Canada Highlights

EY
Building a better working world

# Cybersecurity: Do you know which protective measures will make your company cyber resilient?

21st Global Information Security Survey 2018-2019

# Canada highlights

According to the EY Global Information Security Survey (GISS), 70% of Canadian respondents have increased their cybersecurity budgets in the last 12 months, while 91% said they will inject more resources into cybersecurity in the next year.

While it seems Canadian organizations are considering cybersecurity threats a reality, cybersecurity budgets remain low when compared to overall IT budgets. In fact, 63% say their total spend on information security is less than 10% of the overall IT budget.

This comes in a time of regulatory changes. In 2018, the world witnessed the enforcement of the General Data Protection Regulation (GDPR) in Europe, which reinforces privacy rights for individuals and raises obligations for personal data controllers and processors. The GDPR has impacted other jurisdictions, and as of 1 November 2018 Canada has announced changes to the Personal Information and Electronic Documents Act (PIPEDA), making the notification of data breaches under certain circumstances mandatory.

Canada is on track to become one of the world's leading technology innovation hubs. To protect the Canadian economy from risks in the cyber world, the federal government recently launched the National Cybersecurity Strategy, which outlines specific actions to reduce risk. With this strategy, Canada has found a way to strike a balance between innovation and protection.

**Yogen Appalraju**
Partner
Canadian Cybersecurity Leader

# Privacy compliance and reputational risk

## Top most valuable information to cyber criminals:

1. Customers' personal identifiable information and passwords
2. Financial information and strategic plans
3. Senior executives' and board members' personal data

These values reflect two specific concerns: privacy compliance failure and reputational risk.

Canadian and global organizations are right to prioritize these issues. Privacy regulations are responding to the new needs of the digitized world and are reinforcing mechanisms to make organizations accountable for the decisions they make when processing personal identifiable information. Organizations that don't protect personal data can face significant penalties. And if they ever have to report a data breach, it can have a significantly negative impact on their reputation.

While Canadian companies are increasingly recognizing that cybersecurity and privacy strategies are important, they continue to be more reactive than proactive. Privacy and security need to be implemented and operationalized in every organization, not because regulations like the GDPR require it, but because of the benefits these frameworks present. Defining controls in the early stages of information system and process design could reinforce compliance, reduce risks and cut costs significantly.

Although Canadian businesses are concerned about how valuable and attractive personal data is to cyber criminals, 64% of respondents say they don't have a data protection program or only have an informal one. Canadian organizations need to be concerned about data protection and should act by defining the mechanisms to effectively enable cybersecurity and privacy controls in a proactive way.

**58%**

**of Canadian respondents say information security has little or no influence on on their business strategy or plans**


**64%**

**of Canadian respondents confirmed they do not have a data protection program, or they have an informal one**

# The human factor

## Top three vulnerabilities faced in the last 12 months:

1. Careless or unaware employee (39%)
2. Outdated information security controls or architecture (24%)
3. Unauthorized access (11%)

**35%** say phishing was the top threat in the past 12 months

According to 27% of Canadian respondents, the most likely source of a cyber attack is a careless employee. As businesses continue to increase their digital footprint, 36% of respondents cite poor user awareness and behaviour as the top risk associated with the growing use of mobile devices.

People remain the weakest link when it comes to cybersecurity. To build an effective threat prevention strategy, organizations need to offer effective cybersecurity training and education programs to ensure employees can identify and prevent cyber security threats.

# Board oversight

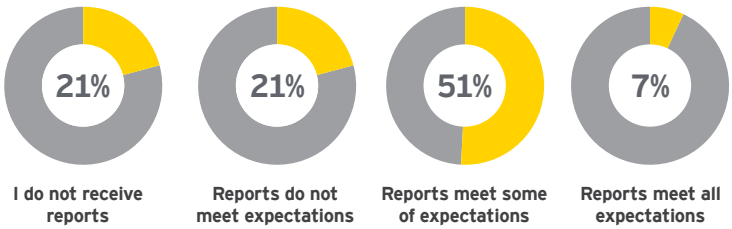
**68%**

of Canadian respondents say the person with direct responsibility for information security is not a member of the board or executive

**only 16%**

say their board has a comprehensive understanding of information security to fully evaluate the cyber risks the organization faces and the measures it takes

## Effectiveness of the organization's information security reports




Detecting and responding to cybersecurity threats is a business issue that makes in-depth cybersecurity education at the board level critical. In order to make the right decisions and develop effective countermeasures, board members should fully understand the cybersecurity risks and challenges their organization is facing and know how to effectively respond to threats and measure success.

# Can we use Digital as an enabler for progress?

Evidence has shown us over time that organizations tend to be more reactive than proactive when it comes to designing a cybersecurity program.

**91%** of Canadian respondents say the discovery of a breach that impacted the organization would cause an increase in their information security budget

Since the early 2000s, organizations have been increasingly investing in IT. In comparison, investments have been considerably lower in cybersecurity. This so-called security gap illustrates that investments in IT are being made without properly addressing the associated cybersecurity risks.

According to EY's Growth Barometer, 86% of respondents are planning to adopt artificial intelligence (AI) over the next seven years. And while the adoption of emerging technologies like AI may help improve business processes over time, it may also expose businesses to new risks. Their success will depend on how they respond to those risks, how willing they are to increase budgets to close the security gap, and how effective they are in protecting data and information.

# Resiliency

Canadian companies recognize the importance of having specialized teams that are focused on cybersecurity. Of those surveyed, 72% say they have a Security Operations Centre (SOC) and 27% say that's how they discovered the most recent significant cybersecurity incident. Canadian companies also consider themselves very mature in incident management, policy and standards framework definition and cybersecurity strategy adoption. However, in areas such as data infrastructure, third-party risk management and the availability of specialized cybersecurity programs, they need to improve significantly:

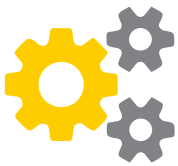
**67%**
do not have a **threat intelligence** program or only have an informal one

**45%**
do not have a **vulnerability identification capability** program or have an informal one

**52%**
do not have a **breach detection** program or have an informal one

**31%**
do not have an **incident response** program or have an informal one

**44%**
do not have an **identity and access management** program or have an informal one



**Only 13%** **say they are excellent at crisis management**

As many organizations have learned — sometimes the hard way — cyberattacks are no longer a matter of if, but when. This means that prevention and dissuasion are not enough. Companies need to know how to react, how to respond, how to recover and how to maintain their security. In other words, organizations need to be resilient.

To do this, companies should keep their business continuity and disaster recovery approaches up to date. Equally important, organizations should develop robust incident and crisis management plans and test them often through table top exercises involving staff and executives to ensure they are prepared should they become victim of a cyberattack.

Cyber threats are one of the top business risks facing organizations. Building your cyber resiliency can have the greatest impact to address this risk and should be a top priority.

# Conclusion

**83%** of Canadian respondents say their information security function is partially meeting their organizational needs, but there are plans to improve

Canadian organizations understand their cybersecurity programs demand attention. Limited knowledge on cybersecurity matters at the board level and the increased interest on assigning more budget to the function show a community committed to improving their cyber resilience, in an environment where government supports and organizations innovate.

Among the challenges for developing a mature cybersecurity function in Canada and around the world is the lack of skilled resources. The good news is that many universities and colleges in Canada are developing cybersecurity and privacy programs and labs which will help build the cyber talent pool and will eventually provide a workforce capable of keeping up with current threats. Managing cybersecurity is an ongoing and constantly evolving journey; no organization can anticipate every threat that will emerge. However, by making cybersecurity a key part of the company's culture, taking the necessary steps to become cyber resilient, and investing judiciously in a proactive cyber program, even the risks organizations can't see can be mitigated.

# Key Canadian findings

**83%**
say their information security function is partially meeting their organization's needs

**27%**
consider a careless employee as the most likely source of a cyber attack

**28%**
do not have a Security Operations Centre, even though they are becoming increasingly common

**16%**
of boards have sufficient information security knowledge to fully evaluate cyber risks

**20%**
say it is unlikely they would detect a sophisticated cyber attack

**35%**
say phishing was the top threat in the past 12 months

**67%**
do not have a threat intelligence program or only have an informal one

**89%**
say they need additional funding to protect their organization

**63%**
say their cybersecurity spend is less than 10% of the overall IT budget

# Ernst & Young LLP contacts

**For a conversation about your cybersecurity strategy, please contact:**


## Toronto

**Yogen Appalraju**
Partner, Canadian Cybersecurity Leader
yogen.appalraju@ca.ey.com
+1 416 932 5902

**Thomas Davies**
Associate Partner, Cybersecurity
thomas.davies@ca.ey.com
+1 416 943 2013

**Bryson Tan**
Associate Partner, Cybersecurity
bryson.tan@ca.ey.com
+1 416 943 3925

**Ryan Wilson**
Associate Partner, Cybersecurity
ryan.wilson@ca.ey.com
+1 416 943 7170

**Carlos Perez Chalico**
Senior Manager, Cybersecurity
carlos.perez.chalico@ca.ey.com
+1 416 943 5338

## Calgary

**Brian Masch**
Associate Partner, Western Canada Cybersecurity Leader
brian.masch@ca.ey.com
+1 403 206 5096

**Vitaly Sokolov**
Associate Partner, Cybersecurity
vitaly.sokolov@ca.ey.com
+1 403 206 5150

## Montreal

**Adam Sultan**
Senior Manager, Cybersecurity
adam.sultan@ca.ey.com
+1 514 879 2826


**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. For more information about our organization, please visit ey.com.

**About EY's Advisory Services**
In a world of unprecedented change, EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

From C-suite and functional leaders of Fortune 100 multinationals to disruptive innovators and emerging market small and medium-sized enterprises, EY Advisory works with clients – from strategy through execution – to help them design better outcomes and realize long-lasting results.

A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions. They work with their clients, as well as an ecosystem of internal and external experts, to create innovative answers. Together, EY helps clients' businesses work better.

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




EYGM no. 00000-000US

2875070

ED None




**ey.com/ca/cybersecurity**