What are Canadian organizations sharing about cybersecurity risk and oversight?

CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

EY Building a better working world

The value of data has grown exponentially around the world. Data is now being considered "the new oil" because of the value it has for a company's operations. But are organizations doing enough to protect their data? If organizational data protection strategies are simply complying with current regulations, are they enough to address emerging threats?

The *2019 EY CEO Imperative Study* reveals that investors and boards expect CEOs to respond to humanity's greatest challenges, and cybersecurity is one of them, not only at the corporate level but at the national one. In the 14th edition of *The Global Risks Report*,[1] released early in 2019, the World Economic Forum identified a risk category related to technological matters and cited four significant technological challenges for humanity:

- Cyberattacks[2]
- Data fraud or theft[3]
- Critical information infrastructure breakdown[4]
- Adverse consequences of technological advances

From a Canadian perspective, in 2018 the federal government released its National Cybersecurity Strategy[5] through the Ministry of Public Safety and Emergency. This document, which was supported by public consultation, recognized how pervasive information technology (IT) is, and how it not only enhances quality of life but also creates risks for organizations.

As part of the initiatives triggered through the creation and release of the National Cybersecurity Strategy, the Canadian Centre for Cybersecurity was established. It coordinated the execution of a National Cyber Threat Assessment,[6] which presented key judgments, including:

- Cybercrime is the cyber threat most likely to affect Canadians and Canadian businesses in 2019.
- Cyber threat actors — of all sophistication levels — will increase the scale of their activities to steal large amounts of personal and commercial data.
- Canadians are very likely to encounter malicious online activity in 2019.
- State-sponsored cyber threat actors will continue to conduct cyber espionage against Canadian businesses and critical infrastructure to advance their national strategic objectives.
- Sophisticated cyber threat actors will likely continue to exploit the trusted relationships between businesses and their suppliers and service providers for espionage and cybercrime purposes.
- Cyber threat actors are adopting more advanced methods, making detection and attribution more difficult.

---

[1] https://www.weforum.org/reports/the-global-risks-report-2019
[2] Among top 10 risks in terms of likelihood and impact
[3] Among top 10 risks in terms of likelihood
[4] Among top 10 risks in terms of impact
[5] https://www.canada.ca/en/public-safety-canada/news/2018/06/national-cyber-security-strategy.html
[6] https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2018

Several high-profile cases of cyber breaches have attracted widespread media attention proving just how damaging cyberattacks can be. These cases emphasize that the warnings made by the Canadian Centre for Cybersecurity through the National Cyber Threat Assessment should be listened to and acted on.

Canadian companies and public reporting

Given the potential consequences of a cyber breach, EY and Chartered Professional Accountants Canada (CPA Canada) are joining forces to analyze Canadian cybersecurity reporting practices. This initiative complements the *EY US Center for Board Matters* initiatives that began in 2018 to explore what US public companies are sharing about cybersecurity risk and oversight.[7]

The study analyzed a sample of 60 TSX-listed companies to understand the nature and extent of cybersecurity-related disclosures in regulatory filings (annual information form, financial statements, management circular, management discussion and analysis, and material change report).

[7] https://www.ey.com/en_us/board-matters/what-companies-are-sharing-about-cybersecurity-risk-and-oversight

Preliminary findings

The full report will be issued in early 2020. Until then, we are pleased to share some initial findings:

- Almost all organizations surveyed disclose cybersecurity risks.
- More than 50% of organizations have a committee overseeing the cybersecurity function.
- Fewer than 50% of organizations share information on how they are responding to cybersecurity risks.
- More than 50% of organizations recognize data privacy compliance as another significant risk.

Once the analysis is complete, the findings will be classified and presented under the following categories:

- Board oversight
- Risk disclosure
- Risk management
- Cybersecurity incident management
- Data privacy

We expect the final report will provide a clearer picture of what public organizations in Canada communicate around cybersecurity. Please stay tuned so we can continue the conversation.