When the world is evolving faster by the second, how can your cybersecurity keep up?

Cybersecurity disclosure report

May 2020

The better the question.
The better the answer.
The better the world works.

CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

EY Building a better working world

In a world where it's not a matter of if you'll be breached, but when, boards, investors, regulators and other governance stakeholders are becoming increasingly interested in how companies guard against, plan for and respond to cybersecurity threats.

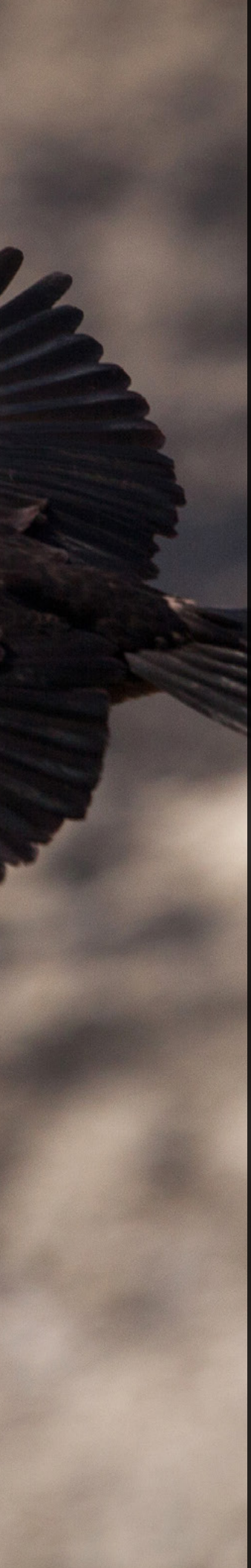
As threats to cybersecurity and privacy become more complex and widespread, stakeholders are expected to scrutinize more closely what corporations disclose about cybersecurity in their public filings.

To help inform Canadian companies about the current level of disclosure, EY and the Chartered Professional Accountants Canada (CPA Canada) have joined forces to analyze the cybersecurity reporting practices of Canadian public companies. This initiative complements the EY US Center for Board Matters initiatives, which in 2018 began to explore what US public companies are sharing about cybersecurity risk and oversight.

The Canadian study analyzed public reports from the 2018 filings made by the top 60 large-cap TSX-listed companies to understand the nature and extent of cybersecurity-related disclosures in regulatory filings, including the annual information form, financial statements, management circular, management discussion and analysis (MD&A), and the material change report, as applicable.

For further details on the scope and methodology, see the appendix.

Cover photo by Vincent Van Zalinge on Unsplash



Key observations

While cybersecurity is a key matter highlighted by many companies, the level of transparency and disclosure varied for Canadian publicly listed companies. Below are the key highlights from our findings.

Summary of key findings

Risk disclosure

98%

of Canadian companies cited cybersecurity as a risk factor.

Board oversight

72%

of Canadian companies disclosed that at least one board-level committee was charged with oversight of cybersecurity matters.

Cybersecurity incident management

42%

of Canadian companies referenced response planning, disaster recovery or business continuity considerations.

Cyberattacks

20%

of Canadian companies disclosed they have experienced some sort of cyberattack.

Risk management

78%

of Canadian companies referenced efforts to mitigate cybersecurity risk such as the establishment of processes, procedures and systems.

Privacy

50%

of Canadian companies disclosed specific concerns and actions defined to comply with privacy legislation.

The cybersecurity and privacy landscape

> “Several high-profile cases of cybersecurity breaches have attracted widespread media attention by proving just how damaging cyberattacks can be and by creating a catalyst for change for cybersecurity-risk disclosures.
>
> **Yogen Appalraju**
> Cybersecurity Leader, EY Canada

The 2019 EY CEO Imperative Study revealed that investors and boards expect CEOs to respond to a broad range of global challenges, with cybersecurity topping the list at both the corporate and national levels.

In its 2020 Global Risk Report, the World Economic Forum identified the following three most significant technological risks for humanity:

1. Cyberattacks
2. Data fraud or theft
3. Critical information infrastructure breakdown

The privacy regulatory landscape is also evolving. The enforcement of the European Union's (EU's) *General Data Protection Regulation* (GDPR) and the *California Consumer Privacy Act* (CCPA) are perhaps the most visible examples, but Canada is no exception. The Office of the Privacy Commissioner (OPC) is in the middle of a process and a series of public consultations to update Canadian regulations, including the *Personal Information Protection and Electronic Documents Act (PIPEDA)*:

- Today, all Canadian companies must notify the OPC of data breaches when they represent a real risk of significant harm to affected individuals.
- In the near future, amendments to federal privacy regulations that support Canada's Digital Charter will give more power to individuals, and authorities will align Canada with international privacy standards.

Canadian and US guidance on disclosing cybersecurity and privacy matters

The Canadian Securities Administrators (CSA) and other institutions have sent a very clear message: cybersecurity-related risks must be taken very seriously. In addition, public companies need to provide sufficient and timely disclosures to the market on what the organization is doing to respond to cyber risks in order to allow investors to make informed decisions.

The CSA has issued the following notices on cybersecurity, highlighting the relevance of disclosure and focusing on cybersecurity. These notices highlight the relevance of disclosure and the CSA's expectation that Canadian public companies will accurately and frankly respond to cybersecurity and privacy challenges, and disclose them to investors.

Figure 1 – CSA cybersecurity notices timeline

1. **CSA staff notice 11-326**
   September 2013
   Describes why the definition of cybersecurity measures should be important for issuers', registrants' and regulated entities' internal control systems.

2. **CSA staff notice 11-332**
   September 2016
   Declares cybersecurity as a priority area and reminds organizations about paying attention to cyber threats given their evolution.

3. **CSA staff notice 51-347**
   January 2017
   Presents the outcome of a review by the CSA of the disclosure provided by the constituents of the S&P/TSX Composite Index on cybersecurity risk and cyberattacks.

4. **CSA staff notice 33-321**
   October 2017
   Presents the results of a survey conducted by the CSA on cybersecurity and social media practices.

5. **CSA staff notice 11-336**
   April 2017
   Shares information on the results obtained from a roundtable session to explore cybersecurity issues and opportunities for better collaboration, communication and co-ordination in the event of a large-scale cybersecurity incident.

6. **CSA staff notice 11-338**
   October 2018
   Offers information on how to address a market disruption as a result of a cybersecurity incident.

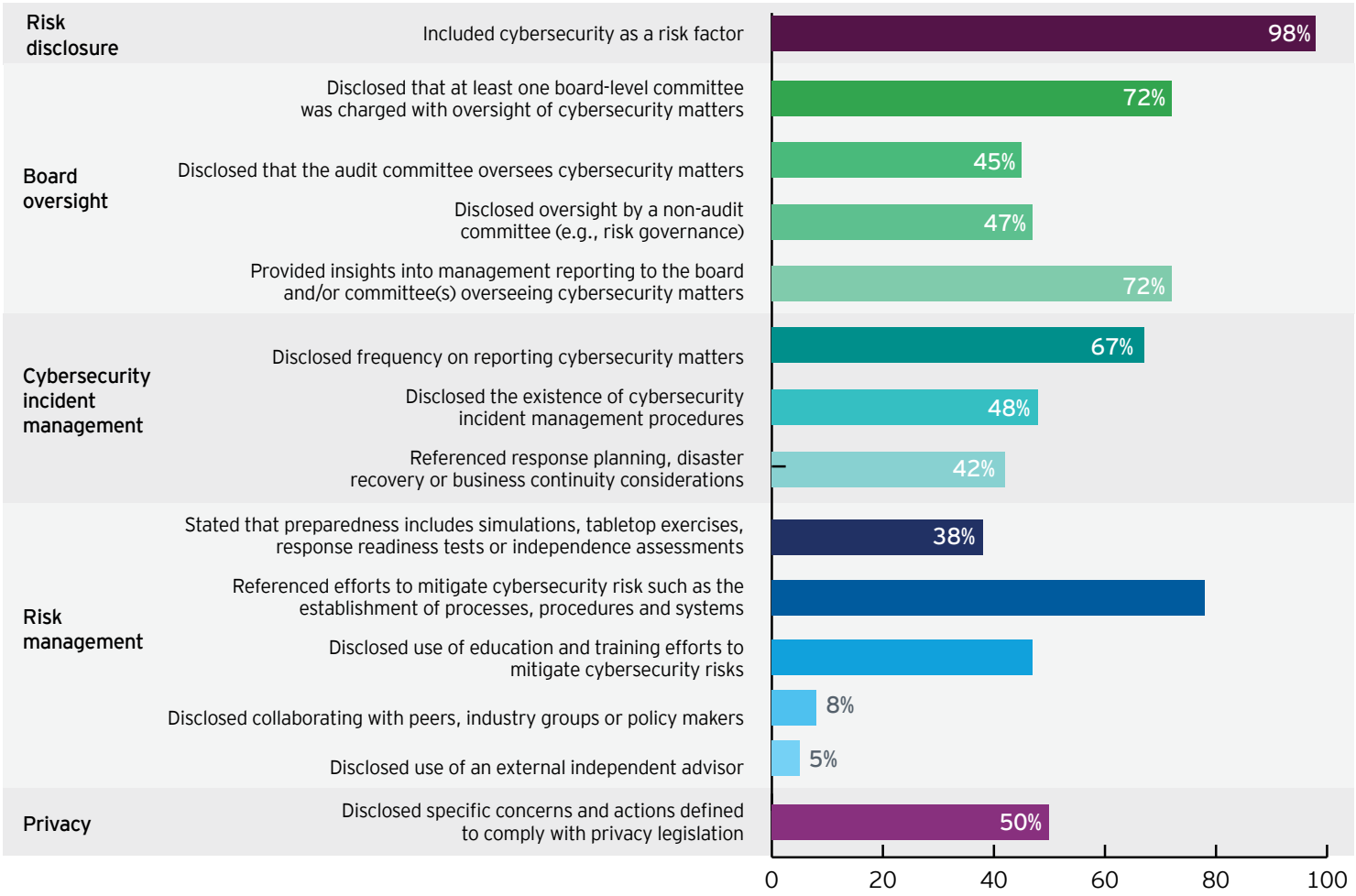
These notices help organizations understand the relevance of cybersecurity reporting and disclosures, and communicate actions the CSA has executed or will execute to respond to cyber challenges.

The US Securities and Exchange Commission (SEC) issued guidelines in 2018 to clarify public companies' obligations to disclose cybersecurity risks, material breaches and their impact on business, finances and operations when trading stock in the United States. The objective was to enable investors to make more risk-informed investment decisions.

Findings

EY and CPA Canada jointly analyzed cybersecurity- and privacy-related disclosures included in public reports issued by the top 60 TSX companies listed by market capitalization as of December 31, 2018. This represents 70% of the TSX market capitalization.

Figure 2 – Cybersecurity-related findings from the filing of Canadian public companies



Risk disclosure

After analyzing the results, almost all Canadian organizations reviewed (98%) recognized the relevance of cybersecurity-related risks. The only organization that did not include cybersecurity in the risk disclosure section focused its disclosure on risks that could impact physical assets.

Board oversight

Approximately half (52%) of organizations reviewed have assigned just one committee to oversee cybersecurity matters; 20% have assigned more than one committee (for a total of 72%). Figure 3 summarizes the committees assigned to this function by the organizations reviewed.

Figure 3 – Boards overseeing cybersecurity

Canadian companies are using both the audit committee (45%) and other non-audit committees (47%) to oversee cybersecurity considerations.

Communicating cybersecurity matters to the board is done by 72% of Canadian organizations. The specification of the frequency for reporting is disclosed by 67% organizations reviewed. Figure 4 illustrates this.

Figure 4 – Frequency of reporting

2%	15%	28%	17%	3%	3%
Annually	Semi-annually	Quarterly	Every 5-8 months	Monthly	Not specified

> Defining a plan to know how to respond to unexpected situations and periodically testing it to confirm its effectiveness are leading practices to successfully overcome an incident.

Carlos Chalico
Cybersecurity Senior Manager, EY Canada

Cybersecurity incident management

Just under half (48%) of Canadian organizations disclosed the existence of cybersecurity incident management procedures to deal with unexpected situations directly impacting their electronic data processing activities. These incidents range from minor issues such as information technology device not working properly to more sophisticated challenges like a distributed denial of service or a privacy breach.

Regarding the use of response planning, disaster recovery or business continuity considerations, the study observed that 42% of organizations have elements to respond to contingencies affecting the operations beyond their electronic data processing capabilities.

More than a third (38%) of organizations disclosed that their preparedness for responding to unexpected situations includes simulations, tabletop exercises, response readiness tests or independence assessments.

Risk management

The majority (78%) of organizations made references to the efforts they have made to mitigate cybersecurity-related risks. The use of specialized processes and procedures, as well as implementing management systems, are among the key elements used to face these challenges. When specifying the frameworks used to support the cybersecurity strategy, ISO 27000,[1] NIST[2] and PCI-DSS[3] were mentioned.

Education and training to mitigate cybersecurity risks is mentioned by 47% organizations. Cybersecurity and privacy awareness sessions are the most common ways organizations are addressing this.

Only 8% of organizations disclosed their involvement in the development of collaboration initiatives to interact with peers, industry groups or policymakers to share ideas and identify leading practices to respond to cybersecurity challenges. Meanwhile, 5% of organizations use an external cybersecurity advisor.

Use of an external cybersecurity advisor was disclosed by 5% of organizations.

1 International Organization for Standardization 27000 series of standards.
2 National Institute of Standards and Technology.
3 Payment card industry – data security standard.

Photo by Geran De Klerk on Unsplash

Privacy

In a time when the Canadian PIPEDA has been amended to make mandatory the notification of data breaches if they represent a real risk of significant harm to the affected individuals, 50% of Canadian organizations identified their interest in effectively responding to privacy regulations, including PIPEDA and the EU's GDPR, amongst others.

One-fifth (20%) of all organizations reviewed disclosed they have experienced some sort of cyberattack. These organizations belong to different industries, including the financial, retail, consumer products, mining, technology, telecommunications and services sectors. Nine organizations who experienced a cyberattack described it as being non-relevant, while three described how the event was significant for them.

Your customers may be at the greatest risk during a cyberattack

Of the significant attacks, the largest impact was on an organization's customers

Loyalty systems and programs were targets in a number of these cases

As a result of some of these attacks, class action lawsuits were filed

Conclusion

This report aims to enhance discussion around cybersecurity-related disclosures by offering insights on current disclosure practices, along with providing perspectives gathered through EY's interaction with investors and boards.

Cyberattacks represent a real threat that companies must consider as a significant element in their enterprise risk management program. Public disclosures present an opportunity for companies to communicate how they are leading the way in responding to cybersecurity and privacy challenges. Transparency demonstrates not only a commitment to care and due diligence, but also to engagement with stakeholders.

> "Cybersecurity, job losses due to technological change and income inequality are the top three global challenges for CEOs. This has made cybersecurity and data privacy one of the eight priorities for boards in 2020.

Michael Massoud
Principal, Research, Guidance and Support CPA Canada

Questions for management and boards to consider

The following key questions may assist management and boards of reporting issuers when assessing their cyber risk disclosure practices:

Understanding industry risk level and stakeholder exposure

- Have we documented, and do we fully understand, the cyberspace in which we and our business partners and other stakeholders operate?
- Have we taken steps to understand investors' concerns about our exposure to cybersecurity risk, and how we should address these concerns in our disclosures?
- Do we understand how our external auditors take cybersecurity risk into account when planning and performing their audit?
- Have we assessed cybersecurity risk disclosures made by other companies in our industry or in other industries but in similar circumstances?

Mitigating risk through employee education and governance structure

- Are we satisfied that cybersecurity risk and its mitigation receive appropriate attention in our governance structure? Is it clear who has the responsibility for overseeing this area?
- Does the individual or group responsible for overseeing cybersecurity risk devote sufficient time to these issues and receive appropriate input, support and resources from our organization as a whole? Is all this sufficiently clear in our disclosures?

Assessing and documenting internal policies and procedures

- Have we assessed the overall adequacy of our disclosure of cybersecurity risk with reference to the considerations set out in the CSA Staff Notices?
- Have we assessed each of our core periodic documents separately for the kind of operational, financial and regulatory cybersecurity-risk disclosures required? Do we have procedures in place to revisit this disclosure practice regularly?
- Have we defined internal procedures for assessing the materiality of cybersecurity breaches or other occurrences?
- Does the design of our disclosure controls and procedures to ensure cybersecurity incidents are communicated to management, and that consequent disclosure decisions are made in a timely manner?
- Have we developed internal key performance measures relating to how we monitor, detect and manage cybersecurity risk? If so, should we disclose these in our external reporting?

Related resources

For more information, the following resources may be useful.

CPA Canada resources

Cyber Security: Establishing a risk management program and reassessing disclosure practices

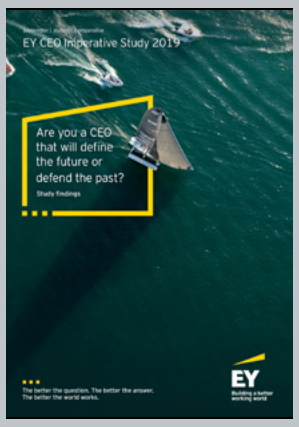
Cyber Security Risks and Incidents – Reassessing Your Disclosure Practises

Cybersecurity: Is it on your radar?

Cybersecurity practices and reporting trends

EY resources

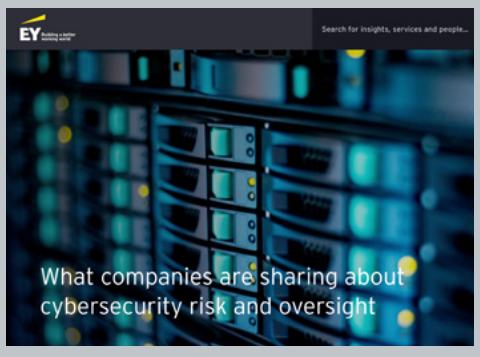
EY CEO Imperative Study



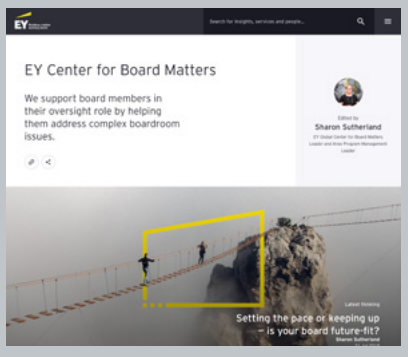
Global Information Security Survey

Eight priorities for boards in 2020

What companies are sharing about cybersecurity risk and oversight



EY Center for Board Matters



IAPP – EY Annual Privacy Governance Report

Contacts

Michael Massoud

CPA, CA, CPA (IL)
Principal, Research, Guidance and Support
CPA Canada

mmassoud@cpacanada.ca

Yogen Appalraju

CPA, CA, CISA
Cybersecurity Leader, EY Canada

yogen.appalraju@ca.ey.com

Carlos Chalico

CISA, CISSP, CISM, CGEIT,
CRISC, ISO27001LA, PbDA
Cybersecurity Senior Manager, EY Canada

carlos.perez.chalico@ca.ey.com

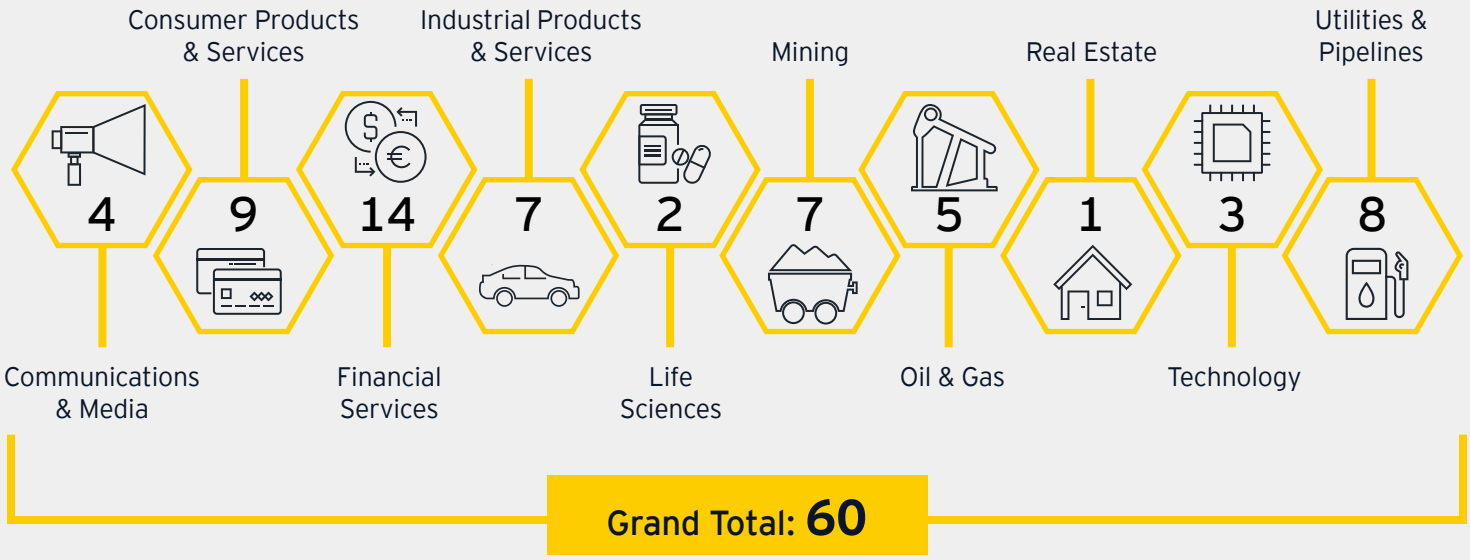
Appendix:

Scope and methodology

This document is based on the review of the top 60 large-cap TSX-listed companies' 2018 regulatory disclosure reports published to the System for Electronic Document Analysis and Retrieval (SEDAR). Disclosure documents reviewed were: annual information forms, management discussion and analysis, financial statements and information circulars.

Company selection

The 60 Canadian companies reviewed represent 70% of the market capitalization[4] of the S&P/TSX Composite Index (TSX) and S&P/TSX Composite Venture Index (TSXV) across 10 major industry sectors. Companies were selected to ensure representation across sectors. The table below summarizes the number of Canadian companies reviewed per sector.



4 Market capitalization percentage calculated as of December 31, 2018.

Analysis

The following list of key words was prepared based on the comments from the survey respondents to determine whether their comments should be considered as part of this report.

The collection of comments related to the key words was used to build the trends reported in this document. The following table presents the key words used as part of this exercise.

Attack	Data set	Passwords
Attacked	Dataset	Penetration
Attacker	Disaster recovery	Personal information
Attackers	Disaster recovery plan	Personal Information Protection and Electronic Documents Act
Attacks	DRP	Phishing
BCP	Encryption	PIPEDA
Bot	GDPR	Privacy
Business continuity plan	General Data Protection Regulation	Protected information
Classified information	Hackers	Ransomware
Cyber	Hacking	Resilience
Cyber insurance	Incident	Restricted access
Cyber security	Incident response plan	Root
Cybersecurity	Information security	Sensitive information
Cyber-security	Information tech	Supervisor
Cybersecurity disclosure	Intrusion	Unauthorized access
Data breach	IRP	Virus
Data breaches	Limited access	Viruses
Data leakage	Malicious software	Vulnerabilities
Data privacy	Malware	Vulnerability
Data risk management	Password	Worms

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

3400510
ED 00

ey.com/ca

About CPA Canada
Chartered Professional Accountants of Canada (CPA Canada) is one of the largest national accounting organizations in the world and is a respected voice in the business, government, education and non-profit sectors.

CPA Canada is a progressive and forward-thinking organization whose members bring a convergence of shared values, diverse business skills and exceptional talents to the accounting field. Domestically, CPA Canada works cooperatively with the provincial and territorial CPA bodies who are charged with regulating the profession. Globally, it works together with the International Federation of Accountants and the Global Accounting Alliance to build a stronger accounting profession worldwide. As one of the world's largest national accounting bodies, CPA Canada carries a strong influential voice and acts in the public interest.

cpacanada.ca