



**The changing faces  
of cybersecurity**

Closing the cyber risk gap

Cyber Risk ●

# Table of contents

<b>Executive summary .....</b>	<b>1</b>
<b>1. Introduction .....</b>	<b>4</b>
Cyber risk in a data-driven, distributed, machine-enabled world.....	5
Closing the cyber risk gap: the human factor.....	6
Moving past the cybersecurity talent shortage .....	7
<b>2. Canada’s cybersecurity talent challenge .....</b>	<b>8</b>
Businesses.....	11
Educational institutions .....	15
Governments.....	17
<b>3. The changing faces of cybersecurity .....</b>	<b>18</b>
Humanizing cybersecurity .....	20
The future will look different .....	24
<b>4. Recommendations and next steps .....</b>	<b>26</b>
Strategy and culture .....	27
The talent life cycle.....	30
<b>5. Conclusion .....</b>	<b>38</b>
Acknowledgments.....	40
Endnotes.....	40
Contacts .....	41

# Executive summary

The world is facing a chronic shortage of cybersecurity talent as new technologies and evolving threats increase the level of cyber risk at a faster pace than existing cybersecurity teams can handle.

In this report, we introduce a new way of thinking about cybersecurity talent: using a human-centric framework to examine Canada's cybersecurity talent challenge, how it is changing, and what key levers businesses, educational institutions, and governments can pull to move past the talent shortage and close the cyber risk gap.

Our findings and analysis are based on interviews and discussions with more than 40 Canadian cybersecurity leaders, educators, and administrators, as well as an in-depth survey of more than 110 Canadian executives from financial services and other key sectors in our economy.

## Canada's cybersecurity talent challenge

Organizations all across the country are being affected by technological evolution and need to constantly improve their cybersecurity capabilities. This trend is creating unprecedented demand for cybersecurity professionals, making the cyber talent shortage one of Canada's most critical challenges.

Deloitte and Toronto Financial Services Alliance joined forces to understand the problem, and offer a path forward to solve it. What we found is that whether you are a leader in financial services, retail, or energy and resources, the challenges and opportunities are similar across the country.

According to our analysis, demand for cyber talent in Canada is increasing by 7 percent annually, with organizations needing to fill some 8,000 cybersecurity roles between 2016 and 2021. Business, government, and academia are all taking steps to close the cyber talent gap; however, their existing efforts and traditional approaches may not be sufficient to solve the problem.

## The changing faces of cybersecurity

Success will require fresh thinking and a fresh perspective. Specifically, a new cyber talent framework that can inspire new and innovative ways to tackle the talent shortage by viewing it through a human-centric lens.

Deloitte's cyber talent framework centres around seven cybersecurity personas: Strategist, Advisor, Defender, Firefighter, Hacker, Scientist, and Sleuth. These personas put a human face on the complex sets of capabilities required for effective cybersecurity. This naming convention makes the required capabilities easier for non-technologists to understand, as well as more stable than traditional cyber talent descriptions and requirements, which tend to focus on narrow technical skills that can quickly become outdated.

The framework's ability to remain relevant and valid in a shifting landscape is especially important given the rapid pace of change in cybersecurity.



## Recommendations and next steps

Applying a human-centric lens to the Canadian ecosystem for cyber talent reveals critical action items that affect every stage of the employee life cycle, from growing the overall talent pool and recruiting the right people to onboarding new hires, continuously developing new skills and expertise, retaining top talent, and even offboarding people in a way that protects an organization's talent brand.

Emerging technologies such as automation and artificial intelligence can and should be used to augment an organization's traditional cybersecurity efforts. However, such technologies do not eliminate the need for human experts.

Governments at all levels play an important role in the cybersecurity talent ecosystem, not only in terms of needing such talent to protect public systems and data, but also in terms of establishing policies and programs to help address the talent shortage.

The cyber talent gap is a global risk; but if courageous enough and with coordination between governments, educational institutions, and businesses, Canada can rise and be seen as a leader by making bold moves and changing the face of this challenge.





1

# Introduction

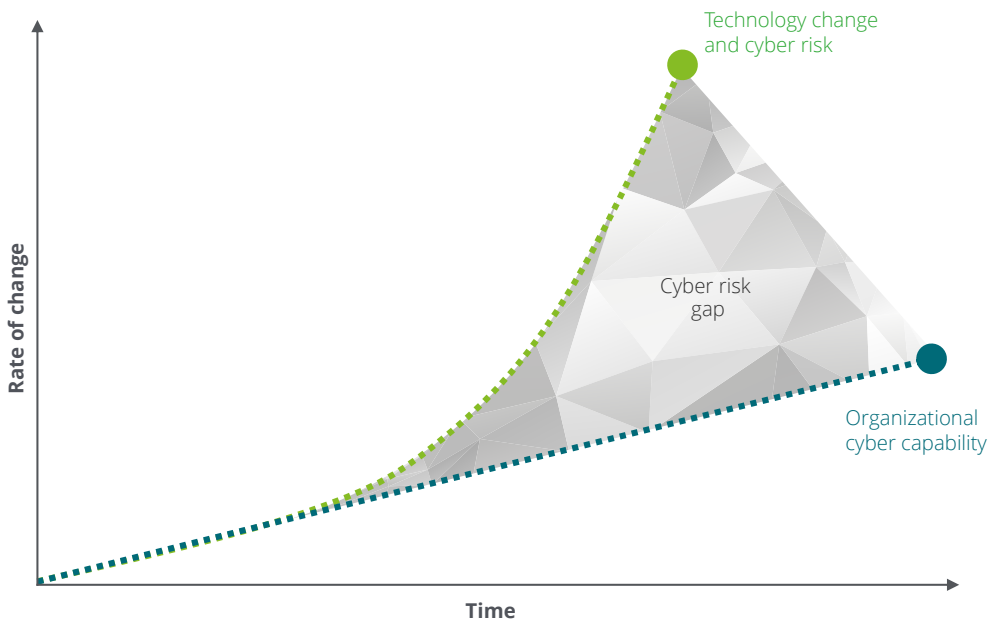
### Cyber risk in a data-driven distributed, machine-enabled world

Rapid technological evolution is changing the way businesses operate. Emerging technologies such as the Internet of Things, cloud computing, automation, and artificial intelligence (AI) are enabling new data-driven, distributed, machine-enabled business models and creating unprecedented opportunities to unlock new value.

This value, however, is not guaranteed. As technology advances, so does the level of cyber risk that organizations must navigate. In fact, analysts estimate that cyber risk globally “could slow the pace of technological innovation by as much as US\$3 trillion in lost economic value in 2020.”<sup>1</sup>

Unfortunately, the rapid march of technology and its associated cyber risks seems to be outpacing the ability of organizations to adapt. Despite significant investments in cybersecurity over the past decade, organizations in every industry are facing a growing cyber risk gap. (Figure 1).

Figure 1: The growing cyber risk gap



#### Cyber risk drivers:

- Proliferation of personal data and economic value online
- Broader cyberattack surface
- More sophisticated cyber threats
- Increased consumer and regulatory pressures for security and privacy

### Closing the cyber risk gap: the human factor

Reducing the widening cyber risk gap and enabling organizations to capture the full promise of new technologies is a defining challenge of our time. A critical element in this quest is the human factor: the cybersecurity professionals who work to protect systems and data every day.

It's no secret that organizations globally face a growing shortage of cybersecurity professionals. According to the latest estimates, the world is "on pace to reach a cybersecurity workforce gap of 1.8 million

by 2022, a 20 percent increase over the forecast made in 2015."<sup>2</sup> This is a staggering figure that will have a major impact on businesses and governments alike.

The good news is that many of the same technologies driving increased cyber risk can also be harnessed to improve productivity and reduce reliance on highly skilled human experts in a tight cyber talent market.

This concept, supported by a growing body of research, is known as **augmented security**.<sup>3</sup> (Figure 2).

Figure 2: Augmented security





These opportunities are promising. And in light of the widening talent gap, organizations really have no choice but to pursue them.

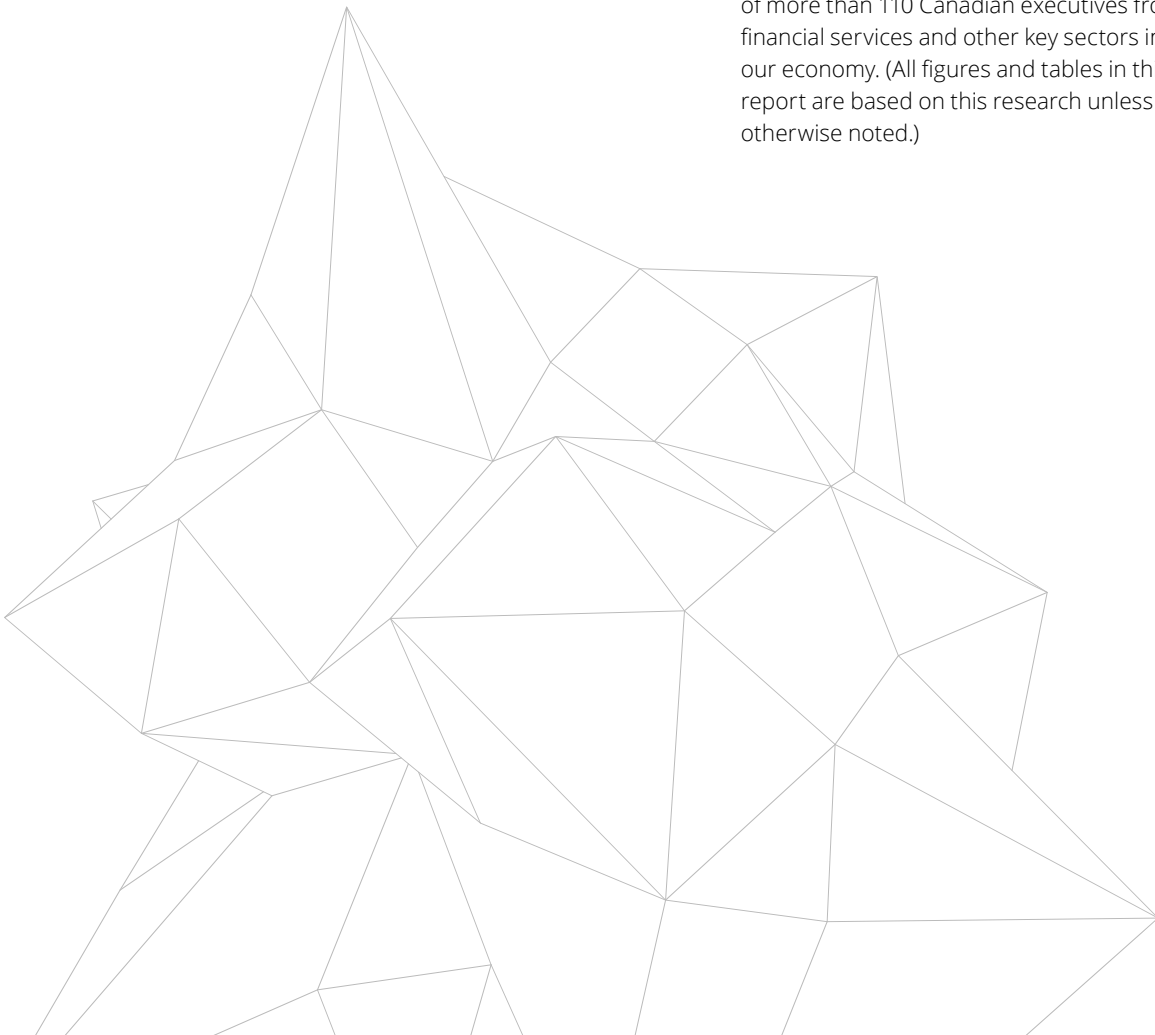
However, while technology-led advancements will drive significant value for cybersecurity teams, solving the cybersecurity talent shortage will require more. In particular, it will require thinking differently about the problem—putting a human face on the challenges and solutions.

## Moving past the cybersecurity talent shortage

This study, conducted by Deloitte and Toronto Financial Services Alliance, articulates a new way of viewing cybersecurity talent: using a human-centric frame to understand the changing faces of cybersecurity.

Through this lens—and with a specific focus on Canada—we examine our nation's cybersecurity talent challenge. We look at how it is changing, and what key levers academic institutions, governments, and businesses can pull to move past the cybersecurity talent shortage and close the cyber risk gap.

This research reflects interviews and discussions with more than 40 Canadian cybersecurity leaders, educators, and administrators, as well as an in-depth survey of more than 110 Canadian executives from financial services and other key sectors in our economy. (All figures and tables in this report are based on this research unless otherwise noted.)





2

Canada's  
cybersecurity  
talent challenge

All of Canada’s major industries—including financial services, retail, and energy and resources—are being affected by technological evolution and need to continue their investment in cybersecurity capabilities.

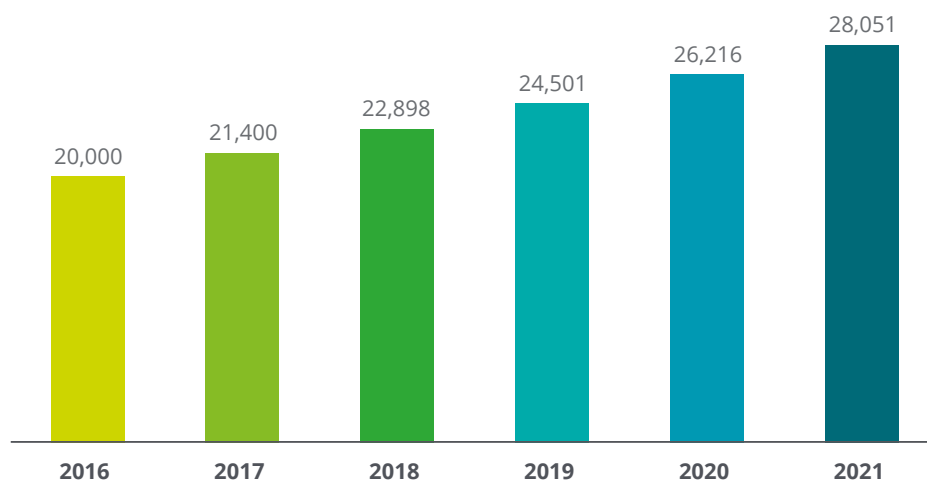
This trend is increasing demand for cybersecurity professionals. Based on data from the Information and Communications Technology Council<sup>4</sup> and Statistics Canada,<sup>5</sup> we estimate that there were approximately 20,000 cybersecurity professionals employed in Canada across all industries in 2016. This conservative estimate represents about 1.6 percent of all information and communication technology (ICT) professionals in the country.

For reference, industry analysts estimate that cybersecurity professionals typically

comprise about 5-6 percent of an organization’s IT staff, which if correct would magnify of the problem.

By 2021, we estimate the number of cybersecurity professionals in Canada will rise to approximately 28,000, representing a compound annual growth rate of about 7 percent and approaching 2 percent of all ICT professionals. Extrapolating from this data suggests that Canadian organizations will need to fill some 8,000 cybersecurity roles between 2016 and 2021. (Figure 3).

**Figure 3: Demand for cyber talent in Canada**



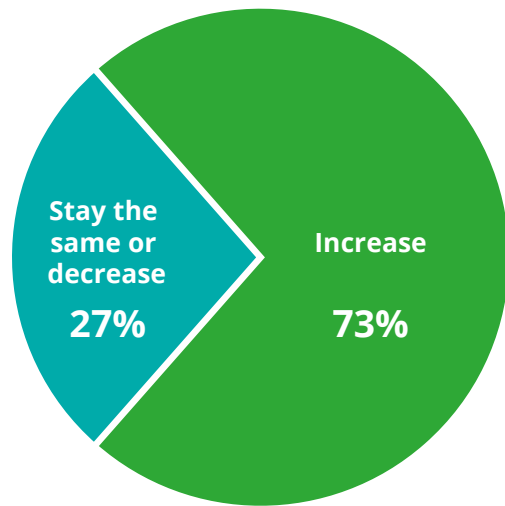
**Source:** Deloitte analysis based on data from ICTC, Statistics Canada. *Canada's educational portrait, 2016 Census of Population, 2017*, <http://www.statcan.gc.ca/pub/11-627-m/11-627-m2017036-eng.htm>

These estimates are consistent with our survey results. According to the survey, 73 percent of Canadian executives expect the number of full-time cybersecurity staff to increase over the next three to five years, with a quarter of respondents expecting their cyber teams to grow by more than 25 percent. (Figure 4). Layered with the fact that we are seeing an increase in traditional cybersecurity staff integrating with fraud teams, corporate

security teams, and other functions, the potential demand is much more daunting.

As these numbers indicate, our nation's demand for cybersecurity professionals is expected to grow significantly in the years to come. The question then becomes: How prepared is Canada to meet the cybersecurity talent challenge—and how are businesses, educational institutions, and governments navigating the headwinds?

**Figure 4: Organizational cybersecurity talent growth trends**



## Businesses

Canadian executives view the cybersecurity talent shortage as one of the top five challenges to managing cybersecurity within their organizations. Moreover, the other four challenges (evolving threat landscape; pace of change; need for security/privacy compliance; disparate security tools) all directly drive demand for increased cyber talent. (Figure 5).

These challenges are not expected to abate any time soon. Looking ahead, survey

respondents highlight “increased frequency and complexity of cyber threats and increased security and privacy regulation” as the trends that will have the most impact on their cybersecurity over the next three to five years.

Leading Canadian businesses are already taking steps to address the cyber talent gap. However, despite their efforts, three specific challenges continue to plague chief information security officers (CISOs): talent life cycle management, productivity, and inclusion.

Figure 5: Top challenges to managing cybersecurity and the cyber risk gap

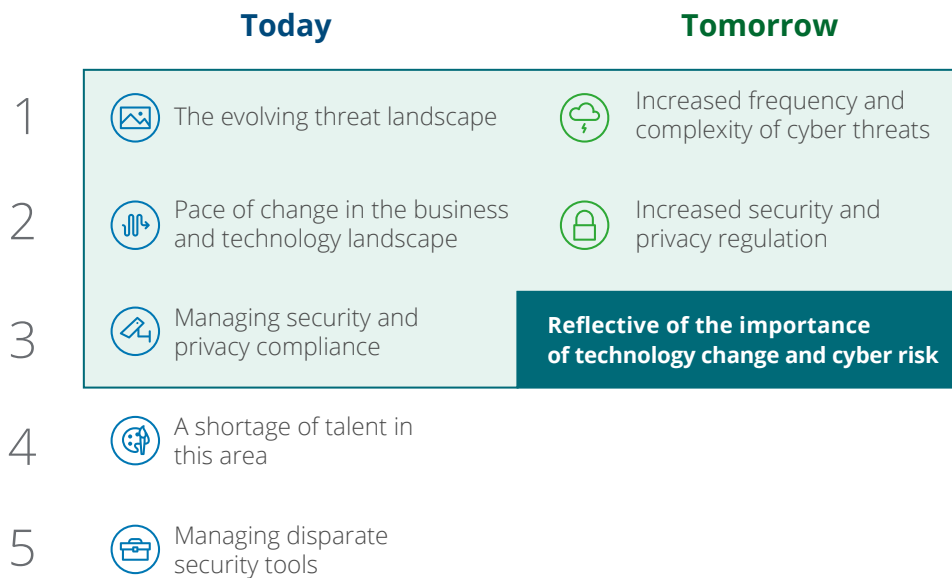
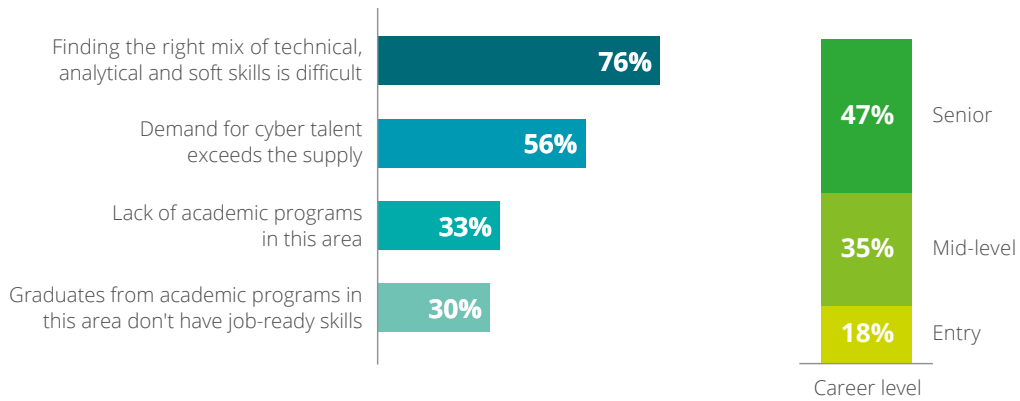


Figure 6: Top recruitment challenges and difficulty by career level



### Talent life cycle management

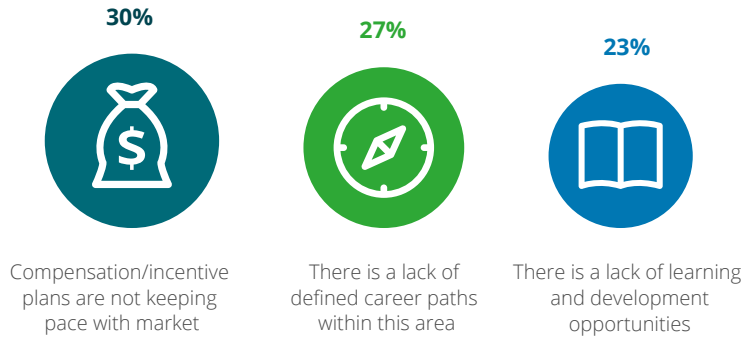
Recruiting, developing, and retaining cybersecurity professionals remains an ongoing challenge. According to our survey, there are a number of specific pain points:

*Recruitment.* The top recruitment challenge for organizations is finding the right mix of technical, analytical, and soft skills. (Figure 6).

When asked to rank the difficulty of recruiting cyber talent at various levels, respondents highlighted senior and mid-level recruiting as being particularly hard. (Figure 6).

The recruiting challenge is amplified by the traditional focus on narrow technical skills, with job descriptions that are increasingly esoteric.

Figure 7: Development and retention challenges



*Development and retention.* Compensation and incentive plans are not keeping pace with market rates—which are continually inflated due to the lack of supply to meet demand—making it difficult to attract and retain qualified cyber talent (including talent from other parts of the business). Additional challenges include a lack of defined career paths in cybersecurity, and a lack of learning and development opportunities. (Figure 7).

These challenges are not unique to Canada. In a recent survey, the Enterprise Security Group found that 66 percent of cybersecurity professionals globally do not have a clearly defined career path or plan for taking their careers to the next level. Also, 60 percent of respondents range from only “somewhat satisfied” to “not at all satisfied” with their current positions.<sup>6</sup>

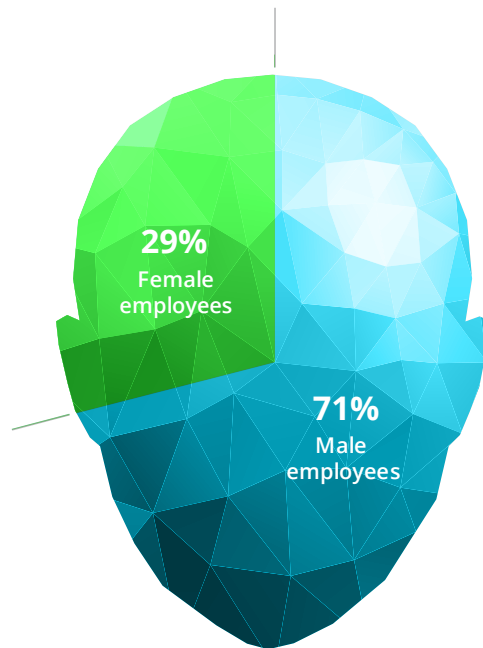
In combination, the challenges that Canadian businesses face in recruiting, developing, and retaining cyber talent lead to two primary effects: a limited ability to hire the right people at the right time and a transient workforce where investments in development could be negated by employees switching companies frequently.

### Productivity

An open secret within the cybersecurity community is that the cybersecurity function faces a major productivity challenge.

A recent study found that organizations across Canada collectively spend about 21,000 hours investigating false or erroneous security alerts, which translates to a cost of roughly \$1.3 million annually.<sup>7</sup> This whack-a-mole approach is partially a function of attacker/defender asymmetry: attackers need to get things right only once in order to cause significant damage, whereas defenders need to get things right all the time. However, the problem is exacerbated by the fact that the typical CISO is tasked with managing more than 70 cybersecurity tools<sup>8</sup> in a business, technology, and vendor environment that is constantly changing. The productivity challenge will only increase as organizations continue to invest in advanced technologies.

Figure 8: Cybersecurity and gender in Canada



### Inclusion

Today's cybersecurity professionals tend to be predominantly male and come from an information technology background. This narrow profile suggests there may be significant untapped potential to address the cyber talent shortage through greater inclusion.

According to our survey results, the average Canadian cybersecurity team is only 29 percent female (Figure 8). In some respects, this is a positive finding since it is much higher than the global average of 11 percent.<sup>9</sup> However, there is still significant room for improvement—especially at the executive level. Our research could find only a handful of female senior executives currently leading major cybersecurity organizations in Canada.

Monolithic backgrounds are also prevalent. According to a study by the International Information Systems Security Certification Consortium (ISC<sup>2</sup>), 70 percent of cybersecurity professionals in North America come from an IT background.<sup>10</sup> Although this is not necessarily a problem, it artificially limits the potential talent pool, potentially inhibits new perspectives and thinking, and may not align with the skills and expertise that businesses will need to manage cybersecurity effectively in the future.



### Educational institutions

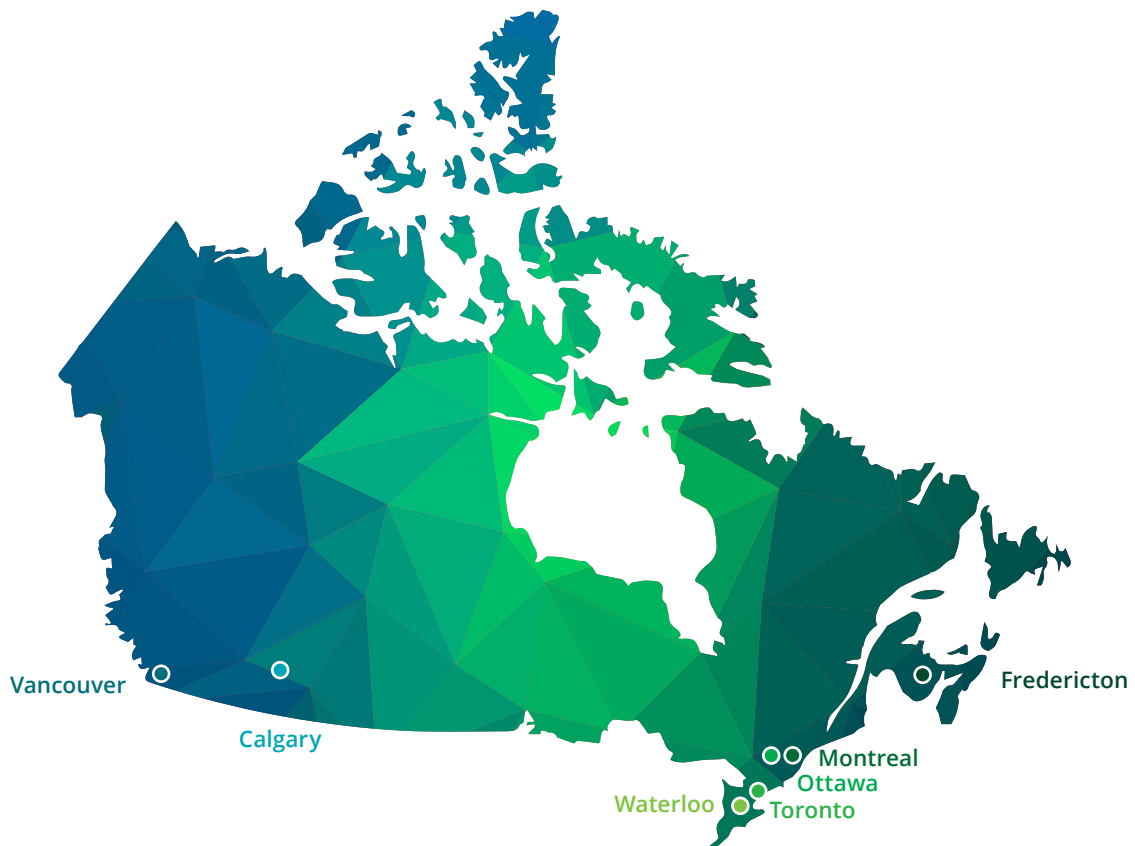
Education is a top priority for Canadians. Our nation boasts a highly regarded educational system, and nearly two-thirds of Canadian adults have completed post-secondary education.<sup>11</sup>

In the area of cybersecurity, educational institutions across the country are playing

an important role as the organic pipeline for cybersecurity talent. (Figure 9).

Canada's educational system recognizes the need to develop cybersecurity talent, and institutions at every level are taking active steps to address the issue. However, there are still significant challenges with which to contend.

Figure 9: Cybersecurity academic hubs in Canada

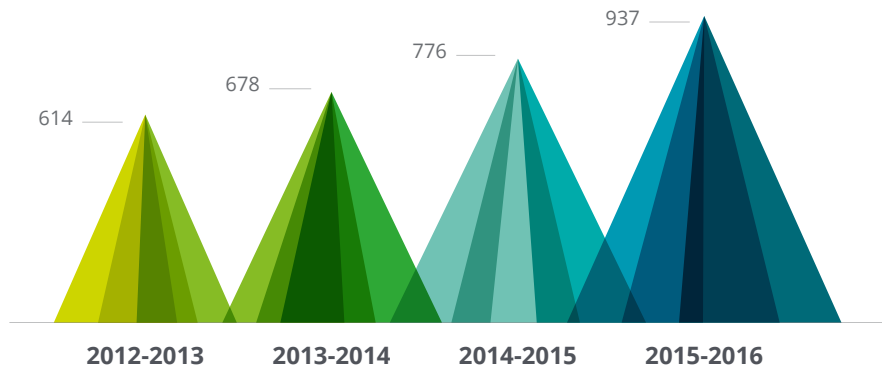


### Colleges make strides, but struggle to keep up

Colleges have been effective in responding to market demand—both from employers and students—and are actively developing the next generation of cyber professionals. This trend is playing out across the country.

For example, in Ontario alone, college enrolment in cybersecurity-focused programs has grown consistently, reaching the level of nearly 1,000 students in 2015-2016.<sup>12</sup> (Figure 10).

Figure 10: Enrolment in cybersecurity-focused college programs (Ontario)



Source: Advanced Education and Skills Development, April 8, 2014, <https://www.ontario.ca/data/college-enrolment>

This rising level of enrolment in cybersecurity programs represents about 7 percent of all college IT enrolments in Ontario.

Colleges across Canada are trying hard to keep pace with the increased demand for cybersecurity education. However, they are encountering a number of significant obstacles. According to our focus group discussion, the field of cybersecurity is moving so quickly that educators find it difficult to keep their curricula up to date. Indeed, specific skills are susceptible to disruption and obsolescence in the blink of an eye—particularly in cybersecurity, where technologies and cyber threats are evolving at a dizzying pace. And, ironically, the cyber talent shortage makes it hard to attract the qualified instructors necessary to train a larger pool of talent. These obstacles are making it difficult for colleges to fully satisfy the needs of the marketplace.

### Universities have strengths to build on, but friction to overcome

Canadian universities are strong in science, technology, engineering, and math (STEM) education, and our focus group showed high student demand for cybersecurity programming at both the undergraduate and graduate levels.

A number of universities have renowned research centres and cybersecurity specializations within broader programs. For example, the computer security stream within Carleton University's computer science program currently has enrolment of more than 100 students, and is growing steadily. Looking more broadly, the SERENE-RISC organization catalogued 450 cybersecurity-related courses across 60 universities in Canada in 2015.<sup>13</sup> Despite these positive findings, a few notable areas of friction stand out at the university level.

Integration of cybersecurity concepts within broader computer science and engineering curricula remains relatively weak, with cybersecurity courses typically positioned as upper-year electives. When cybersecurity concepts are integrated, such as the concept of validation in computer science, they are not provided the import that the current situation warrants. In civil engineering, for example, safety is taught as a core design component.

More fundamentally, the primary driver for universities is research and intellectual advancement—not market demand. As such, our focus group discussion identified a perceived misalignment of incentives between academia and industry, leading to

friction on both sides. Industry perceives a lack of focus on training cybersecurity graduates who can make an immediate contribution to the business, whereas universities perceive a lack of industry support for academic research in cybersecurity.

### Cybersecurity education must start early

A growing number of jurisdictions in Canada and around the world are starting to provide cybersecurity education to students from kindergarten to Grade 12. In Canada, notable efforts include CyberNB's CyberSmart program<sup>14</sup> in New Brunswick schools. The Sisler High School Virtual Network and Cybersecurity Centre is working to prepare high school students across Manitoba for in-demand careers in entry-level information technology, networking, cybersecurity, and virtualization. Israel and other countries are starting to educate their young people about cybersecurity even earlier.

### Governments

Governments at all levels play an important role in the cybersecurity talent ecosystem, not only in terms of needing cybersecurity talent to protect public systems and data, but also in terms of establishing policies and programs to help address the talent shortage.

### Recognizing the importance of cybersecurity

The Government of Canada has taken key steps to recognize the importance of cybersecurity, committing to invest \$507 million over five years as part of a new national cybersecurity strategy outlined in the 2018 federal budget<sup>15</sup>. A principal objective of the strategy is to build an innovative and adaptive cyber ecosystem.

This includes a stated measure to support the creation of up to 1,000 student work placements in cybersecurity.<sup>16</sup>

At the provincial level, notable initiatives include New Brunswick's aforementioned CyberNB agency, as well as the Ontario government's announced \$64 million investment to "enhance existing cyber practices and attract highly skilled and in-demand cybersecurity talent using new recruitment methods, including through innovative partnerships with postsecondary institutions."<sup>17</sup>

While these are positive steps, they will take time to affect the talent ecosystem, and require significant public/private collaboration to be effective.

### Solving tomorrow's problems today

One of the top cyber challenges for organizations is finding experienced talent right now. Moreover, we see that today's cyber risk gap is increasingly driven by the technologies of tomorrow. This hints at a twofold need:

- 1) to grow the talent pool inorganically through channels such as skilled immigration; and
- 2) to recognize and act on the interdependencies between technology advancements and cyber risk.

Governments at the federal and provincial levels play an important role in both areas.



3

The changing  
faces of  
cybersecurity



Positive progress in business, academia, and government has been made. However, current efforts are likely not sufficient to address the cyber talent shortage effectively.

As some have argued, throwing more technology at the problem is not a panacea.

Success will require fresh thinking and a fresh perspective—specifically, a new cyber talent framework that can inspire new and innovative ways to tackle the problem by viewing it through a human-centric lens.

To be effective, such a framework needs to be stable and informative, featuring

stable groupings of talent (focused on enduring capabilities over ephemeral skills), and providing a useful reference point to understand and plan for changing talent requirements in the context of evolving technology. It also needs to be understandable for non-security individuals, making the cybersecurity profession more accessible and inclusive to a broader audience.

## Humanizing cybersecurity

Building on the Cybersecurity Workforce Framework of the United States' National Institute of Standards and Technology's National Initiative for Cybersecurity Education<sup>18</sup>, our cyber talent model centres around seven cybersecurity personas. (Figure 11).

The model has three components:

- **Personas.** These are personifications of the set of capabilities that apply to various cybersecurity functions.
- **Capabilities.** This refers to the broad capabilities that are transferable across tasks and work environments, focusing on those that are most critical to the work associated with a particular persona.
- **Knowledge and skills.** This is an abstracted list of knowledge and skills necessary to execute specific tasks. These are more resistant to disruption than narrow expertise and training on a particular technology; however, they are the least permanent component of the model.

The personas are organized in the shape of a wheel to illustrate their relationship with one another. Personas that are located side-by-side tend to be more similar than those on opposite sides of the wheel. Also, while each persona is distinct, individual cyber professionals are likely to identify with a primary persona but also have an affinity for neighbouring ones.

Figure 11: Cybersecurity personas



To create stability, the framework prioritizes transferable capabilities over specific skills. Although skills remain important, they need to be viewed in a supporting role, not as the lead act. This means that instead of focusing their hiring and training efforts around specific technical skills, Canadian organizations would likely be better served by thinking in terms of broad “personas” with sustainable capabilities that are portable across different occupations and roles.

The purpose of the model is to provide a basis for understanding current and future cybersecurity workforce dynamics, while facilitating communication, education, recruitment, and workforce planning. By personifying key capability groupings, the model strives to put a human face at the centre of the cyber talent discussion.

# Strategist



*Provides cybersecurity management, direction, and advocacy*

# Advisor



*Advises on the concept, design, and/or building of secure systems and networks*

## Capabilities

-  Influence
-  Communication
-  Leadership
-  Ethical impact





## Knowledge and skills

1. Business acumen
2. Policy, legal, regulatory
3. Security architecture
4. Security risk management

## Common roles

- Chief information security officer
- Cyber strategy analyst
- Cyber policy analyst
- Cyber communications analyst
- Cyber program/product manager

## Capabilities

-  Critical thinking
-  Quantitative
-  Communication
-  Influence

## Knowledge and skills

1. Security risk management
2. Security architecture
3. Policy, legal, regulatory
4. Business acumen

## Common roles

- Security architect
- Security risk analyst
- Application security analyst

# Defender



*Supports, administers, and maintains the security of systems, data, and networks*

# Firefighter



*Identifies, analyzes, and mitigates threats to internal systems, data, and networks*

## Capabilities

-  Judgment
-  Collaboration
-  Threat mindset





## Knowledge and skills

1. Infrastructure security
2. Security tools administration
3. Security risk management
4. Security architecture

## Common roles

- Systems security analyst
- Security administrator

## Capabilities

-  Agility
-  Judgment
-  Critical thinking
-  Threat mindset

## Knowledge and skills

1. Security incident management
2. Security tools administration
3. Infrastructure security
4. IT administration

## Common roles

- Cyber analyst
- Security engineer
- Cyber incident responder
- Vulnerability analyst
- Security operations centre manager



# Hacker



*Conducts specialized threat detection and deception activities to identify and mitigate cybersecurity risks*

# Scientist



*Performs specialized analysis of threat intelligence, and cryptographic and security information to improve security posture*

## Capabilities

-  Threat mindset
-  Critical thinking
-  Creativity
-  Ethical impact




## Knowledge and skills

1. Penetration testing
2. Computer forensics
3. Infrastructure security
4. Threat modelling

## Common roles

- Cyber operator
- Threat hunter

## Capabilities

-  Critical thinking
-  Quantitative
-  Threat mindset

## Knowledge and skills

1. Intelligence analysis
2. Data science
3. Cryptography

## Common roles

- Threat intelligence analyst
- Cyber analytics manager



*Investigates cybersecurity events or crimes related to systems, networks, and digital evidence*

### The future will look different

We have seen how the cyber risk gap is driving increased demand for cybersecurity professionals from a quantitative perspective. By viewing the cybersecurity talent challenge through a human-centric lens, we can better understand how it is changing in qualitative terms.

Looking at the survey results, today's cyber workforce in Canada largely reflects cybersecurity's evolution out of the infrastructure and operations world, with an emphasis on roles to protect infrastructure components, and to detect and respond to standard threats. However, over the next three to five years, survey respondents expect that the less conventional personas—such as the Strategist and Scientist personas—will gain the most importance. (Figure 12).

#### Capabilities

- Threat mindset
- Critical thinking
- Social awareness
- Ethical impact

#### Knowledge and skills

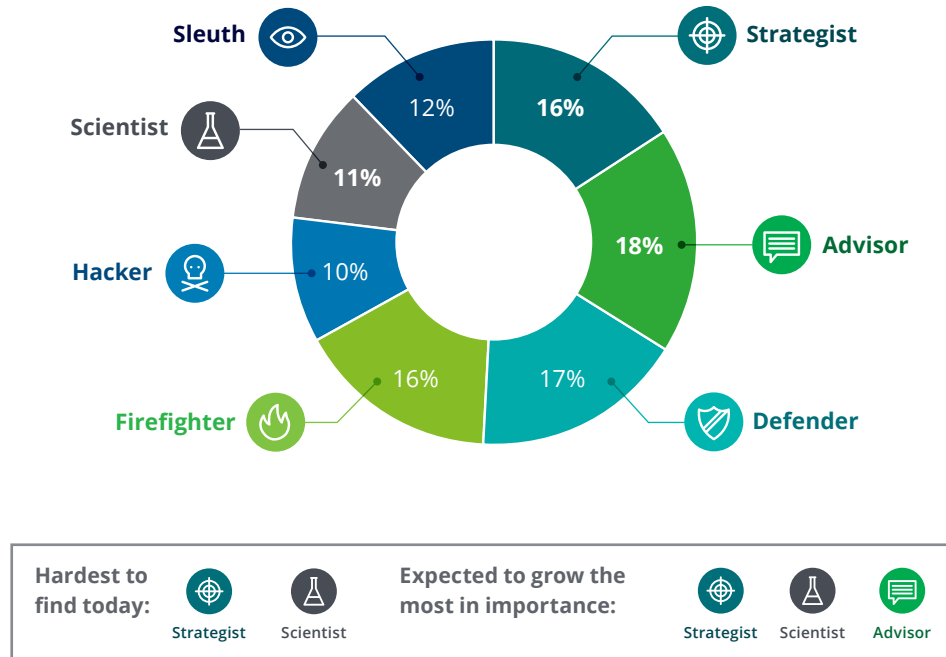
1. Computer forensics
2. Security incident management

#### Common roles

- Cyber forensics analyst



Figure 12: The composition of Canada's cyber workforce



Unfortunately, survey respondents also expect people fitting those two personas will be the hardest to find and recruit.

As businesses and technology delivery models change, Advisors will continue to play a prominent role. In our survey, they are ranked as both the most common cybersecurity professional today and as one of the personas that will become more important in the future. However, the specific role of an Advisor is expected to evolve as hands-on experience with emerging tools (e.g., virtualization, containerization, cloud) becomes increasingly important.

To get the most value from the latest technologies, deep technical expertise will be required in areas such as data science, AI, and machine learning, creating a need for more Scientists.

Defining the problem to be solved continues to be a challenge for many cyber experts who are purely technical. For example, we have seen a growing number of organizations struggle to improve their data science and analytics capabilities

in cybersecurity because they lacked a strategic perspective and context. Also, as the cybersecurity function evolves and matures, navigating the increasingly assertive regulatory requirements and effectively communicating cyber risks to the business will be crucial—thus the increased need for Strategists.

This tension between the need for strategic business acumen and the need for deep technical expertise likely highlights the necessity of defining the next three to five years of cybersecurity. It also hints at a need to create cross-functional partnerships across personas.

Over time, other personas will likely evolve due to disruptive technologies such as robotic process automation, AI, and cloud. Therefore, Defenders may see a reduction in the number of control assessments they need to perform, thanks to automation and AI, along with a shift toward cloud-based managed services. Meanwhile, Firefighters might evolve toward becoming Scientists, as lower-level analysis tasks are increasingly automated.

# 4

## Recommendations and next steps

Applying a human-centric lens to the Canadian ecosystem for cyber talent reveals critical action items for educational institutions, governments, and businesses alike to strengthen our competitiveness on the global stage by securely harnessing the full power and promise of emerging technologies. To succeed, bold moves will be required to move past the cybersecurity talent shortage and close the cyber risk gap.

### Strategy and culture

Overcoming the cyber talent shortage and tackling cyber risk effectively will require an innovative talent strategy, supported by a consistent culture and underlying human and technology infrastructure.

When trying to attract and retain cyber talent, many organizations gravitate toward specific tactics such as hackathons or flexible work programs but lose sight of their overall talent strategy—and the need to build a sustainable talent model.

An organization's cyber talent strategy provides the foundation to identify and align a diverse set of targeted talent tactics, ensuring it will have a plan to access scarce talent and to engage them throughout the talent life cycle. If your organization is ready to transform its cybersecurity talent approach, start with some of the key considerations:

### Vision

Your organization's cybersecurity vision will dictate your organizational structure and the capabilities, skill sets and behaviours required. Each organization will have a unique mix of the personas outlined in the talent framework. For example, the evolution from a technology-centric, IT-focused security program to a program where cybersecurity is embedded throughout the organization will require a different talent model—and potentially a different set of skills. To make such a shift, cybersecurity organizations need to move away from hierarchical models by eliminating layers and placing accountability closer to where decisions have the most direct impact. A greater emphasis on empowerment, communication, collaboration, and business knowledge/appreciation will be needed.



#### Financial services employers partner to move the talent needle

Toronto Financial Services Alliance (TFSA) has developed a coordinated cybersecurity talent strategy to measurably increase the Toronto region's cybersecurity talent pool in financial services through targeted investments. A recently created employer working group has begun to prioritize the development and execution of sector-wide cyber talent initiatives, starting with college collaboration to tailor a post-graduate certificate in cybersecurity that is more suited to industry needs.

"The cyber talent shortage affects all financial services employers, and the demand for talent is outpacing individual recruitment efforts," says Sashya D'Souza, TFSA's senior vice president of talent initiatives. "Participating in TFSA's cybersecurity talent strategy allows our members to operate at a more strategic level to generate solutions that narrow the gap."

### Talent value proposition

The next step is to articulate a talent value proposition that aligns with your vision. Your talent strategy will inform the quality and type of talent needed. The talent value proposition answers the question: “What do you offer your talent in return for them bringing their careers to your organization?”

Consider:

- Defined career paths
- Formal and informal training opportunities
- Incentives and compensation
- Scope of work, experience, and skills gained
- Team structures and access to technical, business, and strategy leaders



#### Deloitte's Talent Value Proposition (TVP)

As a professional services firm, we know people are our most precious asset. To continue attracting top talent, we recently embarked on a mission to understand *why* our people choose Deloitte, and *what* they consider the most important elements of a talent experience when selecting an employer. The result is what we call the Talent Value Proposition (TVP).

“True market leadership depends on our people, and we know our people have choices,” says Norma Kraay, the firm's managing partner for talent. “Our TVP is the foundation of an employee's talent experience at Deloitte. It's the promises we make to each employee, and to each other, every single day.”

### Workforce gaps

Gathering data about your current workforce enables you to thoughtfully and effectively identify and remediate gaps in capabilities, skills, and behaviours.

Key data on areas of work, skills, and gaps provides information to make strategic decisions about alternate ways to approach the work.

- Are there work streams that might be better handled through alternative sourcing or managed services?
- Can cognitive technologies and automation (e.g., automated detection of threats) be used to reduce human involvement?
- Can skills be combined in new ways to solve difficult problems and drive innovation?

Creating a plan to reframe work and maximize existing skill sets allows scarce cyber talent to focus on activities that require human expertise, such as understanding the organization's overall risk profile and setting leadership priorities. Many security organizations are leveraging the latest practices from product/software development by organizing activities around shared objectives, not functions—combining diverse groups of people (e.g., pairing Strategists with Scientists) and giving them a shared objective to work toward.

### New talent models

Non-traditional talent models can help you make the most of limited cyber resources. For example, you can create an agile organization enabled by on-demand workforce models using contingent workers to support activities where the required capacity fluctuates (e.g., vendor risk assessments and risk assessments against emerging technologies and projects). You can also harness innovations such as crowdsourcing to gain quick, global insights about problems, or to obtain specialized knowledge in key focus areas.

### Data analytics

In a complex and rapidly changing cyber environment, harnessing the power of data analytics to tackle cyber talent challenges should be a standard operating practice.

Just as today's businesses are now using customer data to design customer experiences and products that better meet the needs and desires of their customers, forward-thinking security organizations can use data analytics to uncover talent trends, skills gaps, and breakthrough insights that enable smarter talent decisions.

The latest talent analytics capabilities can facilitate a new approach to workforce planning, and can change the game in forecasting talent needs, mapping job categories, anticipating redundancies, and predicting talent supply and demand.

### Culture and talent brand

To achieve and sustain your vision, determine what values you deem most important for your workforce and strategy, and align these throughout your business and operations. That said, keep in mind that today's top talent wants to engage in meaningful work—and organizations would do well to highlight why the cybersecurity function is so critical.

Build and actively live a culture and brand that connects with the cyber workforce you are targeting.

Increase your competitiveness by providing competitive pay, freedom to make an impact, and accountability to perform—and make tough performance choices early in order to avoid mismatched skills and behaviours.

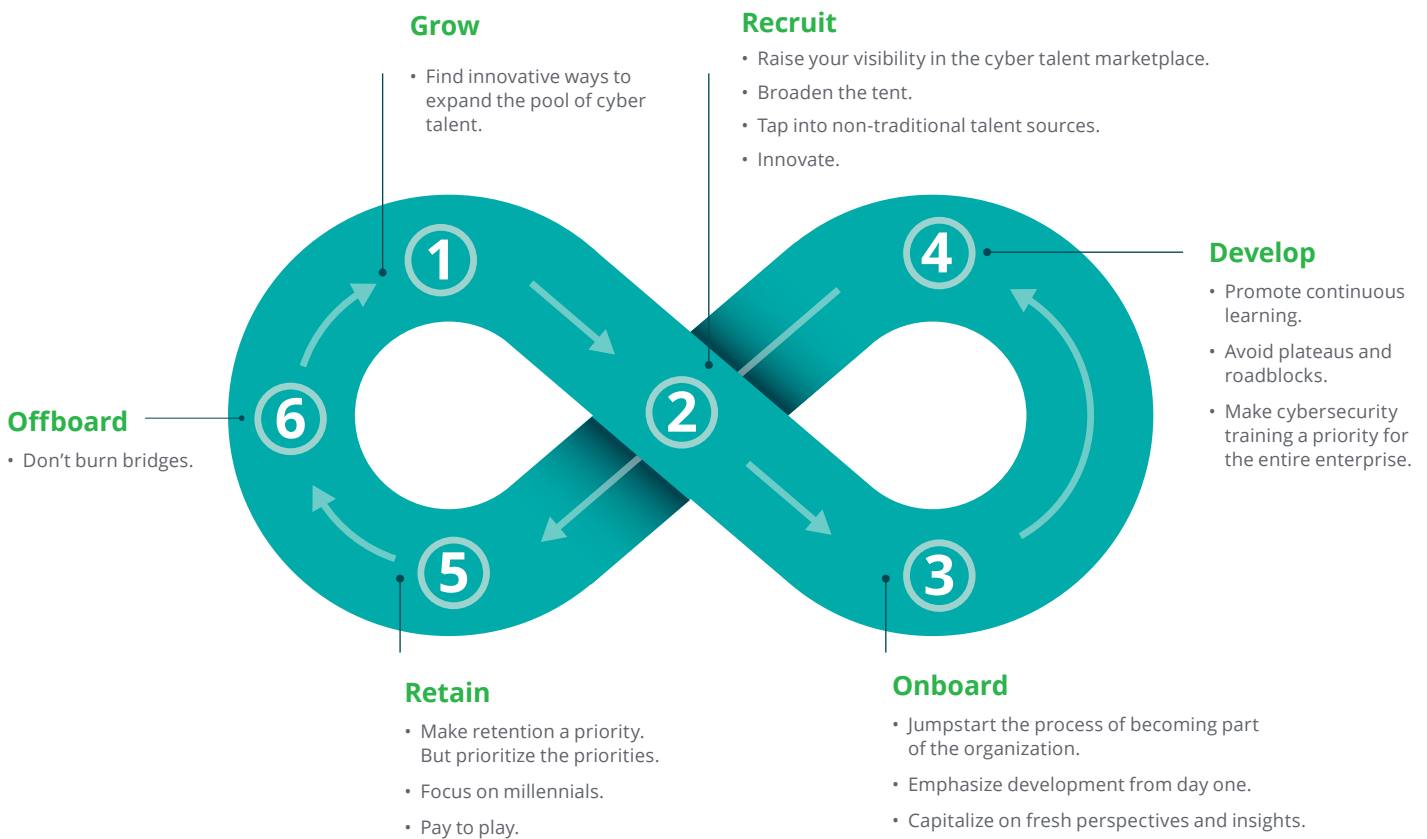
Encourage personal engagement and commitment by providing meaningful work, a positive and trusting work environment, effective management practices and behaviours, and opportunities for growth and development.



## The talent life cycle

An effective way to operationalize your cyber talent program is to organize it around the talent life cycle model: grow, recruit, onboard, develop, retain, and offboard. (Figure 13).

Figure 13: The talent life cycle model



### Grow

**Find innovative ways to expand the pool of cyber talent.** Every organization must shoulder some responsibility for addressing the cyber workforce challenge by working at an ecosystem level to grow the future supply base. This includes educating young people about cybersecurity risks and practices, and building interest in cyber careers.

Today there is a focus on educating youth about the importance of a STEM education and STEM-related career paths. While this focus is important, we also need to look outside of STEM programs for future talent. Different skills and backgrounds are needed across the personas of the cyber talent framework. This talent will increasingly come from non-STEM backgrounds, bringing the skill sets needed in the Strategist and Advisor roles to augment the technically minded Scientists and Sleuths.





### Educating children in STEM, robotics, and computer programming

Chances are, your kids will be working in jobs not yet invented. In Canada and around the world, a fundamental shift is underway toward digitization and using artificial intelligence, robotics, and other advanced technologies to transform businesses across all industries. New jobs are being created while others are being eliminated. On a consumer level, home automation, wearable tech, and programmable robots are transforming how we play and spend our time.

Envision Robotics helps kids develop 21<sup>st</sup> century skills through a STEM-based curriculum using robotics and programming. Armed with these skills, kids will be better prepared for a future full of endless possibilities. “Programs like ours are a critical component to helping Canada solve the domestic skill gap and remain competitive on the world stage,” says John MacKinnon, founder of Envision Robotics.

Exposing developing minds to these challenging fields early in their lives can help shape their interests and positively influence their career choices.

Here are some innovative initiatives taking place around the world to help grow the supply of cyber talent from the ground up:

- In Israel, teaching kids in areas of STEM and cybersecurity is a national mission.
- In the United States, the Girl Scouts have launched new badges in robotics and cybersecurity.
- New startups like Envision Robotics are educating children about the principles of STEM, robotics, and computer programming.
- Deloitte and CoderDojo have formed a community of programming clubs for kids from age seven to 17.
- Carnegie Mellon University's PicoCTF program aims to educate middle- and high-school students about the importance of cybersecurity.
- The Safe and Secure Online program by ISC2 offers resources for educators, leaders, and volunteers to teach cyber safety to the community.
- University College London is teaching girls skills such as coding, app and game development, and cyber fundamentals.



### Upgrading education to keep pace with evolving cyber risk

Polytechnique Montréal and Deloitte have joined forces to revamp Polytechnique's high-calibre training program in the field of cybersecurity. The course content of the three certificate programs in cyber Investigation, online fraud, and IT network computer security have been upgraded to account for current market needs and the changing nature of cybercrimes.

“The Polytechnique and Deloitte collaboration provides students with access to lecturers who have real-world experience with cybersecurity and are among the world's leading experts on cybercrime,” says Amir Belkhelladi, lead partner of the Risk Advisory Security practice in Deloitte's Eastern Region. “As cybercriminals refine their methods, organizations must take steps to ensure that their personnel assigned to cybersecurity stay on top of new threats and the means to counter them. Hence the importance of the training programs offered by Polytechnique.”

Other opportunities to expand the pool of cyber talent include:

- Retraining people already in the workforce and providing a path to transition to a cybersecurity role (e.g., The York University School of Continuing Studies' Certificate in Cybersecurity Fundamentals).
- Increasing the female presence in cybersecurity by working with schools, universities, and recruiters to encourage women to pursue technology careers, and providing them with champions and equal opportunities.
- Building a local cybersecurity ecosystem of educators and employers to reimagine the cyber education experience and align learning with industry skill needs.
- Sponsoring research chairs at universities, and working with colleges and universities to develop and deliver curricula through post-graduate certificates and professional masters programs.
- Working with universities to add or augment cybersecurity courses, fostering collaboration between industry, academia, and government to tailor curriculums.



### Investing in leading-edge cyber education and research

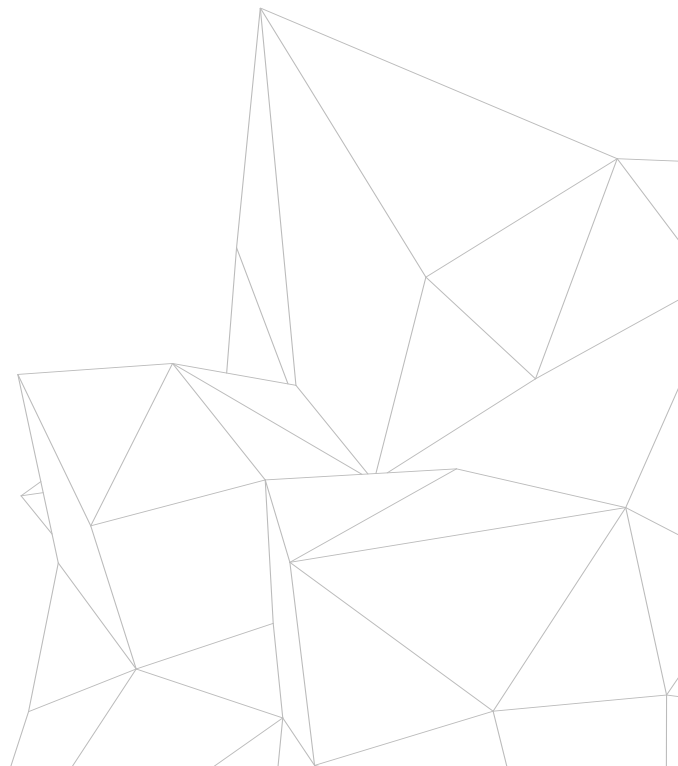
The Royal Bank of Canada (RBC) is opening a cybersecurity lab and investing \$1.78 million to fund cyber research and innovation at the University of Waterloo.

The funding will support cyber-related research in computer science, mathematics, and cybersecurity. Key focus areas include: using machine learning and artificial intelligence to detect and mitigate security threats; developing technologies to enhance the security and privacy of consumer data; and creating strong encryption methods that cannot be cracked by quantum computing.<sup>19</sup>



### Collaborating to reimagine cyber education and build a Canadian cybersecurity ecosystem

The City of Brampton and Government of Ontario are collaborating with Ryerson University and Sheridan College to create a post-secondary campus in Brampton. The site will house a national centre for cybersecurity; an innovation hub to connect students with external organizations in the region; and a centre for education, innovation, and collaboration. "This groundbreaking collaboration between academia and the public and private sectors is helping create the National Centre of Cybersecurity," says Nick Galletto, who leads the Cyber Risk practice for Deloitte. "Our firm is proud to be part of the effort, helping to create a cybersecurity centre that will fuel the development of cyber solutions and educate future generations of cyber talent."





### Funding research to combat cyber risk in financial services

Scotiabank is donating \$2 million to fund cyber-related research at the University of British Columbia (UBC). Over the next five years, Scotiabank's Cybersecurity and Risk Analytics Initiative will support a variety of research and educational initiatives—including internships, speaker series, and hackathons—to improve the financial services industry's understanding of cyber threats and help develop the tools and talent required to manage cyber risk.

The Scotiabank Cybersecurity and Risk Analytics Initiative at UBC will advance the industry's collective understanding of how to further protect digital assets. At the same time, Scotiabank's support will contribute to research and engage students to advance financial modelling to help manage risks and protect customers.<sup>20</sup>

### Recruit

#### Raise your visibility in the cyber talent marketplace.

Use your overall company value proposition to drive your brand as an employer of choice for cyber talent. Build awareness of cybersecurity as a profession—and your organization as a great place for cyber professionals to work—by offering learning sessions and demonstrations.

**Broaden the pool.** As noted earlier, the vast majority of cybersecurity professionals start their careers in other IT roles. This path will likely expand as technologies such as automation, AI, machine learning, and cloud reduce the need for traditional IT staff.

While deep technical skills are needed for the Scientist, Defender, Firefighter and Hacker roles, many of the cyber personas such as Strategist and Advisor require capabilities outside of the technical arena, such as critical thinking, influencing, threat mindset, and quantitative skills. Indeed, 76 percent of survey respondents indicate that finding the right mix of analytical and soft skills is difficult.

Broadening the talent pool to actively engage early talent from non-STEM programs, and mid-career talent with the requisite core skills, will increase diversity—of thought, experience, culture and gender—and will drive innovation on cyber teams.

Engaging with new graduates of risk management, political science, legal, and business administration (MBA) programs

will provide a deeper early talent pool of candidates with critical thinking, quantitative, and leadership skills.

**Embrace career shifters.** The demand for Strategists and Advisors is increasing, but the timeline to grow early talent into these senior roles is long. Making use of the capabilities and skills of career shifters can solve this gap more quickly and add diversity of experience to teams.

Top candidates include mid-career professionals in internal business functions such as enterprise and IT risk, internal audit, governance, strategy, and stakeholder management. Internal recruits will require an investment in technical training but bring a mature mindset and know how to get things done in your environment—a critical skill that allows them to move up the learning curve more quickly.

Embracing career shifters also represents another opportunity to increase the number of women on cyber teams.

#### Tap into non-traditional talent sources.

Expand your cyber recruitment pipeline into untapped populations and alternative sourcing methods in order to meet your talent needs; for example, veterans' programs and experienced individuals coming out of the Armed Forces. Also, some workers with a technical background and nontraditional education could also be prime candidates for the cybersecurity field. Hire for learning ability versus a purely technical skill set.



### Developing top talent with rotation programs

Sun Life offers five rotational leadership development programs that give a select group of newly hired graduates the opportunity to rotate through diverse roles within the company. These programs, which typically involve working in a variety of locations across Canada, provide promising leadership candidates with a thorough understanding of the financial services business while helping them assess and define their career goals.<sup>21</sup>

Create new partnerships, reaching out to government organizations, educational institutions, and academic programs in your region. Expand talent searches into community colleges, private technical schools, and other educational programs, as a growing number of these institutions are offering cybersecurity programs yet remain untapped by employers.

**Innovate.** Traditional job descriptions and online postings can be passive and ineffective in attracting the breadth of talent needed.

Using the cyber talent framework and the personas as a starting point, work with internal teams and hiring managers to document the capabilities, attributes, and skills that are essential for your organization today and in the future.

Determine which capabilities are mandatory, and which skills can be trained.

Attract non-traditional candidates by creating postings that outline the required skills/training offered trade-off. For example, “If you have these foundational capabilities, we will teach you these advanced skills.”

Outline a potential career path that is attainable once the new skills have been mastered.

Experiment with other innovative and active approaches, such as partnering with campus groups to hold cybersecurity-focused hackathons and case competitions, with winners receiving a “golden ticket” to work for your company.

This hands-on interaction with students provides a much stronger signal of competence, and tests both hard and soft skills. As such, they can be an effective channel for identifying early talent and developing cybersecurity skills.

### Onboard

**Jumpstart the process of becoming part of the organization.** Given the shortage of skilled cybersecurity professionals, it is important to support and engage new hires as soon as they join the team. Quickly immerse new hires into the broader ecosystem by introducing them to groups outside of cybersecurity—such as the application development and digital teams—so they become known and connected.

**Emphasize development from day one.**

In addition to having robust onboarding programs, employers should offer early opportunities for mentorships, rotational assignments, and shadowing more experienced colleagues. Define a career path for all cyber talent, and consider offering a management development program that rotates people through different parts of the business.

**Capitalize on fresh perspectives and insights.**

Assign new employees to work on a variety of projects, and engage them in exploring new technologies and processes. This supports their professional development, allows them to immediately demonstrate their value, and provides the team with a fresh new perspective.

**Develop**

**Promote continuous learning.**

Cybersecurity is a highly dynamic field that requires constant learning and upskilling. Invest in employees to make cyber a career, not just a job. Help them build and refine their skills by providing opportunities to stay current—encouraging them to enroll in classes and conferences, and to pursue certifications. Partner cyber talent with peers from adjacent roles in the talent framework, to extend their skill sets and broaden learning. Foster innovation and creativity by allowing people to dedicate a certain amount of time to projects of their own interest.

**Avoid plateaus and roadblocks.**

While some cybersecurity professionals focus on deepening their technical skills, many are looking for new challenges and more ways to advance their careers. Starting with entry-level roles, define clear career trajectories and expected timelines to advancement. Provide rotational programs and partnering opportunities with other functions to increase exposure and develop experience. Offer intensive coaching, stretch assignments, formal and informal mentorship, and reverse mentorship (where senior leaders learn from junior employees). Apply learning opportunities consistently across the cyber team, supporting mid- and late-career talent in their quest for challenge and skill-building.

**Make cybersecurity training a priority for the entire enterprise.**

When it comes to cybersecurity, an organization's employee base is often the weakest link. To reduce risk, increase your commitment to cyber training and awareness for all employees, helping employees protect the organization and themselves from a security breach. Provide awareness and training that not only reduces their cyber risk at work, but also improves how they and their families interact with information and technology at home.



## Retain

**Make retention a priority.** Organizations that invest in people who are aligned to their talent value proposition are better equipped to attract and retain the type of talent needed to remain competitive. However, it is important to recognize that it is impossible to retain everyone, so you need to be strategic. Identify high performance/high potential talent based on their future potential, leadership skills, hard-to-replace capabilities, and value as role models—and then go the extra mile to ensure you can keep them.

### Focus on:

**Millennials.** With cyber, it is especially important to attract and retain younger workers who are the lifeline of future cybersecurity programs. Offer flexible work schedules, more casual work environments, and locations convenient to where younger workers live. Millennials tend to be interested in working for organizations that align with causes they are passionate about, such as current economic, environmental, and social issues. It is important to invest in corporate responsibility initiatives, and to highlight the societal, economic and business importance of the cybersecurity function.

**Mid/late career workers.** Millennials are purported to be looking for interesting, meaningful work—and it turns out that is true of all talent, across the hierarchy and experience continuum. Retaining mid- and late-career talent ensures that you are retaining your experience base, intellectual capacity, training investment and, in many cases, your succession pipeline. Take the time to survey all employees to ensure that you are delivering on your talent value proposition and are incorporating emerging needs into your plan.

**Pay to play.** We reported earlier in this paper that 30 percent of leaders indicated that compensation/incentive plans are not keeping pace with the market, making this the top development and retention challenge. In a critical, resource-constrained field like cyber, salaries are at a premium, and will likely be higher than internal comparators in other departments.

This creates internal tension as leaders attempt to pay market-competitive rates while staying within formal compensation structures and preserving internal equity. Some flexibility or creativity in corporate compensation programs will be needed to give leaders the tools to attract and retain scarce talent.

### Other tactics to consider:

- Strengthen your brand and talent value proposition to broaden the conversation to more than just compensation.
- Implement automation and cognitive technologies to reduce the need for human expertise.
- Pay for solving difficult challenges—crowdsource your most challenging problems and innovation gaps and offer significant prize money to be paid when solved (\$20,000 to \$50,000 or more depending on the complexity and criticality of the issue).

## Offboard

**Don't burn bridges.** In a high-demand market, it is inevitable that some team members will choose to leave. However, it is important to treat them with respect; they may be future hires down the road. Also, you want former employees to speak favourably about your organization and talent brand when they participate in knowledge-sharing communities. Help people find the right external opportunities if your organization is unable to meet their needs, and learn valuable lessons for improvement whenever someone leaves.

5

Conclusion



Closing the cyber risk gap and enabling organizations to capture the full promise and value of new technologies is a defining opportunity of our time. Emerging technologies such as automation, AI, machine learning, and advanced analytics can help augment an organization's traditional cybersecurity efforts; however, those technologies will not eliminate the need for human experts—at least, not any time soon.

For the foreseeable future, Canadian businesses, educational institutions, and governments that look at the cyber talent shortage through a human-centric lens, and take bold and deliberate steps to overcome the challenges will push ahead of their peers.

Using the cyber talent framework and personas to think about skills and roles more fluidly will help organizations to move away from narrow role discussions and identify the critical skills and capabilities needed for success in the future, a strategy that will strengthen our competitiveness and leadership position on the global stage.

# Acknowledgments

This report was prepared by Deloitte in collaboration with Toronto Financial Services Alliance, which is funded in part by the Government of Ontario. We would like to express our thanks to the financial services and post-secondary institution representatives who contributed during our focus groups as well as all of those who participated in interviews and our survey. The authors would like to acknowledge the invaluable contributions of the TFSA team and the Deloitte research and editorial staff.

A special thanks to Victor Platt and Francesco Cammisa; without whom this work would not have been possible.

# Endnotes

<sup>1</sup> Kaplan, J. M., Bailey, T., Rezek, C., OHalloran, D., & Marcus, A. (2015). *Beyond cybersecurity: Protecting your digital business*. Hoboken, NJ: Wiley.

<sup>2,11</sup> Frost & Sullivan. (2017). 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk. Available at: <https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf>

<sup>3</sup> Deloitte University Press. (2017). Augmented security: How cognitive technologies can address the cyber workforce shortage. Available at: [https://www2.deloitte.com/content/dam/insights/us/articles/3992-Augmented-security/DUP\\_Augmented-security.pdf](https://www2.deloitte.com/content/dam/insights/us/articles/3992-Augmented-security/DUP_Augmented-security.pdf)

<sup>4</sup> Statistics Canada. (2017). Canada's educational portrait, 2016 Census of Population. Available at: <http://www.statcan.gc.ca/pub/11-627-m/11-627-m2017036-eng.htm>

<sup>5</sup> The Information and Communications Technology Council. (April 2017). The Next Talent Wave: Navigating the Digital Shift - Outlook 2021. Available at: [https://www.ictc-ctic.ca/wp-content/uploads/2017/04/ICTC\\_Outlook-2021.pdf](https://www.ictc-ctic.ca/wp-content/uploads/2017/04/ICTC_Outlook-2021.pdf)

<sup>6,9</sup> Oltsik, J. (November 2017). The Life and Times of Cybersecurity Professionals. Available at: <https://cymcdn.com/sites/www.issa.org/resource/resmgr/surveyes/ESG-ISSA-Research-Report-Lif.pdf>

<sup>7</sup> Ponemon Institute LLC. (2017, June). 2017 Cost of Data Breach Study: Global Overview. Available at: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SELO3130WWEN>

<sup>8</sup> Frost & Sullivan. (2017). The 2017 Global Information Security Workforce Study: Women in Cybersecurity. Available at: <https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf>

<sup>11</sup> Statistics Canada. (September 2016). Education in Canada: Attainment, Field of Study and Location of Study. Available at: <http://www12.statcan.gc.ca/nhs-enm/2011/as-sa/99-012-x/99-012-x2011001-eng.cfm>

<sup>12,13</sup> Serene-Risc. (2015). Canadian Cybersecurity Course Directory. Available at: <https://www.ontario.ca/data/college-enrolment>

<sup>14</sup> CyberNB. (2018). Opportunities NB and The Department of Education and Early Childhood Development on Cybersecurity Education and Digital Literacy. Available at: [https://cybernb.ca/wp-content/uploads/2017/09/MOU\\_ONB\\_FECD\\_CYBERSECURITY\\_EDUCATION\\_AND\\_DIGITAL\\_LITERACY\\_EN.pdf](https://cybernb.ca/wp-content/uploads/2017/09/MOU_ONB_FECD_CYBERSECURITY_EDUCATION_AND_DIGITAL_LITERACY_EN.pdf)

<sup>15</sup> Department of Finance. (2018). A Plan for Care and Opportunity. Available at: <http://budget.ontario.ca/2018/chapter-2.html>

<sup>16</sup> Employment and Social Development Canada. (September 2017). Student Work-Integrated Learning Program. Retrieved from [https://www.cewilcanada.ca/Library/SWILP/CAFCE\\_ESDC\\_Webinar\\_Slides.pdf](https://www.cewilcanada.ca/Library/SWILP/CAFCE_ESDC_Webinar_Slides.pdf)

<sup>17</sup> Department of Finance. (2018). A Plan for Care and Opportunity. Available at: <http://budget.ontario.ca/2018/chapter-2.html>

<sup>18</sup> Newhouse, W., Keith, S., Scribner, B., & Witte, G. (August 2017). NICE Cybersecurity Workforce Framework. Available at: <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>

<sup>19</sup> Royal Bank of Canada. (January 2018). RBC to open a cybersecurity lab and fund new research at the University of Waterloo. Available at: <http://www.rbc.com/newsroom/news/2018/20180129-cybersecurity-waterloo.html>

<sup>20</sup> University of British Columbia. (March 2017). Scotiabank funds \$2-million cybersecurity and financial data initiative at UBC. Available at: <https://science.ubc.ca/news/scotiabank-funds-2-million-cybersecurity-and-financial-data-initiative-ubc>

<sup>21</sup> Sun Life Financial. (2018). Rotational Leadership Development Program. [http://www.sunlife.com/us/About+us/Careers/Student+and+new+graduate+programs/ch.Rotational+Leadership+Development+Program.mobile?vgnLocale=en\\_CA](http://www.sunlife.com/us/About+us/Careers/Student+and+new+graduate+programs/ch.Rotational+Leadership+Development+Program.mobile?vgnLocale=en_CA)

# Contacts



## Marc MacKinnon

Deloitte  
National Cyber Strategy Leader  
Partner, Risk Advisory  
mmackinnon@deloitte.ca



## Steve Rampado

Deloitte  
Partner, Risk Advisory  
srampado@deloitte.ca



## Sashya D'Souza

TFSA  
Senior Vice President,  
Talent Initiatives  
sdsouza@tfsa.ca



## Julie Bryski

TFSA  
Director, Talent Initiatives  
jbryski@tfsa.ca

### About Toronto Financial Services Alliance

TFSA is a public-private partnership between three levels of government, the financial services sector and academia. TFSA's mission is to lead collective action that drives the competitiveness and growth of Toronto's financial sector and establishes its prominence as a leading international financial centre. For more information, please visit [tfsa.ca](http://tfsa.ca).



[www.deloitte.ca](http://www.deloitte.ca)

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights and service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 264,000 professionals—9,400 of whom are based in Canada—make an impact that matters, please connect with us on LinkedIn, Twitter or Facebook.

Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

© Deloitte LLP and affiliated entities.

Designed and produced by the Deloitte Design Studio, Canada. 18-5551M