CAPSA/ACOR

Canadian Association of Pension Supervisory Authorities
Association canadienne des organismes de contrôle des régimes de retraite

CAPSA Guideline

Cyber Risk for Pension Plans

Date: June 9, 2022

Table of Contents

1. INTRODUCTION

Background

As pension plans increasingly rely on technology, the Canadian Association of Pension Supervisory Authorities (CAPSA) is addressing cyber risk in order to support plan administrators in keeping plan assets safe and protecting the rights and interests of the plan beneficiaries.

Pension plan administrators and their third-party service providers control large amounts of financial assets as well as personal and confidential data, which can make them an attractive target for criminals, cyber-attacks, and fraud. Cyber breaches have far-reaching consequences on plan beneficiaries and their families, as well as reputational damage to the parties involved.

A pension plan must be administered and its assets invested by the plan administrator with the care, diligence and skill required of a fiduciary. Steps therefore need to be taken to protect plan beneficiaries and plan assets against the risk of cyber-attacks. This is a key risk that all plan administrators and their agents need to be aware of and actively monitor and manage.

CAPSA's discussion of cyber risk builds upon CAPSA's foundational guidance on plan governance (CAPSA Guideline No. 4) and risk management (CAPSA Guideline No. TBD) by focusing on the specifics of cyber as a key risk in pension plan management.

[Placeholder - further language to be inserted regarding proportionality]. A pension plan should implement the expectations in this Guideline commensurate with its size; the nature, scope and complexity of its operations; and risk profile.

What is Cyber Risk?

Cyber risk is the risk of financial loss, operational disruption or reputational damage from the unauthorized access, malicious and non-malicious use, failure, disclosure, disruption, modification, or destruction of information technology systems and/or the data contained therein. In the context of a pension plan, cyber risk includes both internal risks (e.g., disgruntled employees or a lack of controls on access) and external risks (e.g., hacktivists, state-sponsored threat activists or cybercriminals).

Examples of cyber risk include:

- malicious software (also known as malware);
- phishing emails (i.e., acquiring sensitive data through a fraudulent solicitation, in which the perpetrator masquerades as a legitimate business or reputable person);
- hacking (i.e., obtaining unauthorized access to networks, computer systems and digital devices);
- inadvertent information disclosure (e.g., the accidental leaking of private member information).

Key Takeaways from this Guideline:

- Cyber risk is a key risk for all plans, regardless of plan size or characteristics. It should be regularly reviewed and assessed to ensure appropriate controls are in place to allow the plan to manage the risk. Cyber risks are complex and evolving and require a dynamic response.
- In discharging their fiduciary responsibilities, plan administrators should ensure that the plan has access to the required skills, expertise and/or training to understand and manage cyber risk.
- Roles and responsibilities relating to cyber risk should be clearly defined, assigned, and understood, including with respect to any activities delegated to third-party service providers (and all applicable subcontractors).
- Plan administrators should have a strategy in place for responding to and reporting cyber incidents.

2. INTEGRATING CYBER RISK IN GOVERNANCE AND RISK MANAGEMENT

CAPSA's expectation is that plan administrators will incorporate the management and monitoring of cyber risk into the same governance and risk management frameworks used to assess and respond to other material risks to the plan.

Considerations for Integrating Cyber Risk

To effectively integrate cyber risk, plan administrators may want to keep in mind some of the characteristics that can make cyber risk challenging. This includes the evolving nature of technology, cyber practices, and data standards, the need for specialized technological expertise and training, as well as the sensitive nature of information retained by plans that may have long-term implications in the event of disclosure (e.g., identity theft) and which can lead to loss of trust and reputational risk.

In integrating cyber risk into the plan's governance and risk management frameworks, plan administrators should consider questions such as those set out in Appendix A.

Examples of controls that may be relevant to cyber risk management activities are set out in Appendix B. As for any other risk, appropriate controls vary depending on the nature, potential impact, and likelihood of the risk at issue. The basic process of risk identification, prioritization, management, and monitoring should be followed for all risks, including cyber risk.

Third-party Contracting

Plan administrators should be aware of CAPSA's general expectations that apply whenever plan administrators delegate part of the administration and investment of the pension fund to third-party service providers. With respect to cyber risk, pension plan administrators should be aware and understand the following with respect to their third-party service providers:

- Cybersecurity posture[1] and cybersecurity capabilities.
- Information technology risks and controls.
- Certifications and seals of compliance with applicable standards.
- Process of how and when the plan administrator would be informed of an incident at the third-party (and applicable subcontractors), its impact on plan beneficiaries and assets, and the frequency of updates throughout the incident.
- Process to provide updates on cyber risks and guidance on cyber threats to relevant parties.

Pension plan administrators should ensure that all third-party service providers have implemented sufficient controls to protect plan beneficiary data and plan assets. Cyber risk should be an active consideration in the selection of a third-party service provider and suitable provisions should be included in contracts.

3. CYBER RISK – PLANNING FOR THE INCIDENT AND RESPONSE

Cyber risks generally involve an "incident" and a "response". Pension plan administrators must build their cyber resilience – meaning, the ability to assess and minimize the risk of a cyber incident occurring, but also to recover when an incident takes place. To ensure effective management of an incident, plan administrators should work with all relevant parties (including in-house functions, third-party service providers and employers) to determine:

- how cyber incidents will be detected;
- how the plan will recover from the incident and restore normal operations (see Resiliency Plans); and,
- what disclosures should be made, and to whom, with respect to any incident (see Incident Reporting).

Resiliency Plans

Management of cyber risks may include establishing resilient contingency plans to deal with incidents and swiftly and safely resume operations. The core elements of a resiliency plan

[1] Cybersecurity posture means the strength of the cybersecurity controls and protocols for predicting and preventing cyber threats, and the ability to act and respond during and after an attack.

would typically address business continuity, disaster recovery and the incident response. A resiliency plan should cover a range of scenarios and the likelihood of different types of incidents. It should set out:

- the roles and responsibilities of the incident response team, including third-party responsibilities and their incident response processes;
- the resources required to investigate the cyber incident and maintain critical functions (e.g., payments of benefits) and processes;
- in-crisis communications including how and when reporting will be made to board members or trustees (as applicable); and,
- the process, thresholds, and time limits for notifying other parties including the supervisory authorities, law enforcement (in cases of fraud), third parties, and where necessary, plan beneficiaries.

Plan administrators may also benefit from creating various cyber breach playbooks and conducting regular tabletop exercises with all relevant parties, employees, third-party vendors and service providers, outsourcing companies, etc., to practice and improve cyber incident management capabilities.

Incident Reporting

As it relates to incident reporting:

- pension plan administrators should be clear on how and when cyber incidents should be reported to them, to plan beneficiaries, and to other appropriate parties;
- pension plan administrators should determine whether notification of a cyber incident to other parties is required, whether voluntary or as prescribed by any legislation, and should ensure reporting complies with any prescribed timelines;
- plan beneficiaries should be informed about any cyber incident that has an impact on their benefits, financial or personal interests; and,
- pension plan administrators should ensure that the measures being taken to mitigate the impact of these incidents are communicated to affected plan beneficiaries.

Evolving Nature of Cyber Risks

Cyber risks are complex and rapidly evolving and require a dynamic response, therefore:

- controls, processes, and response plans should be regularly tested and reviewed;
- plan administrators should be regularly updated on cyber risks, incidents, and controls;
- plan administrators and other relevant parties should seek appropriate information, and guidance, on cyber security threats to enhance the plan's ability to respond to, and recover from, cyber incidents.

Appendix A

In ensuring that cyber risks are sufficiently integrated into the plan's governance framework, plan administrators should consider the following types of questions:

- Are the roles and responsibilities in respect of the plan's approach to cyber risk clearly defined and documented?
- Does the plan have in place sufficient training, skills and expertise to ensure that cyber risk is well understood and managed?
- Has the plan identified its critical technology assets (e.g., software or hardware), access management (i.e., the framework of policies and technologies used authenticate user access) and data protection frameworks?
- Is there a sufficient understanding of the potential impact of a cyber incident as well as the likelihood of different types of breaches occurring?
- Is there an understanding of the extent of the plan's cyber exposure, including that arising from the actions or inactions of third parties?
- Is there a discussion of third-party cyber risk management with third-party clients (at both the onboarding phase and regular intervals)?

In ensuring that cyber risks are sufficiently integrated into the plan's risk management framework, plan administrators should consider the following types of questions:

- Are cyber risks appropriately identified, and are they reviewed regularly including when there are significant changes to the plan's operations? Does the review include metrics that track the efficacy of the responses to cyber incidents?
- Are existing controls sufficient and proportionate to minimize the risk of a cyber incident as well as its potential impact?
- Does the plan have a third-party regularly assess its cyber risk program?
- Does the plan have in place an appropriate cyber insurance policy and, if so, what is covered by the insurance (e.g., incident response)?
- Does the plan have in place a formal Information Security program?
- Does the plan have a process to assure that any third parties with which the plan contracts have sufficient controls in place to address cyber risks?
- Does the plan have in place incident response plans to respond quickly and minimize harm in the event of a cyber incident?
- Does the plan have a documented and approved Cyber Risk Appetite statement?

Appendix B

The following are examples of controls that plan administrators may find relevant to their cyber risk management activities:

- Managing physical, environmental and virtual access to systems and data.
- Increasing system resilience and recovery by leveraging the expertise of Information Technology (IT) experts/departments.
- Establishing sound policies and processes such as:
  - hardware and software asset management;
  - hardware, software, and firmware regular updates;
  - firewalls, antivirus software and other detective and protective tools;
  - acceptable use of devices (including removable and personal devices), email and internet (including social media);
  - use of passwords and other means of authentication;
  - safe practices while home and mobile working;
  - data access, protection (including encryption), use and transmission, and storage in line with data protection legislation and guidance;
- Developing and testing a communication protocol that would be activated in the event of a cyber incident.
- Providing appropriate training to staff and trustees, if applicable. Training should include awareness of cyber risks and how to report incidents.
- Encouraging members to adopt best practices with respect to passwords (e.g., log in credentials to an online pension portal) and security of their personal data.
- Monitoring of systems and networks for unusual activity or unauthorized access.
- Regularly reviewing and testing of controls, processes, and response plans (e.g., Disaster Recovery Plans) to ensure they remain adequate.
- Conducting tabletop exercises to both test crisis response plans and ensure that primary and alternate contacts understand their roles.