CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Reporting Alert

CORPORATE REPORTING

JUNE 2018

Cyber Security: Establishing a Risk Management Program and Continuing to Reassess Disclosure Practices

Background

In today's fast-paced, highly connected business environment, various aspects of an organization's business activities are carried out in "cyberspace." Cyberspace is where people and organizations create an electronic presence and engage in virtual activities, exchanging information, products and services through the Internet. While operating in cyberspace offers many advantages, it also makes organizations vulnerable to cyber attacks.[1] These threats apply to all organizations, including publicly accountable entities, private enterprises, not-for-profit organizations, government-related entities, and others.

The term "cyber security" refers broadly to the processes and practices in place to protect computer systems and data from threats originating in cyberspace. Accountability for aspects of cyber security may fall across many areas of an organization, often including the finance department. Given the significant reputational, operational, financial, legal, and regulatory implications of recent high-profile data breaches, investors and other stakeholders are increasingly interested in understanding an organization's exposure to cyber security risk and the related policies, processes, and controls it has in place to address this risk. The February

1 A report by the board of the International Organization of Securities Commissions (IOSCO) defines cyber attacks as "attempts to compromise the confidentiality, integrity and availability of computer data or systems." *Cyber Security in Securities Markets — An International Perspective, April 2016*.

2018 federal budget allocated approximately $500 million over five years to cyber security to be spent in part on establishing a new Canadian Centre for Cyber Security and a National Cybercrime Coordination Unit.

Purpose of this Reporting Alert

On January 19, 2017, the Canadian Securities Administrators (CSA) published **CSA Multilateral Staff Notice 51-347—Disclosure of cyber security risks and incidents** (CSA Staff Notice 51-347), which outlined expectations for disclosures by reporting issuers relating to cyber security risks and cyber incidents. In our April 2017 reporting alert **Cyber Security Risks and Incidents—Reassessing Your Disclosure Practices**, we provided an update on CSA Staff Notice 51-347 and on issues relating to cyber security disclosure.

This publication builds on our April 2017 alert in two ways:

- It sets out considerations for management of all entities in developing a cyber security risk management program.
- It provides an update on the current disclosure environment for registrants and reporting issuers, including recent guidance issued by the CSA and the U.S. Securities and Exchange Commission (SEC).

Developing a Cyber Security Risk Management Program

In 2017, the American Institute of Certified Public Accountants (AICPA) in the U.S. developed a reporting framework that helps organizations communicate relevant and useful information about the effectiveness of their cyber security risk management programs.[2] The AICPA also issued **System and Organization Controls (SOC) for Cybersecurity (SOC for Cybersecurity): Reporting on an Entity's Cybersecurity Risk Management Program and Controls** for CPA practitioners to examine and report on such information.[3] The cyber security risk management examination report includes the following three key components:

- a management-prepared narrative description of the entity's cyber security risk management program encompassing information about how the entity identifies its most sensitive information, the ways in which the entity manages the cyber security risks that threaten it, and the key security policies and processes implemented and operated to protect the entity's information assets against those risks[4]
- an assertion by management about whether the description is presented in accordance with criteria developed by the AICPA, and whether the controls within the program were effective to achieve the entity's cyber security objectives based on the AICPA's control criteria
- a CPA practitioner's opinion on management's description and management's assertion as to the effectiveness of controls within the cyber risk management program.

2 **www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurityfororganizations.html**

3 SOC for Cybersecurity: The CPA Canada Guide, *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*, adapted for Canadian auditing standards is currently in progress and will be available soon on the CPA Canada CPAstore.

4 The AICPA's description criteria is to be used by management in designing and describing their cybersecurity risk management program and can be accessed at: **www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity/description-criteria.pdf**

The AICPA has issued an illustrative example of such a cyber security risk management report, including criteria for evaluating the management description and the effectiveness of controls established to achieve the entity's cyber security objectives, providing a useful reference point for management of all entities in designing and implementing a cyber security risk management program.[5] The Appendix to this publication sets out some questions for management and boards in developing a cyber security risk management program based on the AICPA's description criteria and illustrative example.

Recent CSA and SEC Guidance on Cyber Security Risks

On October 19, 2017, the CSA published **CSA Staff Notice 33-321 Cyber Security and Social Media** (CSA Staff Notice 33-321) summarizing survey results of cyber security and social media practices of firms registered as investment fund managers, portfolio managers and exempt market dealers. CSA Staff Notice 33-321 provides guidance to such firms by suggesting policies and procedures in the areas of cyber security and social media practices.

On February 26, 2018, the SEC published interpretive guidance to assist public companies in preparing disclosures about cyber security risks and incidents.[6] The content of the guidance is similar in many respects to that of CSA Staff Notice 51-347. Even for Canadian reporting issuers that are not U.S. registrants, the SEC guidance provides an additional reference point in considering the ongoing adequacy of their disclosures and practices. For example, it focuses in greater detail on matters that may affect financial statements, noting that cyber security incidents may result in:

- expenses related to investigation, breach notification, remediation and litigation, including the costs of legal and other professional services
- loss of revenue, the need to provide customers with incentives, and loss of the value of customer relationships as an asset value
- claims related to warranties, breach of contract, product recall/replacement, indemnification of counterparties, and insurance premium increases
- diminished future cash flows, impairment of intellectual, intangible or other assets
- recognition of liabilities or increased financing costs.

The SEC sets out an expectation that a company's financial reporting and control systems will be designed to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cyber security incident will be incorporated into its financial statements on a timely basis as the information becomes available. Canadian reporting issuers required to establish and maintain internal control over financial reporting (ICFR), and for which certifying officers are required to address the evaluation of effectiveness of ICFR in their certification of annual filings, should likely also note the areas set out above as risk considerations in designing ICFR and when considering how to evaluate its effectiveness.

5 Section 3 within the link below includes an illustrative example of management's description of the entity's cyber security risk management program: **www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/illustrative-cybersercurity-risk-management-report.pdf**

6 **Release Nos. 33-10459; 34-82746 Commission Statement and Guidance on Public Company Cybersecurity Disclosures**

Appendix

Some Questions for Management to Consider When Developing a Cyber Security Risk Management Program

The following questions are based on the illustrative description of the risk management program contained in the AICPA's illustrative cyber security risk management report. The issues raised are not exhaustive.

Nature of Business and Operations

Have we appropriately assessed and documented the nature of our business and operations, including the principal products or services we sell or provide and the methods by which we distribute them?

Nature of Information at Risk

Have we assessed the principal types of sensitive information we create, collect, transmit, use, or store that carry an inherent cyber security risk?

Cyber Security Risk Management Program Objectives

Has management established, under the direction of the board, our principal cyber security risk management program objectives related to availability, confidentiality, integrity of data, and integrity of processing, and the process for maintaining and approving those objectives for all business units and functions?

Factors That Have a Significant Effect on Inherent Cyber Security Risks

Have we identified and documented the factors that have a significant effect on our inherent cyber security risks, including:

- characteristics of our technologies, connection types, use of service providers, and delivery channels
- organizational and user characteristics
- environmental, technological, organizational and other changes relating to us and our environment?

For security incidents that significantly impaired the achievement of our cyber security objectives, have we fully assessed and documented the nature, timing and extent of the incident, and how it was resolved and remediated?

Cyber Security Risk Governance Structure

Have we established processes for:

- establishing, maintaining, and communicating integrity and ethical values to support the functioning of the cyber security risk management program
- cyber security accountability and reporting lines
- board oversight of the program
- hiring and developing competent individuals and contractors and for holding those individuals accountable for their cyber security responsibilities?

Cyber Security Risk Assessment Process

Have we established processes for:

- identifying cyber security risks and environmental, technological, organizational and other changes that could have a significant effect on our cyber security risk management program, including relevant legal and regulatory requirements
- assessing the related risks to achieving our cyber security objectives
- identifying, assessing, and managing the risks associated with vendors and business partners?

Cyber Security Communications and Quality of Cyber Security Information

Have we established a process for internally communicating relevant cyber security information necessary to support the functioning of our cyber security risk management program, including:

- objectives, expectations and responsibilities for cyber security
- thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents requiring a response, remediation, or both?

Monitoring of the Cyber Security Risk Management Program

Have we established processes for:

- conducting ongoing and periodic evaluations of the operating effectiveness of key control activities and other components of internal control related to cyber security
- evaluating and communicating, in a timely manner, identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective actions, including management and the board of directors, as appropriate?

Cyber Security Control Processes

Have we established processes for:

- developing a response to assessed risks, including the design and implementation of control processes
- reviewing our IT infrastructure and the characteristics of its network architecture
- reviewing the key security policies and processes implemented and operated to address our cyber security risks, including those addressing the following:
  - preventing intentional and unintentional security events
  - detecting security events, identifying security incidents, developing a response to those incidents, and implementing activities to mitigate and recover from identified security incidents
  - managing processing capacity to provide for continued operations during security, operational, and environmental events
  - detecting, mitigating, and recovering from environmental events and using backup procedures to support system availability
  - identifying confidential information when received or created, determining the retention period for that information, retaining the information for the specified period, and destroying the information at the end of the retention period?

Other Resources

- CSA Staff Notice 11-326 Cyber Security
- CSA Staff Notice 11-332 Cyber Security
- CPA Canada: Board Bulletin: Cybersecurity Risk—Questions for Directors to Ask

Comments

Comments on this *Reporting Alert*, or suggestions for future Reporting Alerts should be sent to:

Dina Georgious, CPA, CA
Principal, Research, Guidance and Support
CPA Canada
277 Wellington Street West
Toronto ON M5V 3H2
Email: dgeorgious@cpacanada.ca