Can cybersecurity unlock future business growth?

Yogen Appalraju, EY Canada Cybersecurity Leader

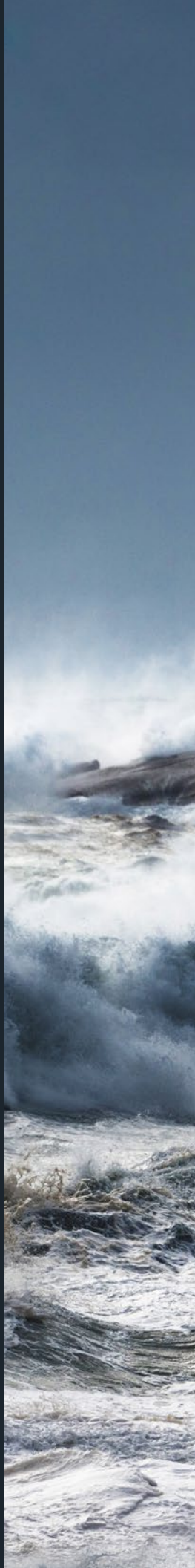
EY Global Information Security Survey 2021: Canadian highlights

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

EY
Building a better working world

Welcome

Contents



INTRODUCTION

Canadian CISOs face a critical crossroads

Something unexpected happened over the course of the pandemic. As the world shifted to immediately focus on secure, remote access and connectivity, Chief Information Security Officers (CISOs) found themselves suddenly thrown into the spotlight.

Eighteen months later, those leaders — and the cybersecurity, privacy and risk management functions they lead — have a tremendous opportunity to cement themselves as true enablers of strategic business growth.

How so? New cyber risks are proliferating. Threat actors have hit next-level maturity. Consumer demands around privacy are evolving accordingly. Innovation is increasingly taking place in non-traditional ecosystems (think Cloud 2.0). Taken together, these factors reinforce an urgent need for CISOs, and cybersecurity, to play broader roles across organizations for Canadian organizations.

Getting there may not be easy. Our latest 2021 EY Global Information Security Survey (GISS) shows operational silos hold progress back. Legacy

risk frameworks require fresh thinking. Internal disconnects continue to drive awareness gaps around the value that cybersecurity can bring. Even so, the opportunity remains.

The right strategy can empower CISOs to translate progress gained during the crisis into sustainable collaboration, more integrated operations and stronger relationships meant to generate long-term value in a market transformed.

Opportunities like these don't come along twice. Will you lean into the possibility, or let the moment pass your organization by?

Executive summary

With transformational change comes transformational opportunity. Our 2021 EY GISS shows CISOs now have a unique chance to build on the momentum created over the last 18 months and bolster their presence and effectiveness in Canadian organizations.

Doing so now can shape cybersecurity – and overall business results – for the better in an era when security, privacy and compliance will continue to be top of mind for internal and external stakeholders.

The key is to harness the progress made over the course of the pandemic and work as a united leadership team to:

1. TAKE DOWN OPERATIONAL SILOS TO CREATE A CONNECTED PATH FORWARD.
2. EMBRACE A NEW WAY OF MANAGING RISK.
3. DRIVE A CULTURAL SHIFT BY CULTIVATING INTERNAL AWARENESS.

1 Take down operational silos to create a connected path forward

Redrawing the organizational chart and making cybersecurity and privacy the connective thread between functional capabilities doesn't only make your organization stronger. It can also support efficiency, cut down costs, and foster the kind of collaboration that speaks directly to internal and external calls for secure products, services and solutions.

40% of leaders have never been as concerned as they are now about managing cyber threats.

WHY?

Risk itself has changed.

Our GISS findings show more than 40% of leaders have never been as concerned as they are now about managing cyber threats the business faces. You cannot tackle that increase in disruptive risk without drawing better connections between functional teams.

Innovation is happening everywhere.

Cloud is now the foundation for emerging technology. Developers are building new code and defining the server to house it themselves. Yet nearly 40% of organizations view the relationship between security and product development/R&D teams as a neutral one, characterized by low levels of consultation. That prevents security and privacy by design from taking hold.

Cybersecurity and privacy are invited to the party late.

Although many organizations are already looking beyond Cloud 2.0 and its focus on containerization to address serverless technologies and blockchain through Cloud 3.0, cyber resources remain disconnected from the planning process. Less than one quarter of Canadian organizations bring cyber and privacy in at the planning stage. This can lead to costly ramifications, sending designs back to the drawing board at the 11th hour because they were built without appropriate security safeguards and default privacy settings.

Figure 1: managing cyber threats

To what extent do you agree or disagree with the following statement: I have never been as concerned as I am now about our ability to manage the cyber threats that we face as a business

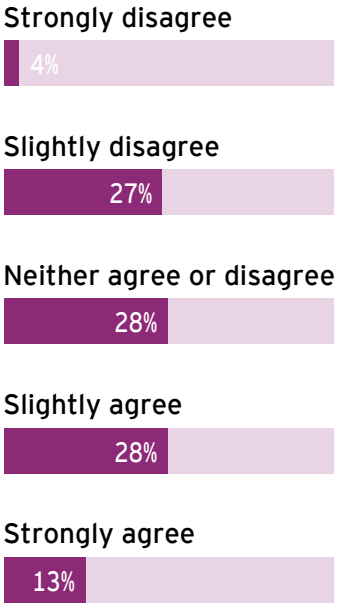
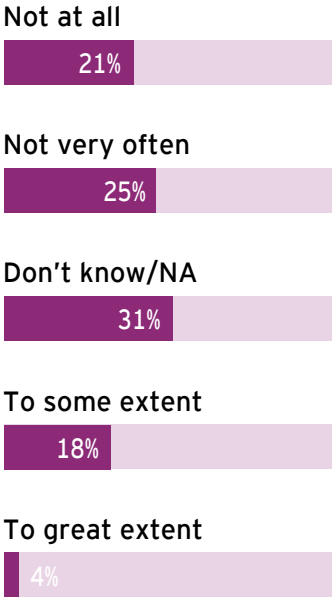


Figure 2: cybersecurity team consultation

Cybersecurity teams are either not consulted, or are consulted too late, when urgent strategic decisions are being made



HOW CAN ORGANIZATIONS TAKE ACTION NOW?

1 Set tone from the top

Assess connection points between CISOs and the broader leadership team to ensure cybersecurity and privacy are represented at all the right executive leadership tables. This should include addressing heighted concerns and cyber visibility at the Board level too.

2 Cross-pollinate cyber resources

Integrating cyber team members directly within IT, application development, business development, product design and other areas of the business can weave safety and privacy thinking into the dialogue earlier on.

3 Draw a new R&D framework

Refreshing processes and guidelines for research and development to include a cybersecurity and privacy step in the earliest stages can be an easy way to move cyber from late-stage compliance consideration to early-stage input provider.

"

The adage that there is no cloud, only 'someone else's computer,' is an outdated and precarious approach to operate modern IT and cyber security by. Today, emerging technologies offer organizations the ability to consume a myriad of cloud services offered across infrastructure, platform and software as a service and this necessitates a major shift in how emerging cyber risks must now be managed.

Amin Lalji
EY Canada National Cloud Security Leader

2 Embrace a new way of managing risk

As markets and organizations evolve, there's room to reshape the way cybersecurity and privacy teams operate, too. Assessing ways of working, embracing new models and reimagining required skillsets can help this critical function shift to better address the changing needs and demands of the business, as well as the customers and regulators these groups serve.

73% say cybersecurity doesn't actually enable innovation.

WHY?

Regulatory expectations are changing.

Half of Canadian execs say ensuring compliance in today's regulatory landscape is the most stressful part of their job. Some 70% expect regulations to become increasingly fragmented, making them harder and more time consuming to manage. Internally, fragmented responses can hamper efforts further, exposing the organization to additional risk. By reframing regulatory requirements from a risk-based perspective, cyber and privacy teams can get ahead of changing regulations and initiate proactive relationships that serve the entire organization better.

Innovation is cycling more quickly than ever before.

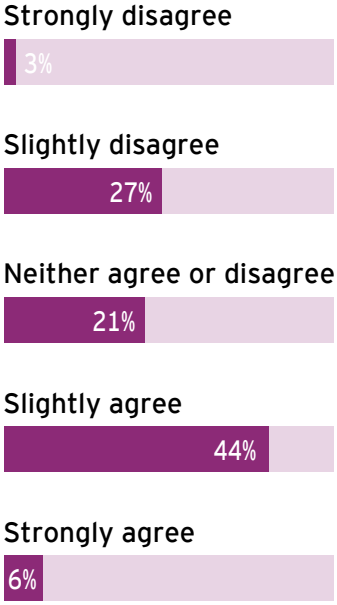
While most organizations feel cybersecurity protects the business, 73% say this function doesn't actually enable innovation. That's a missed opportunity. Innovation cycles are shorter than ever, magnifying the importance of security and privacy. Reframing the function's focus to prioritize innovation alongside security and privacy can help businesses build solutions that are inherently more secure at a time when stakeholders are increasingly concerned about their privacy in a hybrid business world.

Business-centricity is everyone's responsibility.

Only 20% of CISOs are confident they speak the same language as their peers across the business. But there's a real business case for cybersecurity and privacy specialists to contribute to all functional areas. Progressive organizations want to see how cybersecurity teams are getting creative to secure new products, digital offerings and broader business improvement initiatives. As business units adopt agile ways of working, building "security and privacy by design" is becoming more realistic. Cybersecurity teams must also adapt to approach risk through a commercial lens to drive more efficient overall business outcomes.

Figure 3: ensuring compliance can be stressful

To what extent do you agree or disagree with the following statement about regulation?: Ensuring compliance in today's regulatory landscape can be the most stressful part of my job



HOW CAN ORGANIZATIONS TAKE ACTION NOW?

1 Assess the skills you have

Effective cybersecurity will be achieved by cyber practitioners who have deep domain knowledge. This function will now need skills beyond foundational security and privacy expertise to contribute more broadly.

2 Realign the talent agenda

Upskilling existing talent to better address the changing face of the function, and hiring for net new capabilities, can help reinvent what cybersecurity and privacy are capable of. This will reinforce value in the organization and support cross-functional alliances.

3 Shift regulator relationships

Building out a new approach to regulator relationships can help the entire organization stay ahead of change. Nurturing and influencing these relationships allow organizations to become joint problem-solvers as opposed to policy followers.

> "Privacy regulations are more than just another compliance exercise. They represent a way of holding organizations accountable for how they collect and process personal data and protect individuals' right to privacy. The bigger objective is helping organizations create ethical business practices while gaining consumer trust.

Roobi Alam
EY Canada. Privacy & Data Trust Leader

3 Drive a cultural shift by cultivating internal awareness

Change is only as impactful as our ability to manage it meaningfully. If you're taking down operational silos, or changing the way cybersecurity and privacy operates, the organization needs to know. Internal education and awareness building transforms cross-functional teams into stewards of privacy, data protection and cybersecurity. Succeeding on this front can unlock benefits for both the organization and its stakeholders while bolstering the bottom line.

34% of executive management teams say they'd describe cyber as flexible and collaborative.

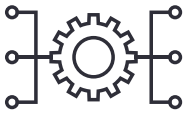
WHY?

New investments are creating new risks.

In our latest survey, 45% of organizations said they planned significant investments in data and technology over the next 12 months. But fewer than 30% describe cybersecurity as an innovation enabler. Bridging that gap requires internal education around the specific capabilities and skillsets that security and privacy can bring to the innovation table so they're considered earlier on in the process.

People don't know what they don't know.

Only 34% of executive management teams say they'd describe cyber as flexible and collaborative. There's no point in working to bring something new to the cybersecurity mix if the organization is holding on to legacy views of who you are and what you stand for. Creating opportunities to get to know the function better drives fruitful collaboration and profitable results.



Collaboration doesn't always come naturally.

Just over two thirds (68%) of CISOs say executive management wouldn't describe the role of cybersecurity as commercially minded. Changing that perspective will require cybersecurity and privacy teams to show, not tell, what they're capable of. Showcasing innovation stories centred on cross-functional teaming can bring people on board.

HOW CAN ORGANIZATIONS TAKE ACTION NOW?

1 Make a plan for change

Effective change management begins with strong planning. Draw a clear plan for how you'll eliminate organizational silos and reframe the way you approach risk overall. Get cross-functional buy-in for the plan.

2 Focus on storytelling through internal channels

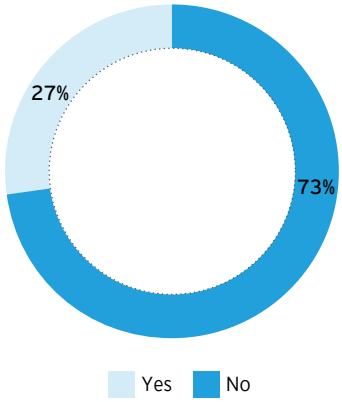
As you work through the transformation, use internal channels to deliberately and consistently share stories that highlight the "why" behind the change. Use examples, numbers and outcomes to build an internal business case and narrative for embracing cybersecurity and privacy in this new way.

3 Celebrate wins without moving the goal posts

Sustainable change takes time. Strong governance for managing a change such as this should include ways to acknowledge progress, celebrate wins and recognize achievement. Make this transformation about the journey, not just the destination, to motivate people.

Figure 4: cybersecurity and innovation

In your opinion, which of the following terms would the executive management team use to describe the role of cybersecurity within the organization? - Enables innovation



> "In a digitally transformed organization, cybersecurity and privacy functions cannot solely focus on risk reduction. In addition to value protection, they also need to enable value growth and optimization. This requires cybersecurity and privacy to transcend legacy paradigms and operating models. That means engaging and educating across functional lines on integrating cyber and privacy into their ventures from the outset. and transforming cyber and privacy from gatekeepers to agile functions that operate as true partners to the business.
>
> **Ali Varshovi**
> EY Canada Financial Services Cyber Leader

What's the bottom line?

In Canada and around the world, security functions are facing a critical inflection point. Seizing this moment to bring cybersecurity and the business closer together tells the market your security and privacy matter most. Start by dismantling operational silos, supporting a new view of risk, and driving meaningful internal culture change. Doing so now can bake security and privacy into everything you do and differentiate your organization in a sea of competition.

SURVEY METHODOLOGY

The data in this year's GISS report is based on a survey of CISOs and other senior leaders at 1,010 organizations, including 71 Canadian respondents, carried out between March and May 2021. CISOs and other C-suite professionals comprised 50% of respondents; the others were C-1 cybersecurity professionals. Surveys were primarily conducted via telephone, with a minority completed online.

Contact our leaders

TORONTO

Yogen Appalraju
yogen.appalraju@ca.ey.com

Roobi Alam
roobi.alam@ca.ey.com

Omer Arshed
omer.arshed@ca.ey.com

Jason Green
jason.b.green@ca.ey.com

Amin Lalji
amin.lalji@ca.ey.com

Chandra Majumdar
chandra.majumdar@ca.ey.com

Atul Ojha
atul.ojha@ca.ey.com

Bryan Pollitt
bryan.pollitt@ca.ey.com

Esha Ponnappa
esha.ponnappa@ca.ey.com

Bryson Tan
bryson.tan@ca.ey.com

Ali Varshovi
ali.varshovi@ca.ey.com

Ryan Wilson
ryan.wilson@ca.ey.com

OTTAWA

Jamie O'Hare
jamie.ohare@ca.ey.com

CALGARY

Brian Masch
brian.masch@ca.ey.com

MONTRÉAL

Frederic Georgel
frederic.m.georgel@ca.ey.com

Nicola Vizioli
nicola.vizioli@ca.ey.com

VANCOUVER

Simon Wong
simon.y.wong@ca.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

387692
ED 0000

ey.com/ca