report the incident to other key partners and stakeholders who may be affected by the incident.

Alert! HIROC recommends healthcare organizations consider reporting verified and confirmed criminal activities to law enforcement agencies in order to protect the healthcare system as a whole. It may also be beneficial to report such incidents to specialized national bodies such as the Canadian Cyber Incident Response Centre.

8 Final Thoughts

The real benefit of a strong cyber risk management program is the ability to reduce or deflect losses associated with cyber security events.

(HIROC)

No one is immune to a cyber security incident and at this point in time, healthcare organizations of all sizes and types are particularly vulnerable. A combination of administrative, logical and technological solutions needs to be employed by healthcare organizations – and even when those steps are employed, your organization must remain vigilant about keeping protective measures current and viable. The first step towards building cyber resiliency for healthcare organizations is knowing your vulnerabilities and cyber posture.

The real benefit of a strong cyber risk management program is the ability to reduce or deflect losses associated with cyber security events.

To understand your HIROC insurance policy or learn more about cyber security, please contact us at inquiries@hiroc.com.

References

- Amazon Web Services. (2017). Amazon web services: Risk and compliance.
- Animas Corporation. (2016). Important Information about the cybersecurity of your OneTouch ping insulin infusion pump.
- Bartock MJ, Cichonski JA, Souppaya MP, et al. (2016). Guide for cybersecurity event recovery. NIST Special Publication 800-184.
- Cloud Security Alliance (CSA). (2016). Consensus assessment initiative questionnaire. V3.0.1 (12-5-16 Update).
- Creasey J. (2013). Cyber security incident response guide. CREST.
- Deloitte. (2016). Cyber crisis management: Readiness, response, and recovery.
- Finkle J. (2016). Insulin pumps could be hacked warns Johnson & Johnson. Global News.
- Food and Drug Administration (FDA). (2016). Postmarket management of cybersecurity in medical devices: Guidance for industry and food and drug administration staff.
- Freedman BJ. (2017). Cyber risk management guidance for corporate directors. Borden Ladner Gervais LLP (BLG).
- Freedman BJ. (2016). Data security Incident Response Plans – Some Practical Suggestions. BLG.
- Freedman BJ. (2017). Important changes to password best practice guidance. BLG.
- Freedman BJ. (2017). Legal Privilege for Data Security Incident Investigation reports. BLG.
- Grassi PA, Fenton JL, Newton EM, et al. (2017). Digital identify guidelines: Authentication and lifecycle management. NIST Special Publication, 800-63B.
- Grassi PA, Garcia ME, Fenton JL. (2017). Digital identity guidelines. NIST Special Publication 800-63, 3.
- Federal Bureau of Investigation (FBI). (2016). How to protect your networks from ransomware.
- Health Information Trust Alliance (HITRUST). (2016). Healthcare sector cybersecurity framework implementation guide.
- Investment Industry Regulatory Organization of Canada (IIROC). (2015). Cybersecurity best practices guide for IIROC dealer members.

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). (2016). Animas OneTouch ping insulin pump vulnerabilities. Advisory (ICSMA-16-279-01).
- Information and Privacy Commissioner of Ontario. (2016). Protecting against ransomware. Technology Fact Sheet.
- Information and Privacy Commissioner of Ontario. (2016). Thinking about clouds? Privacy, security and compliance considerations for Ontario public sector institutes.
- Magee K. (2017). Practical cyber security governance: A guide for hospital boards and executives.
- National Institute of Standards and Technology (NIST). (2016). Back to basics: Multi-factor authentication (MFA).
- NIST. (2014). Framework for improving critical infrastructure cybersecurity.
- Public Safety Canada. (2016). Fundamentals of cyber security for Canada's critical infrastructure community.
- Public Safety Canada. (2017). Ransomware – petya. AL17-008.
- Pricewaterhouse Coopers (PwC). (2014). Cyber security crisis management: A bold approach to a shadowy nemesis.
- Salazar D. (2016). Cloud security framework audit methods. SANS Institute InfoSec Reading Room.
- United States Computer Emergency Readiness Team (US-CERT). (2016). Ransomware and recent variants. Alert (TA16-091A).
- US Department of Homeland Security. (2016). Cyber resilience review (CRR): Self-assessment package.
- Williams C. (2016). 5 action lists for a cyber crisis in your hospital. Hospitals & Health Networks (H&HN).

Appendix: Ransomware Protection

A ransomware attack can lead to temporary or permanent loss of access to critical information systems which can lead to operational destruction/loss, financial loss, reputational loss, etc. The following checklist summarizes important risk management considerations that will help protect against ransomware attacks:

- Know your current state and identify your potential vulnerabilities. Following are a few items to consider.
    - Take inventory of all systems, computers, servers, operating systems, applications (including versions), other hardware that support the infrastructure, etc.
    - Take inventory of data/information that need protection and their classifications.
    - Are there any devices or computers that are running outdated and using unsupported operating systems/ applications? If so, could you isolate those from your regular network or take them offline?
    - How often do you apply upgrades and patches to your systems? When security patches are released, how quickly do you deploy them?
    - How often do you provide information security and privacy training to staff members (including volunteers, students, residents, independent practitioners)? How do you monitor compliance?
- Ensure a robust data backup and recovery strategy is in place - run drills to ensure the backup and recovery strategy is adequate and complete. Ensure backups are not easily accessible from the local network.
- Keep up-to-date with all patch releases, security updates, software/system upgrades, etc. and consider reducing the timeline for updating applications and operating systems.
- Ensure you have up-to-date antimalware or antivirus solutions in place and that these are set to automatically conduct regular scans.
- Scan, filter and block/remove executable files that are attached to incoming and outgoing e-mails to prevent them from reaching users.

- Adopt least privilege access control permissions for files, directories, and networks. Oversee the management of privileged accounts closely. No user should have administrative access and those privileges should only be used when it is absolutely necessary.
- If feasible, run annual or semi-annual penetration tests to identify and address your vulnerabilities.
- Provide role-based cyber security training and education to staff, including identification of malicious links, social engineering attacks, ransomware attacks, etc.
- Follow best practice recommendations to protect network infrastructure and related components and devices, including segregated networks and functions, hardening of network devices, secure access to infrastructure devices, etc.
- Ensure a strong and validated incident response and business continuity plan is in place so that remediation efforts can be efficiently deployed.
- Subscribe to reliable cyber risk alerts and industry bulletins (e.g. Canadian Cyber Incident Response Centre).

Head Office
4711 Yonge St, Suite 1600, Toronto, ON M2N 6K8
Tel: 416.733.2773 | Fax: 416.733.2438 | Toll Free: 1.800.465.7357 | Fax: 1.800.668.6277
riskmanagement@hiroc.com

Western Region
1200 Rothesay St., Winnipeg, MB R2G 1T7
Tel: Tel: 204.943.4125 | Fax: 204.949.0250 | Toll Free: 1.800.442.7751
westernregion@hiroc.com

www.hiroc.com

HIROC is Canada's leading provider of healthcare liability insurance. As a not-for-profit, we partner with our subscribers to provide innovative insurance and risk management solutions that help them reduce risk, prevent losses and improve patient safety.