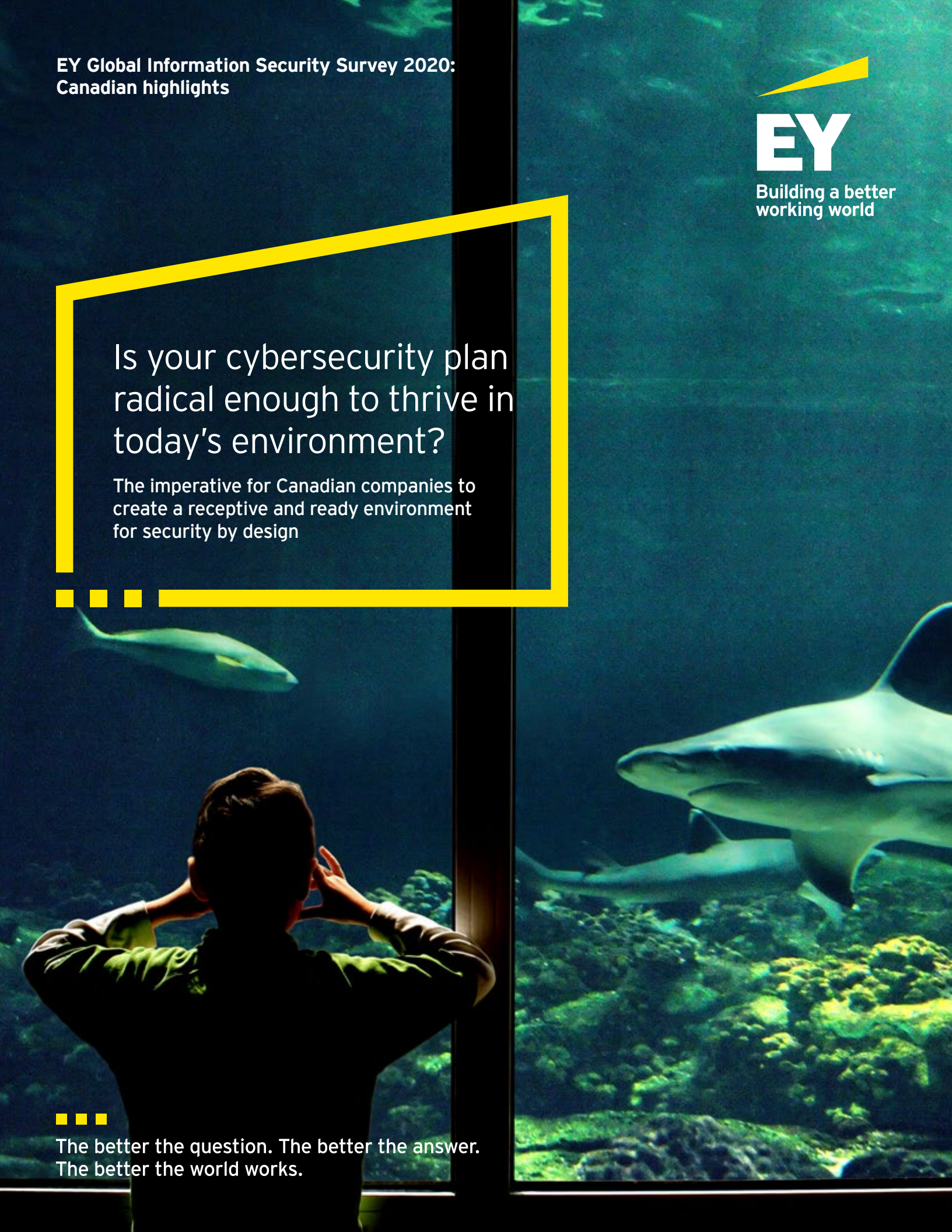
EY Global Information Security Survey 2020:
Canadian highlights

Building a better working world

Is your cybersecurity plan radical enough to thrive in today's environment?

The imperative for Canadian companies to create a receptive and ready environment for security by design



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

Yogen Appalraju
EY Canada Cybersecurity Leader

An unprecedented start to 2020 reinforces how security by design can enable businesses to seize the upside of disruption.

Now more than ever, insights that help guide organizations through unprecedented times such as COVID-19 are essential for enterprise resilience and recovery planning. Organizations in Canada and around the globe are increasingly vulnerable to cyberattacks arising from remote working and new types of online interactions with customers and businesses.

The 22nd annual EY Global Information Security Survey (GISS) explores the most important cybersecurity issues facing organizations today.

The Canadian results from the survey show that organizations have certainly made progress in maturing their security functions. But there is still much work to be done. Canada still lags behind its global counterparts.

Why does maturity matter? The more mature the security function, the more successful organizations can be in adopting and growing a **security by design** mindset. This year's GISS explores these ideas in more detail.

Together, we can improve cybersecurity for all and build a better working and more secure world.

What is security by design?

A strategic and pragmatic approach that integrates risk thinking from the inception of a product, service or initiative to embed trust in systems, designs and data, so that organizations can mitigate risks, lead transformational change and innovate with confidence.

Executive summary

Canadian organizations have made progress in maturing their security functions, but have still yet to catch up to companies in other parts of the world. For Canadian companies to thrive amid disruption, they need to embrace security by design, which integrates risk thinking at the development stage of any product, service or initiative. Having a mature security function is fundamental for security by design.

How organizations can take advantage of a security by design approach

Based on the findings from this year's Canadian GISS, there is a real opportunity to position cybersecurity at the heart of business transformation and innovation. Canadian organizations can reach the maturity of their global peers by:

1 **Focusing on board engagement**

With more effective alignment between cybersecurity and the board, security by design becomes possible, allowing organizations to integrate risk thinking from the development stages of transformation initiatives.

2 **Increasing cyber budgets to align to future initiatives**

With improved board engagement, cybersecurity and the board can work together to clarify business risk and define security investment priorities.

3 **Building productive relationships with every function of the organization**

Cybersecurity needs to develop better alliances within the organization to gain an understanding of different business priorities and critical assets, and in turn educate about security risks and potential impacts.

1 Engaging the board

With improved engagement, cybersecurity and the board can communicate more effectively about business priorities and the risks facing the organization, and work together more productively to support the future of the business.

KEY GISS FINDINGS

Why the disconnect?

Creating synergy between cybersecurity and the board is a legacy issue that stems from security's origins in IT. It was common for security professionals to rely on technology to solve cybersecurity issues, with little or no input from the board.

Going forward, to adopt an effective security by design culture, cybersecurity must be able to account for business considerations that matter to the board.

Here's how the cybersecurity function can more effectively engage the board:

Speak the language of the business and help the board understand the severity and business impact of different risks, with a plan of how to deal with them.

Build proper alliances across the business and educate the board to help foster commitment and promote the engagement needed to respond to cybersecurity measures.

WHAT CAN YOU DO TODAY?

Across any organization, different departments and priorities compete for budgets. CIOs and CISOs must increasingly make their voices heard. While boards recognize the importance of committing to cybersecurity, they aren't always given the tools and language to communicate the urgency in business terms.

"Establishing a strong relationship and speaking the board's language can help present cybersecurity risks in a way board members can relate to, expediting funding for initiatives and technologies needed to address the risk facing the organization.

Yogen Appalraju
EY Canada Cybersecurity Leader

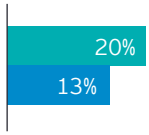
2 Increase cyber budgets to align to future initiatives

Consistent with trends from 2019, Canadian organizations are devoting less revenue to cybersecurity compared to their global peers. However, encouraging evidence shows Canada is ahead of organizations in other countries in terms of budget being spent on securing new technologies and other new initiatives.

KEY GISS FINDINGS

Organizations are spending less than 5% of revenues on cybersecurity

Organizations are directing 15% of their cybersecurity budgets to protect new technologies



Last year's GISS survey revealed that 86% of Canadian organizations expressed interest in adopting artificial intelligence (AI) in the next 7 years. And this year revealed there is increased commitment to securing new technologies. Balancing innovation and security is a positive trend for Canada.

Some investment initiatives can include:

Connecting people and devices securely is the foundation of true digital transformation. Every digital experience encompasses numerous touch points across an ecosystem. So anyone or anything that is connecting within that ecosystem and experience must have a verified identity and attributes to participate fully and securely.

Realizing the flexibility and cost benefits of cloud requires configuring and governing the cloud securely. Because the native security in today's cloud solutions is so advanced, it is important to invest in the right cyber skills. With the right expertise, organizations can deploy the cloud securely to fully maximize its benefits.

WHAT CAN YOU DO TODAY?

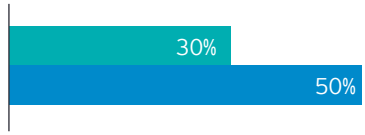
The board needs to understand cybersecurity challenges, and cybersecurity leaders need to better grasp the business agenda. With that shared knowledge, cybersecurity and the board can work collaboratively to identify risks and investment priorities.

3 Build productive relationships with every function of the organization

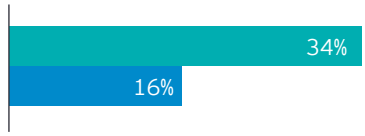
For cybersecurity to play a central role in enabling business transformation, it must take a formalized approach to aligning with business strategy and integrating with other functions in the organization. Improved alignment and integration creates a mutual understanding of potential threats, the impact to assets and how to best mitigate risk exposure.

KEY GISS FINDINGS

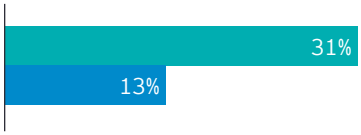
Organizations identify cybersecurity as a business risk



Organizations have not articulated their cybersecurity risk



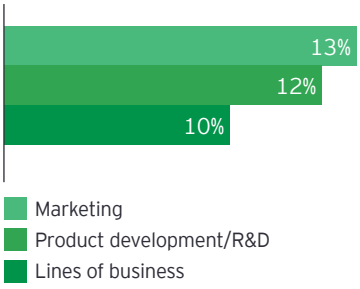
More than 75% of data breaches identified by Canadian organizations were the result of employee weakness, such as weak passwords, phishing, device loss, failure to patch and similar problems.



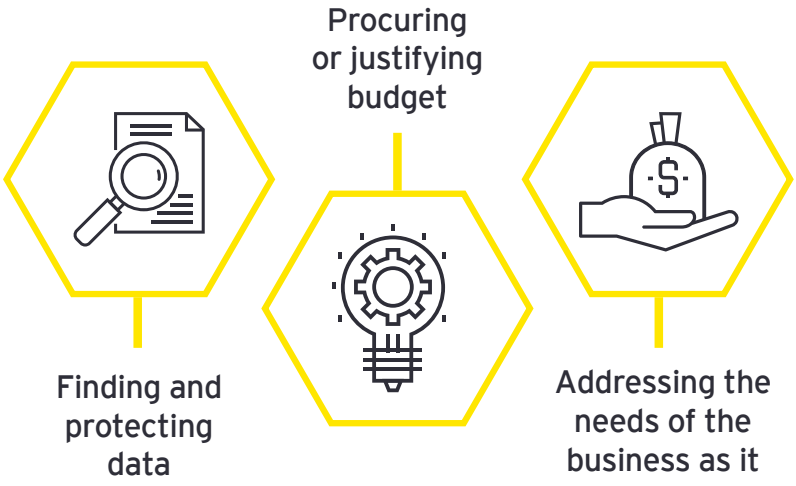
Cybersecurity's relationships across the organization

73% of Canadian organizations indicate a relationship with IT characterized by high trust and consultation.

Conversely, trust and consultation diminish significantly between cybersecurity and marketing, product development/R&D and lines of business.



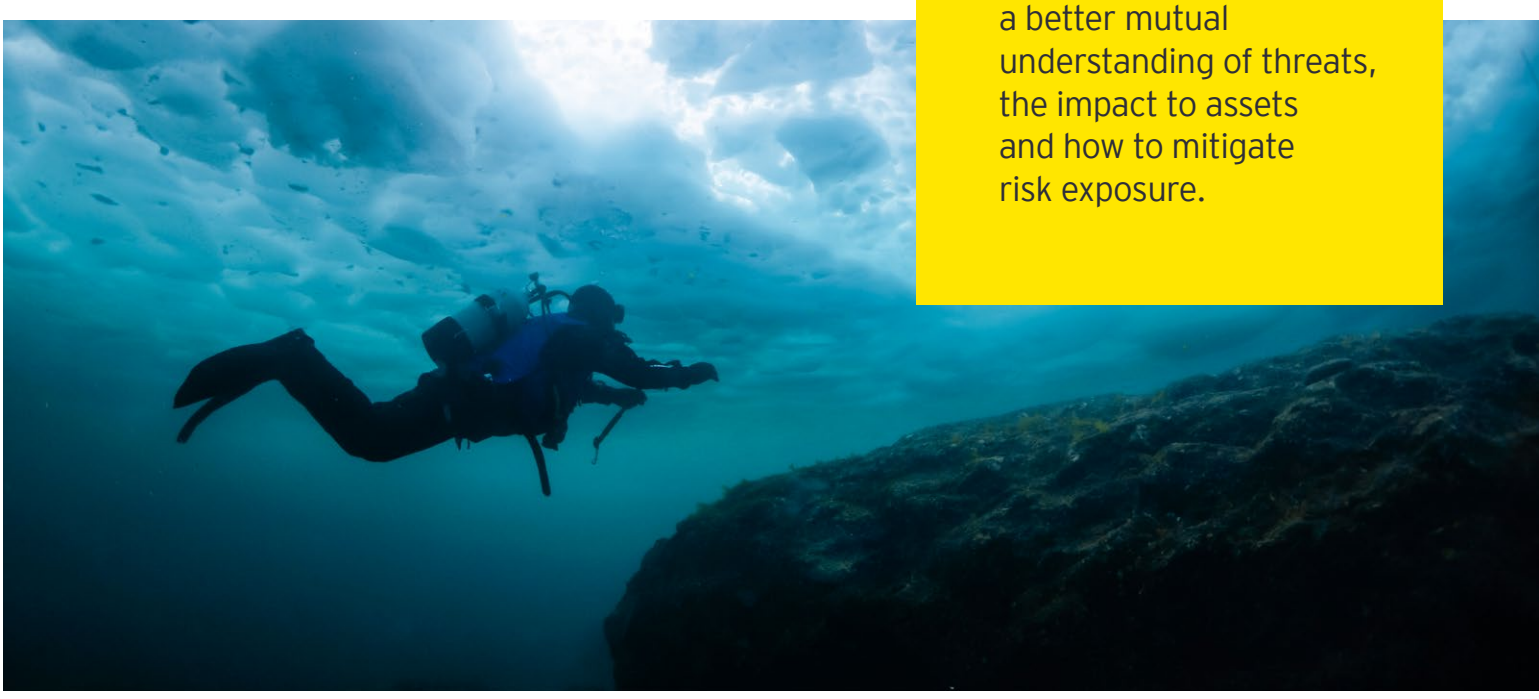
Canadian organizations indicated the following as their top 3 challenges in managing the cybersecurity function:



WHAT CAN YOU DO TODAY?

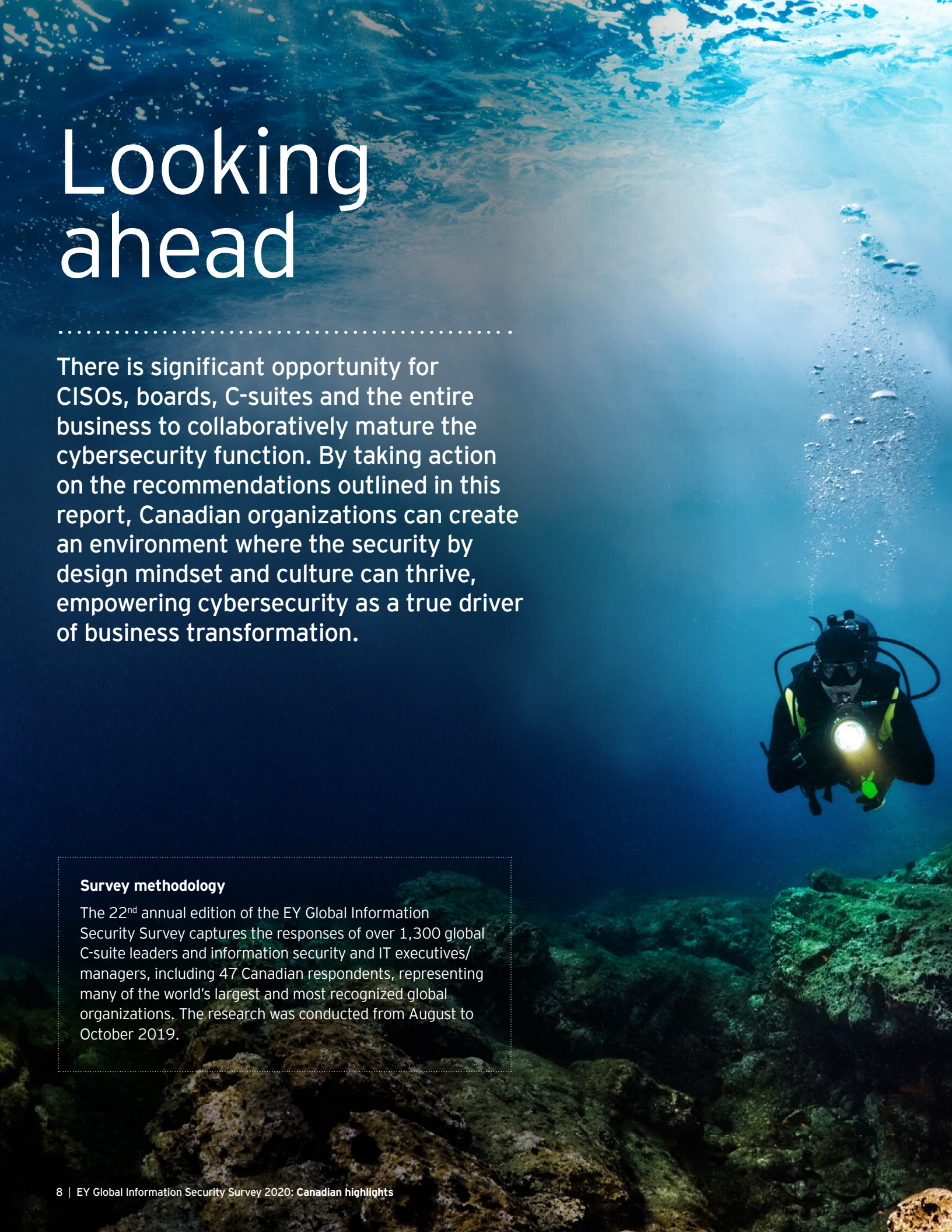
Knowing the activities of each business function and what is needed from cybersecurity requires strong, productive alliances. The conversation must focus on cyber risk experience, possible impacts and business continuity to effectively mitigate risks.

- The security function needs to understand the critical assets and operational processes for each line of business.
- Business lines need to understand the impact of key assets and the possible consequences if they are disrupted.
- These alliances create a better mutual understanding of threats, the impact to assets and how to mitigate risk exposure.



Looking ahead

There is significant opportunity for CISOs, boards, C-suites and the entire business to collaboratively mature the cybersecurity function. By taking action on the recommendations outlined in this report, Canadian organizations can create an environment where the security by design mindset and culture can thrive, empowering cybersecurity as a true driver of business transformation.



Survey methodology

The 22nd annual edition of the EY Global Information Security Survey captures the responses of over 1,300 global C-suite leaders and information security and IT executives/ managers, including 47 Canadian respondents, representing many of the world's largest and most recognized global organizations. The research was conducted from August to October 2019.

For a conversation on maturing your cybersecurity strategy, please contact a member of our Cybersecurity team.

CENTRAL CANADA

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

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

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

WESTERN CANADA

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

EASTERN CANADA

Nicola Vizioli
Associate Partner, Cybersecurity
nicola.vizioli@ca.ey.com
+1 514 879 8046

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.

3487373
ED none

ey.com/ca/cyber