Canadian Insurance Services Regulatory Organizations

Cybersecurity Readiness

Preamble

The use of technology by regulated insurance intermediaries[1] (“intermediaries”) to collect, store and use information for the purpose of selling or servicing insurance products comes with the responsibility of safeguarding it from unauthorized access.

This publication provides general information for intermediaries on cybersecurity practices to safeguard confidential information, increase their resiliency to cybersecurity incidents and properly respond to such incidents when they occur. While there are cybersecurity practices and risk controls that may apply to everyone, some are meant to be implemented in a manner appropriate to the size and structure of each organization.

Cybersecurity refers to any practice that safeguards the confidentiality, integrity, and availability of business, employee, and customer data using computer systems. Breakdowns in these safeguards are referred to as incidents. They may be the result of a human error, a system not working properly, or a deliberate and calculated intrusion such as a cyber attack. Being proactive in implementing appropriate measures is key to preventing cyber incidents that could compromise or lead to the theft of client information and to mitigate its impact on both the intermediaries and their clients.

As cyber incidents, and specifically cyber attacks, become more frequent it is important that all intermediaries assess their data and technology systems to determine what data may be attractive to cybercriminals and what systems may be vulnerable to cyber attacks. They should review their cybersecurity practices and take appropriate measures to address or mitigate any identified risks.

Intermediaries should consider the assistance of a cybersecurity professional who can help with the assessment and review of their current practices and provide specific advice based on their needs. They should also ensure that the cybersecurity measures implemented are compliant with applicable privacy legislation.

Intermediaries should stay up to date with the continuously evolving cybersecurity environment and consider cyber liability insurance as an option to help them in their effort to achieve cybersecurity readiness.

---

[1] **Definition of Regulated Insurance Intermediary:** Intermediary is given broad meaning, and will differ based on the applicable definitions within different jurisdictions across Canada. It encompasses adjusters, agents, brokers and representatives, as well as business entities that distribute insurance products and services, including managing general agencies and third-party administrators. It also applies to all distribution methods, including over the internet.

Cybersecurity Readiness

To achieve cybersecurity readiness, intermediaries should establish a strategy that is adapted to their organization and the risks relevant to their business. Here are suggestions to assist intermediaries in achieving cybersecurity readiness.

1. Make cybersecurity a priority

Building a culture of cybersecurity within the organization and ensuring that the appropriate expertise and resources needed are made available is key to achieving cybersecurity readiness.

Organization

- Give someone the responsibility for overseeing and reporting on the organization's cybersecurity risks and ensure this person is supported and has access to the necessary resources, including access to a cybersecurity professional's advice and assistance when necessary.
- Develop policies and procedures on cybersecurity practices for everyone in the organization to follow.
- Ensure everyone within the organization is aware of their role and responsibilities with regard to the organization's cybersecurity policies and procedures.
- Promote awareness and provide regular training to everyone within the organization on good cybersecurity practices, preventing cyber incidents and knowing how to respond when they occur.
- Instill an approach to cyber incident response that makes everyone feel safe to report incidents. The objective should be focussed on understanding and mitigating the incident as quickly and effectively as possible.
- Inquire about how cyber liability insurance can help in the organization's cybersecurity readiness. Obtaining cyber liability insurance, where reasonably accessible, could help organization identify risks, assist with cyber readiness, provide access to technical resources and help cover costs in response to cyber incidents.

Individual

- Attend cybersecurity training and understand and follow the organization's policies and procedures on cybersecurity.
- Stay alert to cyber threats such as suspicious e-mails, text messages or phone calls.

2. Know what client information and technology to safeguard

Knowing what client information is held during the course of the organization's business activities, and how it is being stored, is fundamental to determining what cybersecurity measures should be put in place to facilitate a response to a cyber incident.

Organization

- Identify all computing devices used during the course of business activities, noting:
  - The type of device (e.g. desktop, laptop, tablet, smartphone, smartwatch, or USB keys) and details of each device (e.g. what they are used for, model, serial number)
  - Their user(s) (e.g. administrators, IT personnel, employees, intermediaries, etc.
- Know what information the organization holds electronically, where it is stored and consider the importance of having back-ups and storing it on off-site servers, including digital cloud storage.
- Identify the level of sensitivity of the information held by the organization and its importance to the organization's ability to operate.
- Understand how the electronic records and data can be accessed through the organization's network including:
  - What devices, software or applications are connected to the organization's network (e.g. computing devices, printers, routers, servers) and how they are connected.
  - How the organization's network is connected to the Internet.
  - What electronic records or data can be accessed through the organization's network and who has access to it.

Individual

- Use the device provided by the organization only for authorized work-related activities and do not allow others to use the device or access the organization's network, electronic records, or data.
- Avoid use of personal devices to access the organization's network or, if permitted by the organization, only use in accordance with the policies and procedures.
- Avoid use of public Wi-Fi and unsecured networks when accessing sensitive information. The use of a virtual private network (VPN) could be a safer solution.

3. Identify Cyber risks arising from the organization or outsourcing activities to third-party service providers

Identifying the relevant risks to the confidentiality, integrity, and availability of client information, technology risks arising from access granted to staff, management, or third-party service providers or the potential risk of a cyber attack is fundamental to determining what cybersecurity measures should be put in place to facilitate a response to a cyber incident.

Organization

Risk pertaining to the organization

- Continuously assess the risk of cyber incidents to the organization's computer devices, electronic records and networks, estimate the likelihood of such incidents occurring and understand the business impact of these incidents.

- Periodically review who has access to the organization's computer devices, electronic records and data and determine what access is necessary for them during the course of their business activities, while ensuring to remove any access no longer required.

Risk pertaining to third-party service providers

- Assess third-party service providers' cyber security practices, as intermediaries are responsible for any services outsourced to third parties.

- Verify third-party service providers through reference checks, web searches or other means and ensure they have adequate cybersecurity practices in place that are aligned with the intermediary before entering into an agreement with them.

    - Ensure that the agreement entered into with third-party service providers considers the confidentiality of client information and security of the organization's computer systems and networks.
    - Contracts should consider where the third party's responsibility for cybersecurity, in the operation of the service, end and where the organization's responsibility begin.
    - Incorporate a third-party cyber breach response plan to cyber attacks. Include third-party points of contact and set up a coordinated plan with the third party.
    - Require third parties to immediately notify the organization of cybersecurity incidents involving unauthorized access to client information or the organization's systems.

- Regularly monitor third party cyber security readiness as part of your risk mitigation strategy.

Individual

- Inform the person within the organization responsible for overseeing cybersecurity if you become aware of access that you do not need.

- Follow the organization's policies and procedures on interacting with third-party service provider personnel, granting access to the organization's computer systems or client information.

4. Implement adequate cybersecurity measures

Implementing appropriate measures is essential to adequately prevent or mitigate identified cyber risks, such as monitoring threats or unauthorized access to client information and technology and adjusting the cybersecurity strategy accordingly.

Organization

- Control access to electronic records, data and the organization's network:
  - Restrict and/or monitor the collection, storage, transfer, and use of sensitive client data, including restricting or prohibiting the use of external devices such as USB keys.
  - Limit and monitor the number of employees with privileged access to the organization's networks and information, ensuring that access is limited only to what is required to carry out an employee's duties.
  - Control and limit physical access to the organization's office(s)/building(s) to only the appropriate employees, including key card access, ID badges and visitor access.
  - Monitor the network for unusual traffic or unauthorized access.
  - Enable multi-factor authentication (MFA) to provide an additional layer of security.
- Ensure secure disposal or recycling of computing devices, electronic records, and data.
- Catalog and back-up client information to facilitate recovery should the information be lost or severely altered.
- Ensure that the organization's operating systems and networks are up to date and properly patched, and that an appropriate update schedule is in place and followed.
- Test the organization's computer systems and networks for vulnerabilities.
- Consider cyber liability insurance as it may help with the organization's resiliency to cyber attacks or provide access to technical resources.

Individual

- Understand that you are the first line of defense against cyber incidents, therefore always be alert of your actions and potential causes of a cyber incident.
- Follow the organization's policies and procedures and apply cyber safety practices in your day-to-day activities such as:
  - Ensure your devices and applications are always up to date.
  - Use a strong and unique password for each device or application used and do not share it with anyone.
  - Secure your devices when you are not using them by locking your session.
  - Avoid using your work devices for personal use.
  - Do not use text messages or e-mails to send personal or sensitive information.
  - Do not download applications to your work devices without your organization's authorization.
  - Do not use your work devices to navigate unsafe or unrelated websites.
  - Do not open links or attachments from unknown or suspicious sources.

5. Detect and respond to cyber incident

Having a plan to detect, evaluate and respond to cyber incidents is key to ensuring that staff, management and service providers are aware of the actions they must take to detect cyber incidents or respond to them when they occur.

Organization

- Invest in intrusion detection systems and implement regular monitoring, such as antivirus systems and activity logging.
- Develop a written cybersecurity incident response plan to protect client information, minimize service disruption, help with incident mitigation, and document incidents (see Cyber Incident Response Plan below).
- Appoint a response team composed of staff and management responsible for handling cyber incidents and seek external expertise when needed. The goal of the response team is to minimize the impact and the time it takes to resolve an incident.
- Establish a communication protocol in writing to guide the response team in the evaluation of the information that may need to be shared with stakeholders, external parties, regulators, or law enforcement and ensure the information is communicated effectively and in a timely manner. Intermediaries should be aware of their obligation to report incidents or take other action under applicable privacy legislation.
- Test the cyber incident response plan for effectiveness and make necessary adjustments.
- Investigate the root cause of a cyber incident, evaluate the risk of the incident reoccurring and implement the measures that may be necessary to prevent or mitigate its reoccurrence.

Individual

- Cybersecurity is everyone's responsibility, as such it is important to be aware of any actions that may cause a cyber incident and do not hesitate to report it immediately.
- Be proactive in detecting potential cyber threats and incidents, report any suspicious activity and follow the organization's procedures. For example:
    - Notifying the organization's appropriate or designated cybersecurity personnel.
    - Powering off the device.
    - Noting the time and date of the incident, what programs were running and description of the incident.

Elements to include in a Cyber Incident Response Plan

Investigation	Investigate the nature and the extent of the cyber incident and it's impact on the organisation and the clients.
Mitigation	Apply mitigation measures such as suspending access to impacted client information or technology. This includes identifying vulnerabilities, correcting them and restoring affected systems or lost information as well as implementing safeguards.
Evaluation	Evaluate whether the incident causes client information or technology to be unavailable for a significant period of time and whether it triggers the business continuity plan.
Communication	Communicate with stakeholders affected by the cyber incident, applicable regulators or law enforcement and determine what steps need to be taken to mitigate harm to affected stakeholders.
Documentation	Document the steps to uncover and respond to the cyber incident while ensuring to preserve any evidence and documentation detailing the analysis of the incident. Document when systems are back online and fully functional and when the cyber threat is no longer present.