



## **New report introduces innovative framework to grow Canada's cyber talent supply**

*Demand for cybersecurity professionals will reach 28,000 by 2021*

**Toronto, ON, July 4, 2018** – The world is facing a cyber talent deficit and unless countries and organizations make bold moves to address it, their ability to harness the full potential of emerging technology is limited. However, Canada has an opportunity to lead by taking a strategic “human” approach to tackling the problem, according to a new report released today by Deloitte in collaboration with the [Toronto Financial Services Alliance](#) (TFSA).

**[The changing faces of cybersecurity: Closing the cyber risk gap](#)** sheds light on the severity of the issue: organizations 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 a critical global challenge.

Deloitte's analysis reveals that demand for cyber talent in Canada, specifically, is increasing by *7 per cent annually*, with statistics showing Canadian organizations will need to fill approximately 8,000 cybersecurity roles between 2016 and 2021.

The report – based on interviews with more than 40 Canadian cybersecurity leaders as well as an in-depth survey of more than 110 Canadian executives from financial services and other key sectors of our economy – shows that business, government, and academia are all taking steps to close the cyber talent gap. However, their current efforts and traditional approaches may not be sufficient to solve the problem.

“While there has been significant discussion to date around the cybersecurity talent gap, our new report adds a fresh and necessary perspective, putting a human face on the complex sets of capabilities required for effective cybersecurity,” said Marc MacKinnon, a partner and the Canada Cyber Strategy leader at Deloitte. “The report outlines our cyber talent framework, which identifies seven relevant personas to fill the cyber talent gap. The personification of capabilities provides a common reference point to understand and plan for changing talent requirements in the context of evolving technology.”

The report goes on to say that viewing the cyber talent shortage through a human-centric lens makes a career in cybersecurity more accessible. It argues that this approach to talent is more stable than traditional cyber talent descriptions and requirements, which tend to focus on narrow technical skills that can quickly become outdated.

The report finds that overcoming the cyber talent shortage and tackling cyber risk effectively will require organizations to commit to an innovative talent strategy, supported by a consistent and reinforcing culture. This includes, among other things, the necessity of Canadian businesses to articulate a talent value proposition that aligns with their vision and support it with enabling infrastructure, as well as the need for educational institutions to reimagine the cyber education experience and upgrade education to keep pace with evolving cyber risks.



The imperative of governments at all levels to, among other strategies, establish policies and programs to help address the talent shortage, will also play an important role in the cybersecurity talent ecosystem.

“What we heard from business leaders across the country was that the current cybersecurity talent gap is a key focus when managing cybersecurity within organizations,” said MacKinnon. “The increased frequency and complexity of cyber threats as well as increased security and privacy regulation were identified as the most impactful trends on cybersecurity over the next three to five years. As a country, we must continue to strengthen our cybersecurity ecosystem.”

The report also addressed the fact that today’s cybersecurity professionals are predominantly male and come from an IT background. According to the survey results, the average Canadian cybersecurity team is only 29 per cent female. While significantly better than the global average of 11 per cent, there’s room for improvement, and an opportunity to narrow the talent gap by identifying ways to tap into latent potential.

[\*\*\*The changing faces of cybersecurity: Closing the cyber risk gap\*\*\*](#) report serves as a call to action for Canadian business leaders to use the cyber talent framework to think about cybersecurity talent differently, while moving away from narrow role discussions.

“Cybersecurity is of critical importance to Canada’s financial services (FS) firms, which allocate one of the highest dollar amounts to cybersecurity as a percentage of overall IT spend, second only to national governments. Talent is key to the equation,” said Jennifer Reynolds, TFSA’s president and CEO. “Yet, 74 per cent of the FS executives we surveyed are challenged to find the right mix of technical, analytical, and soft skills for cybersecurity roles within their organizations. TFSA is working with our FS members and academic partners to tackle the issue. This new cyber talent framework is an innovative lens through which to do so and will help to inform our efforts.”

“Using the framework 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,” MacKinnon said. “As one of the world’s most digitized economies, we have a duty to help reduce the global cyber talent deficit and an opportunity to lead the charge.”

### **About Deloitte**

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.

**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).

- 30 -

**For more information, please contact:**

Tonya Johnson  
Deloitte  
416-607-0741  
[tonjohnson@deloitte.ca](mailto:tonjohnson@deloitte.ca)

Marilyne Plouffe  
Deloitte  
514-393-5471  
[Mplouffe@deloitte.ca](mailto:Mplouffe@deloitte.ca)

Sonia Prashar (TFSA media contact)  
spPR Inc.  
416-560-6753  
[soniaprashar@sppublicrelations.com](mailto:soniaprashar@sppublicrelations.com)