Deloitte.

Ontario Centres of Excellence

TFSA TORONTO FINANCIAL SERVICES ALLIANCE

# Harnessing the cybersecurity opportunity for growth

## Cybersecurity innovation & the financial services industry in Ontario

October 2016

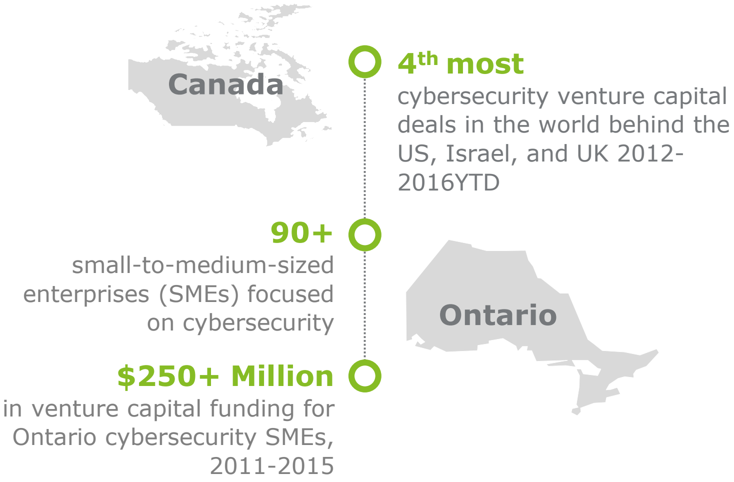
# Contents

# Executive summary

## Background

In the World Economic Forum's Global Risk 2016 report, cybersecurity risk is recognized as one of the top commercial risks along with geopolitics, the environment, and the economy.[1] Following a string of high-profile cyberattacks, with significant value at risk, and increasingly digitized business models, the financial services industry has been particularly impacted by the imperatives of cybersecurity.

Emergent from this heightened risk landscape, however, is opportunity. Opportunity that is driving a new global competitive environment, threatening Ontario's leadership in cybersecurity innovation and financial services.



**4th most** cybersecurity venture capital deals in the world behind the US, Israel, and UK 2012-2016YTD

**90+** small-to-medium-sized enterprises (SMEs) focused on cybersecurity

**$250+ Million** in venture capital funding for Ontario cybersecurity SMEs, 2011-2015

Recognizing this context, a vibrant startup community, and an important financial services cluster in Ontario, the purpose of this study is to understand how to harness the cybersecurity opportunity to position Ontario as a global cybersecurity innovation hub with a focus on the financial services industry.

## Key findings

We found that Ontario has all the ingredients to become a global hub for cybersecurity innovation but has not yet reached the scale and gravity necessary to compete at the highest levels. Our analysis identified a number of areas of strength and friction within Ontario's cybersecurity innovation ecosystem on which to build and solve for:

1. The future of innovation in the financial services industry is intimately linked to cybersecurity creating opportunities for shared growth.
2. While Ontario has organically developed significant clusters of cybersecurity innovation, there is no single centre of gravity, coordination, or systemic catalyst to bring it all together.
3. There is a cybersecurity talent shortage globally and in Ontario.
4. There is limited collaboration on applying Ontario's R&D strengths in related fields to cybersecurity problems.
5. Ontario is well positioned to access some of the largest domestic and international cybersecurity markets and sources of capital. A lack of visibility, a limited culture of 'buying Canadian,' and a relatively risk-averse domestic market has historically hindered this potential advantage for cybersecurity innovators in Ontario.
6. Cybersecurity is an area of strategic collaboration for financial services and other industries.
7. A historically sound regulatory environment has potentially led to a risk-averse approach to innovation within the financial services industry.

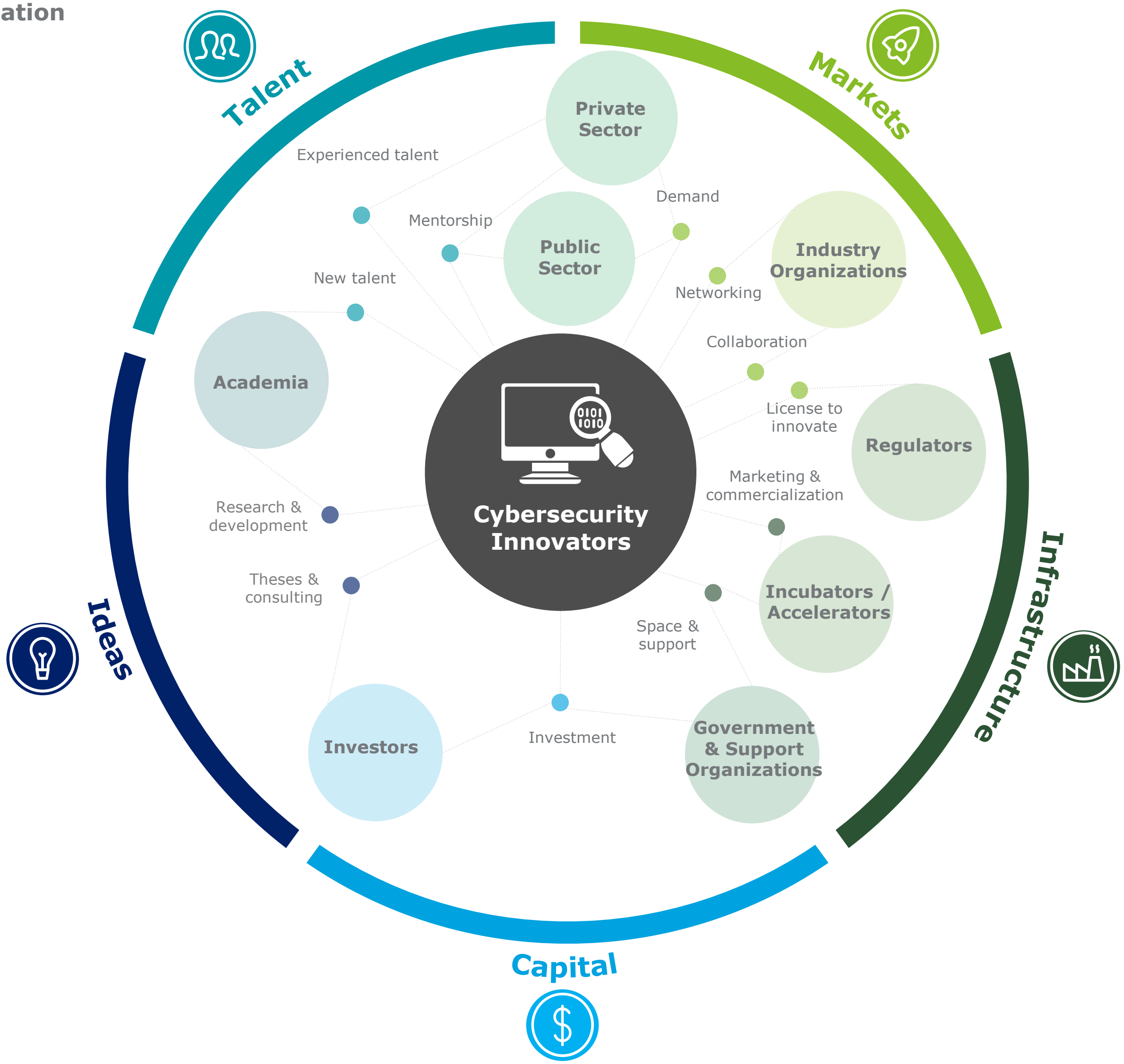
## Call to action

Despite the requisite ingredients and historically strong performance, Ontario risks losing its competitive position through failing to match the concerted efforts of governments and industries around the world who are ramping up investment and coordination in fostering cybersecurity innovation. Focused and immediate intervention by public, private actors is required harness the cybersecurity opportunity and position Ontario as a global cybersecurity innovation hub.

**Ontario must harness the cybersecurity opportunity for growth - the long term security and prosperity of the financial services industry and Ontario's economy may depend on it.**

# Executive summary

## Cybersecurity innovation ecosystem model



# Harnessing the cybersecurity opportunity for growth

Cybersecurity innovation & the financial services industry in Ontario

# Introduction & methodology

## Introduction

In the World Economic Forum's Global Risk 2016 report, cyber risk is recognized as one of the top commercial risks along with geopolitics, the environment, and the economy.[1] Following a string of high-profile cyberattacks, with significant value at risk and increasingly digitized business models, the financial services industry has been particularly impacted by the imperatives of cybersecurity.

In parallel, the financial services industry faces growing competition from new technology-enabled business models threatening to disintermediate incumbent organizations from their customers and unbundle the services they provide. This is forcing financial services firms to up their game and invest to secure new channels, products, and services.

Emerging from this heightened risk landscape, however, is opportunity. Cybersecurity innovators, including many in Ontario, are garnering significant investment, experiencing fast growth, and creating wealth for their economies.

## Research

Recognizing this context, a vibrant startup community, and an important financial services cluster in Ontario, Deloitte has been retained to undertake this study on behalf of Ontario Centres of Excellence (OCE) and the Toronto Financial Services Alliance (TFSA). The purpose of the study was to understand how to harness cybersecurity threats and opportunities to position Ontario as a global cybersecurity innovation hub with a focus on the financial services industry.

## Methodology

The report is comprised of four main sections: The first discusses the trends driving cybersecurity innovation for the financial services industry; the second reviews the innovation opportunity for Ontario; the third assesses Ontario's cybersecurity innovation ecosystem; and the final section outlines our key findings and strategic recommendations on how to position Ontario as a global cybersecurity innovation hub.

In preparing this report, we conducted primary and secondary research and employed an innovation ecosystem model to structure our analysis. Primary research methods included a series of structured interviews with 11 cybersecurity leaders from Ontario's leading financial services institutions. The interviewees were primarily Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) from across the banking (4), insurance (3), lending (1), payments (1), exchange (1), and investment management (1) sectors. We also conducted unstructured interviews with representatives from key ecosystem actors such as incubators, accelerators, venture capitalists, industry organizations, academics, and former cybersecurity startup executives.

In addition, we executed a sensing exercise to identify and profile small-to-medium sized enterprises (SMEs) focusing on cybersecurity within Ontario. We scraped data on these SMEs from public and proprietary sources such as CrunchBase, AngelList, LinkedIn, and PitchBook to identify relevant attributes such as size, location, and funding and exit activity. For the purposes of this exercise, we define cybersecurity SMEs as companies headquartered in Ontario, with fewer than 1,000 employees, and who are focused on providing cybersecurity products and services. The list of SMEs is not, and is not intended to be, comprehensive but to provide high-level insights into the current state of cybersecurity innovation in Ontario. Findings from the interviews and sensing exercise are quoted throughout the report and augmented by secondary research.

# Cybersecurity trends in the financial services industry

There are a number of trends driven by social, economic, and technological factors that are shaping cybersecurity innovation for the financial services industry.

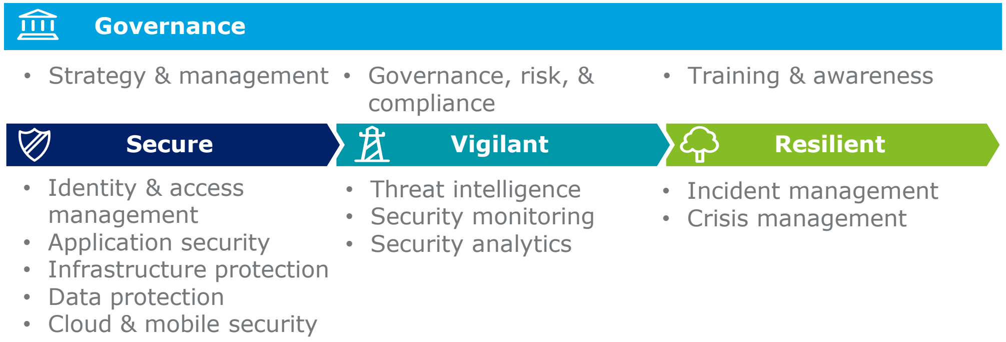
Cybersecurity is defined as *the capabilities and related technologies enabling the preservation of the confidentiality, integrity, and availability of information systems and the information that they process, store, and transmit.*

Within the financial services industry, cybersecurity is an increasingly important operational risk, critical to maintaining customer privacy, securing the transfer of value, and the trusted reputation on which the financial system relies.

The industry is facing increasingly sophisticated cyber threats from cyber criminals, insiders, hacktivists, terrorists, and nation states for financial gain, competitive advantage, or for political purposes. This cyber threat landscape is forcing financial services institutions to improve their core cybersecurity capabilities and secure emerging technologies against new types of cyberattacks.

Financial services institutions meet these threats by implementing capabilities to become more *secure*, *vigilant*, and *resilient.* These capabilities are coupled with appropriate governance to make sound investments, manage risk, compliance, and raise the awareness of employees, customers, and vendors. The following diagram outlines some of the key cybersecurity capabilities that financial services institutions implement to meet these threats. The cybersecurity capabilities also offer a way to segment the market for cybersecurity products and services.

**Cybersecurity capabilities**



**Governance**

- Strategy & management
- Governance, risk, & compliance
- Training & awareness

**Secure**

- Identity & access management
- Application security
- Infrastructure protection
- Data protection
- Cloud & mobile security

**Vigilant**

- Threat intelligence
- Security monitoring
- Security analytics

**Resilient**

- Incident management
- Crisis management

Not only are financial institutions under threat from cyber criminals, the industry faces growing competition from technology-enabled business models threatening to disintermediate incumbents from the customer and unbundle the services they provide. This phenomenon is broadly referred to as fintech, or financial technology innovation, and is strongly tied to cybersecurity innovation in two important ways.

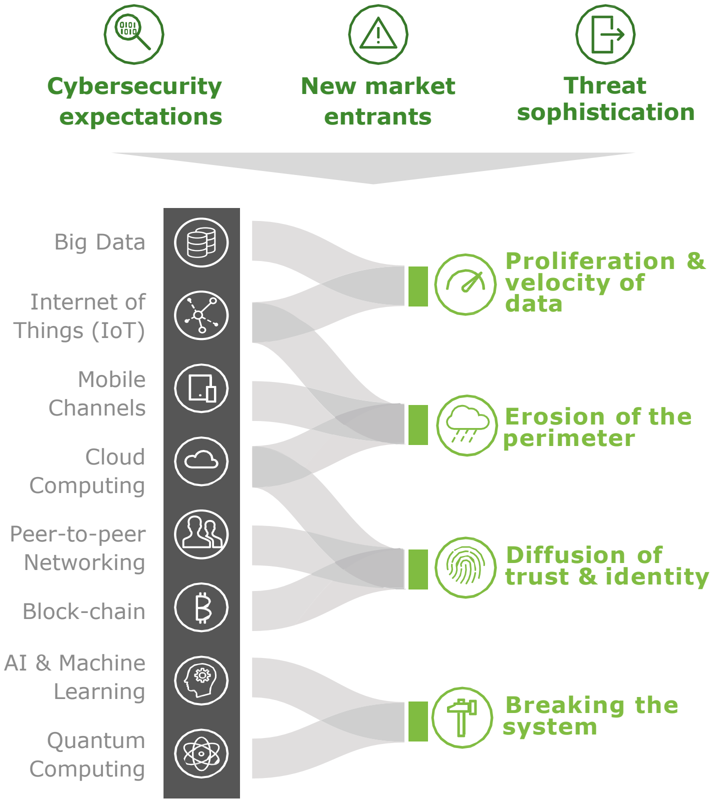
First, cybersecurity and fintech innovations often rely on common enabling technologies and skillsets. For example, block-chain aims to guarantee trust and the integrity of transactions using cryptographic protocols – a traditional cybersecurity domain. Second, as fintech innovations introduce new opportunities, they also introduce new cybersecurity risks. Given the high-trust requirements of the financial industry (e.g. storage of customer information, integrity of transactions, clearing, etc.), cybersecurity must be part of the core functionality of emerging fintech solutions. For these reasons, we posit that the futures of fintech and cybersecurity innovation are tightly linked and contribute to the backdrop of the social, economic, and technological trends shaping cybersecurity innovation in the financial industry.

**The futures of fintech and cybersecurity innovation are tightly linked and contribute to the backdrop of the social, economic, and technological trends shaping cybersecurity innovation in the financial industry.**

# Cybersecurity trends in the financial services industry

Layering over the social and economic backdrop of fintech innovation, increasing threat sophistication and rising stakeholder expectations, emerging technologies are shaping the cybersecurity needs of the financial services industry.

### Social & economic trends



Cybersecurity expectations

New market entrants

Threat sophistication

Big Data

Internet of Things (IoT)

Mobile Channels

Cloud Computing

Peer-to-peer Networking

Block-chain

AI & Machine Learning

Quantum Computing

Proliferation & velocity of data

Erosion of the perimeter

Diffusion of trust & identity

Breaking the system

### Technological trends

## Increasing cybersecurity expectations

### Summary

High-profile breaches are increasingly common place. This has translated into increased scrutiny by customers, boards, business partners, and regulators.

### Drivers

- Media coverage of large-scale cybersecurity breaches and the revelations of Edward Snowden on the scale of internet surveillance have increased customer concerns around privacy.
- Boards, regulators, and the audit function have responded to this challenge by elevating cybersecurity to a key operational risk and expecting more comprehensive reporting on cybersecurity preparedness and posture. Regulators, at the government's behest, continue to administer cyber-specific assessments and craft more specific requirements.

### Implications

- Canadian financial institutions are looked upon by customers as trusted entities to serve as custodians of their assets and private information. It is vital that financial institutions do everything they can to preserve that reputation with customers.
- Chief Information Security Officers require a firm grasp on the cybersecurity posture of their organization. This means greater time spent collecting and analyzing data and managing the expectations of the board, auditors, and regulators.

# Cybersecurity trends in the financial services industry

## Increasing cybersecurity threat sophistication

### Summary

Cyber threats are becoming increasingly sophisticated, provoking financial institutions to continually keep pace with new threats.

### Drivers

- Criminals are increasingly recognizing that cyber crime offers high rewards with lower risk of consequences compared to more traditional crime methods.
- Attack tools continue to proliferate and reach economies of scale through commercialization. The rise of cyber crime as a service has reduced the barriers to entry into conducting sophisticated cyber operations.[2]

### Implications

- This increasing sophistication requires financial institutions to invest in advanced detection methods to identify advanced persistent threats.
- Recognizing it’s a matter of “when” not “if” for cyberattacks, financial institutions are increasingly focusing on response and recovery capabilities.

## Increasing competition from outsiders

### Summary

Growing competition from new market entrants threatens to disintermediate incumbents from the customer and unbundle the services they provide.

### Drivers

- New technologies, combined with new or existing business models, are fostering increased industry competition.
- Existing enterprises such as telecommunication companies and new players are targeting traditional financial services (e.g. Apple Pay).

### Implications

- Increased competition is forcing incumbent innovation and the rapid adoption of new technologies.
- Despite the requirement for agility, adequate security must be built into new products in an effective and efficient manner.

## Erosion of the perimeter

### Summary

The traditional network perimeter, which offered a clear boundary for protection, is becoming blurred due to the rise of IoT, mobile, and cloud-based channels. This in turn is increasing the importance of protecting individual endpoints.

### Drivers

- Consumers are increasingly expecting financial products and services to be available 24/7 and from any device connected to the internet.
- Financial services institutions are increasingly integrating with vendors for the delivery of services and to streamline back-end operations.
- The advent of embedded sensors in devices increases both avenues for attack and the volumes of data collected by financial institutions.

### Implications

- With the assumption that attackers will breach the perimeter, protecting the endpoint becomes more critical. As attackers intend to keep a low profile, it is also essential to develop advanced threat intelligence and detection capabilities.

# Cybersecurity trends in the financial services industry

## Diffusion of trust & identity

### Summary

The proliferation of distributed platforms and channels is challenging financial services institutions' ability to manage digital identity and maintain trust within and between networks.

### Drivers

- The increasing number of ways in which customers and employees can access products and services.
- The role of block-chain and peer-to-peer networking in enabling anonymous transactions between individuals and businesses.

### Implications

- Diverse platforms and channels are forcing the financial services industry to invest in new ways to manage digital identity while ensuring convenience throughout the customer journey.
- New platforms and channels challenge the current and future role of incumbent financial services institutions as guarantors of trust across untrusted networks.

## Proliferation & velocity of data

### Summary

The increased volume, variety, and velocity of data collected by financial institutions and startups is enabling new insights and strategies and allowing for increased agility. These new capabilities require an agile security approach as well as close attention to maintaining customer privacy.

### Drivers

- The increasing accessibility of data through online channels and embedded sensors.
- Improvements in technology, deep learning, and processing power.

### Implications

- The increasing amount and variety of customer information stored by organizations increases the importance of ensuring that customer privacy is maintained.

## Breaking the system

### Summary

Emerging technologies such as artificial intelligence and quantum computing are poised to undermine traditional approaches to cybersecurity.

### Drivers

- Continued development of quantum computing technology.
- Increasingly powerful computers and sophisticated algorithms are making inroads into roles traditionally performed by human actors.

### Implications

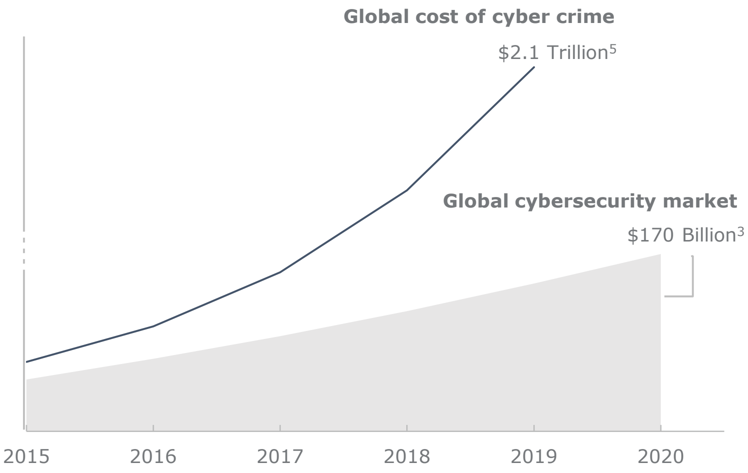
- Traditional cryptographic systems that protect financial transactions and personal information and underpin emerging technologies such as block-chain are not resistant to quantum computing power. As the technology develops, new cryptographic systems will need to be implemented to "quantum-proof" technology.
- Advancements in artificial intelligence may augment the cyberattacker arsenal while also potentially improving organizations' ability to detect and respond to cyber threats.

# The cybersecurity opportunity for Ontario

These social, economic, and technological trends are driving changes to the market and creating new opportunities for cybersecurity innovators in Ontario and around the world.

Current estimates place the size of the global cybersecurity market at $106 billion in 2015 and predict an average compound annual growth rate of approximately 10% through 2020.[3] At the same time, the global costs of cybercrime are estimated to be growing even faster.[5]

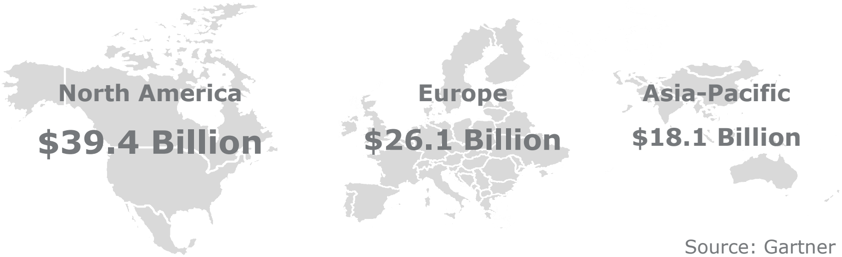
### Global cybersecurity economic outlook 2015-2020



Sources: Markets and Markets,[3] Juniper Research[5]

Disparate growth between the cost of cybercrime and cybersecurity spending and the difficulty of capturing true cybersecurity spend across organizations has led some analysts to project that the cybersecurity market will exceed $1 trillion by 2021, though this is much higher than consensus estimates.[6]

This growth in demand is not equally distributed across geographies, industries, or the types of cybersecurity products and services that are poised for growth. North America and Europe are the current (2016) and foreseeable top buyers with the Asia-Pacific region rapidly emerging as a key cybersecurity market.[4]

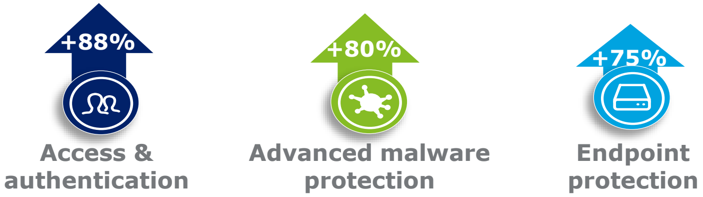


Source: Gartner 2016[4]

From a domestic perspective, some analysts posit that cybersecurity spending in Canada is set to exceed $2 Billion in 2016.[7]

From an industry perspective, financial services firms have been the prime target for cybercrime followed by the telecommunications, defence, and energy/resource industries.[8] Not surprisingly, financial services firms allocate one of the highest dollar amounts to cybersecurity as a percentage of overall IT spend, second only to national governments. This translates to the average financial institution spending approximately $980 per employee on cybersecurity in 2016.[9]

When looking at how the aforementioned trends are shaping the market dynamics, there are a number of cybersecurity technologies that are poised for the highest growth globally and across industries:



Source: SANS 2016[10]

These investment priorities are largely echoed by the responses to our survey of Canadian financial services industry cybersecurity leaders who cite *training and awareness*, *identity and access management*, and *cloud and mobile security* as the top domains for increased investment over the next 2-5 years.

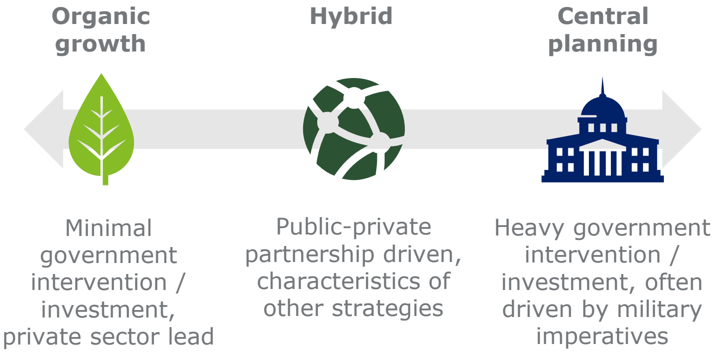
# The cybersecurity opportunity for Ontario

The importance of cybersecurity to a secure economy coupled with rapid market growth is driving innovation and has spurred governments to invest in supporting the growth of cybersecurity innovation ecosystems.

Generally, strong innovation/entrepreneurial ecosystems are linked with "rapid job creation, GDP growth, and long-term productivity increases".[11] When it comes to cybersecurity innovation, the positive externalities are also significant. A thriving cybersecurity innovation ecosystem provides a highly skilled talent pool, a cyber-aware population, and first-mover access to the latest cybersecurity products and services to secure government and private sector systems.

The primary purpose of this report is to understand how to position Ontario as a global hub for cybersecurity innovation. As such, there are established and emerging cybersecurity innovation hubs that serve as case studies and represent potential competitors in achieving the vision.

These case studies demonstrate a spectrum of strategic patterns to fostering cybersecurity innovation:



**Organic growth**

Minimal government intervention / investment, private sector lead

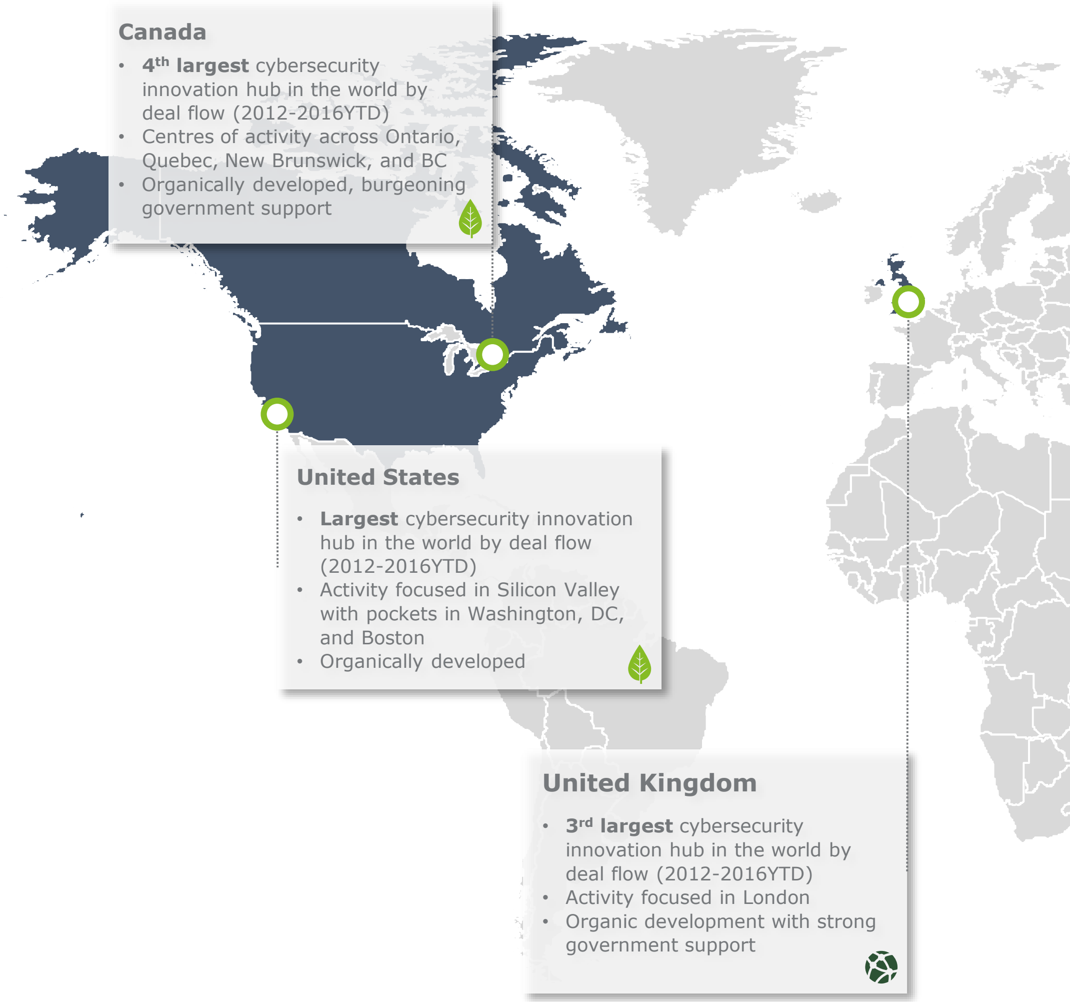
**Hybrid**

Public-private partnership driven, characteristics of other strategies

**Central planning**

Heavy government intervention / investment, often driven by military imperatives

## Cybersecurity innovation hubs



### Canada

- **4th largest** cybersecurity innovation hub in the world by deal flow (2012-2016YTD)
- Centres of activity across Ontario, Quebec, New Brunswick, and BC
- Organically developed, burgeoning government support

### United States

- **Largest** cybersecurity innovation hub in the world by deal flow (2012-2016YTD)
- Activity focused in Silicon Valley with pockets in Washington, DC, and Boston
- Organically developed

### United Kingdom

- **3rd largest** cybersecurity innovation hub in the world by deal flow (2012-2016YTD)
- Activity focused in London
- Organic development with strong government support

# The cybersecurity opportunity for Ontario

**Israel**

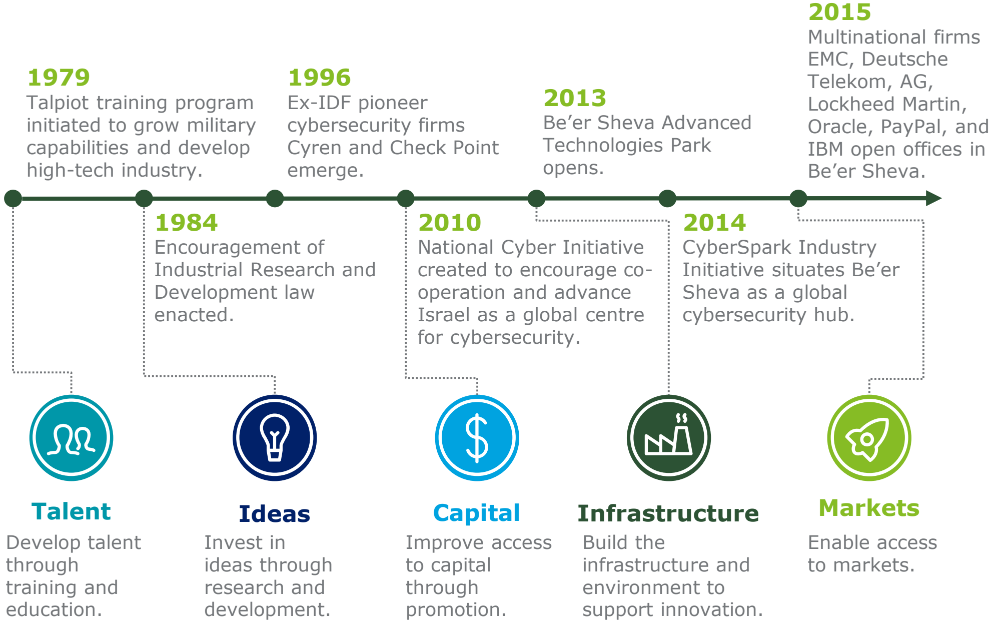
- **2nd largest** cybersecurity innovation hub in the world by deal flow (2012-2016YTD)
- Activity focused in Tel Aviv and Be'er Sheva
- Highly influenced by government policy

**Singapore**

- **Emerging** cybersecurity innovation hub
- Activity focused in Singapore City
- Strong government support

## Spotlight on Israel's cybersecurity innovation ecosystem

Israel represents the largest and most successful cybersecurity innovation hub outside the US. The following timeline illustrates key events in its development:



**1979** Talpiot training program initiated to grow military capabilities and develop high-tech industry.

**1984** Encouragement of Industrial Research and Development law enacted.

**1996** Ex-IDF pioneer cybersecurity firms Cyren and Check Point emerge.

**2010** National Cyber Initiative created to encourage co-operation and advance Israel as a global centre for cybersecurity.

**2013** Be'er Sheva Advanced Technologies Park opens.

**2014** CyberSpark Industry Initiative situates Be'er Sheva as a global cybersecurity hub.

**2015** Multinational firms EMC, Deutsche Telekom, AG, Lockheed Martin, Oracle, PayPal, and IBM open offices in Be'er Sheva.

**Talent** Develop talent through training and education.

**Ideas** Invest in ideas through research and development.

**Capital** Improve access to capital through promotion.

**Infrastructure** Build the infrastructure and environment to support innovation.

**Markets** Enable access to markets.

In reviewing the literature, and global cybersecurity innovation hubs, five key factors to a thriving ecosystem are apparent: the requisite *infrastructure*, *talent*, *ideas*, and access to *capital* and *markets*. Each of these factors can be thought of as the necessary conditions or ingredients for a healthy innovation ecosystem.

**There is strong competition in cybersecurity innovation. If Ontario is to become a global hub, it must act now and be competitive in terms of *infrastructure, talent*, *ideas*, and access to *capital* and *markets*.**

# Ontario's cybersecurity innovation ecosystem

We have structured our analysis using a cybersecurity innovation ecosystem model comprised of **five factors** and **nine players**.

An innovation ecosystem models the economic dynamics of relationships between players whose functional goal is to enable innovation.[12] This goal is supported by the five factors introduced in the previous section. We have identified nine players specific to cybersecurity ecosystems:

**Cybersecurity innovators**

- Startups, SMEs, and large enterprises developing new cybersecurity products and services

**Private sector**

- Large enterprises providing experienced talent, mentorship, and demand for new cybersecurity products and services

**Academia**

- Post-secondary institutions educating talent and conducting research and development into cybersecurity-related areas

**Investors**

- Individuals, institutions, private equity and venture capital firms proving capital to cybersecurity innovators

**Public sector**

- Military and government security/intelligence organizations providing experienced talent, mentorship, and demand

**Incubators / accelerators**

- Organizations providing space and commercialization support to cybersecurity innovators

**Government & support organizations**

- Government and not-for-profit organizations providing capital, support, and policy enablement for innovation

**Regulators**

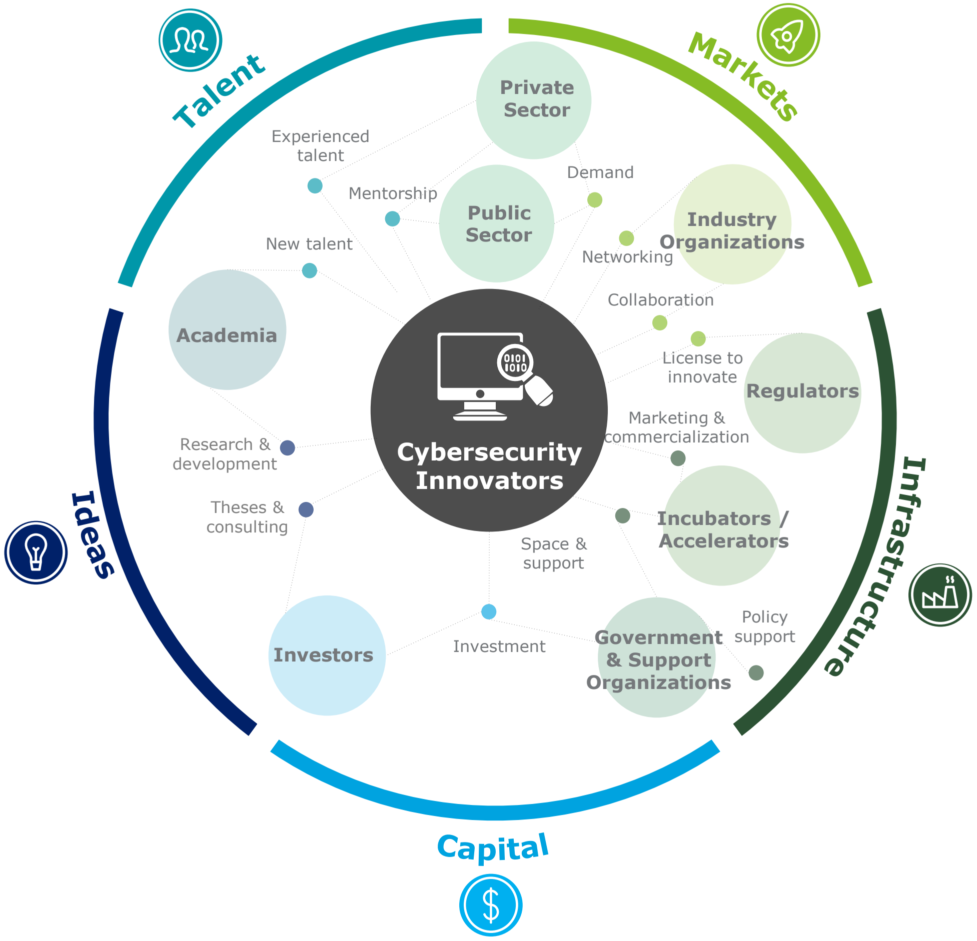
- Bodies that regulate industries

**Industry organizations**

- Organizations that represent industries and promote collaboration or advance a specific aim

The model provides a structure with which to understand the dynamics and performance of Ontario's cybersecurity innovation ecosystem and is used to organize our analysis.

**Cybersecurity innovation ecosystem model**

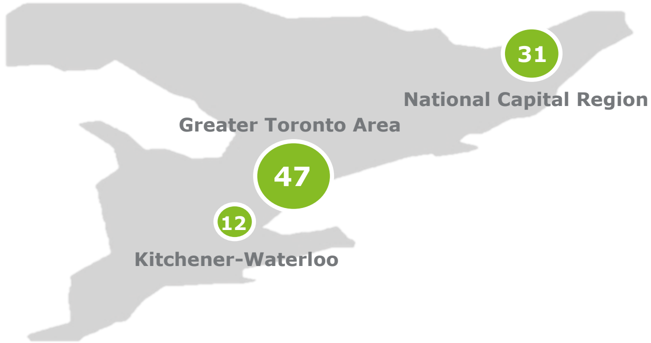


# Ontario's cybersecurity innovation ecosystem

**We found natural clusters of cybersecurity innovation in Ontario centred in the Greater Toronto Area, National Capital Region, and Kitchener-Waterloo.**

As part of our analysis we profiled 90 SMEs that focus on developing cybersecurity products and services in Ontario. Of these, we estimate that ~75% are currently active. Our list was compiled through open source and proprietary analysis and is not meant to be exhaustive, but to provide insights into the state of cybersecurity innovation in Ontario. One of the key findings from our analysis was the geographic distribution of the SMEs that indicated natural clustering.

## Natural clusters of cybersecurity innovation in Ontario

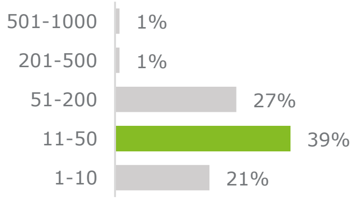


While the disparate clustering within these locales is largely a function of population, there are additional sources of gravity that are worth noting:

- Confluence of academia and major industry within the GTA
- Significant military, security intelligence, and technology hubs in the NCR
- Technology-focused academic institutions (e.g. Institute for Quantum Computing) and anchor organizations (e.g. BlackBerry) in Kitchener-Waterloo

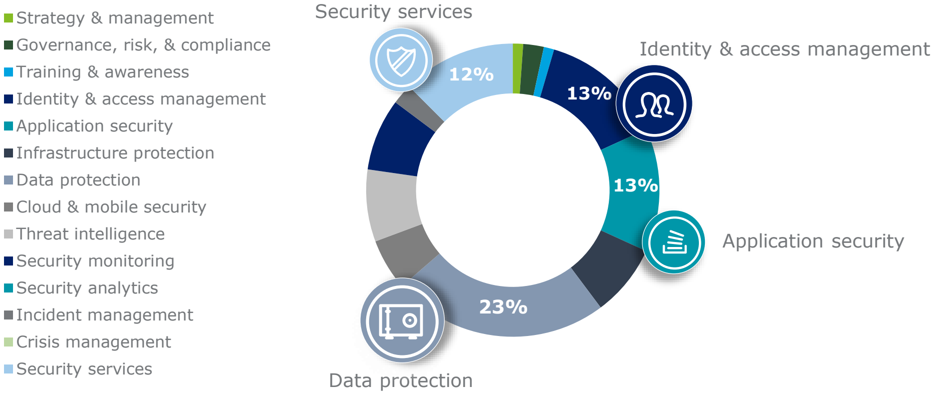
## Cybersecurity SMEs by number of employees

The majority of profiled Ontario cybersecurity SMEs have less than 50 employees. This suggests a large portion of early stage SMEs which can be considered startups and potentially poised for fast growth.



When looking at the types of cybersecurity products and services offered by these firms, there were a number of interesting conclusions. The majority of profiled Ontario cybersecurity SMEs are focused on providing data protection, identity and access management, and application security solutions. There is also a strong contingent of security consultancies providing a wide range of security services.

## Cybersecurity SMEs by domain



**Ontario cybersecurity SMEs show strengths in data protection, identity and access management, and application security products and services.**

# Ontario’s cybersecurity innovation ecosystem

## Talent

Ontario is home to a highly educated, international population and some of the worlds preeminent academic institutions. The clustering of academia and industry, particularly in the GTA and the Kitchener-Waterloo regions, also provides a significant experienced talent pool to draw on. Ontario employs over 250,000 people in IT, 30,000+ of which work in IT for financial services firms.[13]

Despite this confluence of talent, a main theme in our research and discussions with Ontario financial industry leaders is a cybersecurity talent shortage. The (ISC)$^2$ estimates there will be a global shortfall of cybersecurity talent in excess of 1.5 million resources by 2020.[14] Among other impacts, the talent shortage has driven up wages in established companies, providing an incentive against experienced cybersecurity practitioners starting new businesses.

### Cybersecurity education in Ontario

Ontario’s post-secondary institutions are world class in areas related to cybersecurity. The University of Toronto and the University of Waterloo both rank in the top 25 globally for computer science and information systems.[15] Moreover, at the college level, there are a number of well-regarded diploma programs that provide applied cybersecurity training such as Sheridan College’s Information System Security program.

**9** University-level cybersecurity degree programs

**30+** College-level cybersecurity diploma programs

Despite this strength, the talent shortage remains a fact for new businesses as well as incumbents. While there is a relatively low number of dedicated cybersecurity programs at the university and graduate level vis-à-vis colleges, there are over 175 cybersecurity-related course offerings at Ontario’s universities.[16] Nevertheless, we found weak integration of cybersecurity concepts within computer science and engineering curricula with the aforementioned courses largely positioned as upper-year electives.

The cybersecurity field is increasingly requiring new thinking to understand convergence with areas such as fraud, political, and country risk. There are very few cross-disciplinary programs that marry the technological aspects of cybersecurity with financial literacy, political, and economic studies.[17] This cross-disciplinary sentiment is echoed through our discussions with key ecosystem players who posit that the real shortage for Ontario is not in technical talent but in those with the skills to scale startups into successful businesses.

To this aim, there are a number of leaders working to foster cross-disciplinary educational opportunities. Key examples include both the Technology Innovation Management, and Infrastructure Protection and International Security programs at Carleton University, as well as the Smart Cybersecurity Network (SERENE-RISC) which has partnered with OCE in this area.

Globally, organizations in countries such as Israel are experimenting with introducing cybersecurity education as early as the 8th grade in order to meet the growing need for cyber specialists.[18]

# Ontario's cybersecurity innovation ecosystem

## Ideas

The Ontario research and development (R&D) apparatus represents a significant portion of all R&D expenditures in Canada. Ontario spent $14.1 billion on R&D in 2013, representing 44% of all R&D expenditure in Canada. This spend was largely driven by the business and higher education sectors at $7 and $5.3 billion, respectively.[19] Moreover, six of Canada's top 15 most impactful research universities are located in Ontario.[20]

Ontario boasts world-class R&D capabilities and thought leadership in a number of cybersecurity-related areas:

**Machine learning & artificial intelligence**
- Led by the University of Toronto's Department of Computer Science
- Thought leaders such as Prof. Geoffrey Hinton
- Spin-off companies: Deep Genomics and DNNresearch (acquired by Google)
- Sample cybersecurity application: threat detection and response

**Quantum computing**
- Led by the University of Waterloo's Institute for Quantum Computing
- Thought leaders such as Prof. Raymond Laflamme (Waterloo)
- Sample cybersecurity applications: quantum encryption, data protection

**Block-chain**
- Centred in Toronto around Decentral, Ethereum
- First Global Bitcoin Expo held in Toronto in 2014
- Sample cybersecurity applications: identity and access management

**Privacy**
- Led by Ryerson University's Privacy & Big Data Institute
- Thought leaders such as Dr. Ann Cavoukian
- Sample cybersecurity applications: identity and access management

These are areas where Ontario can compete globally in the cybersecurity space. As yet, there has been limited large-scale collaboration and application of these technologies and approaches to cybersecurity problems.

While it is early days yet, there are signs that this is changing: BlackBerry has announced a pivot to focus on cybersecurity products, and the University of Ottawa and University of Waterloo recently announced a partnership with IBM to train Watson in the language of cybersecurity.[21] [22] From a government perspective, Ontario Centres of Excellence, PROMPT, and the Natural Sciences and Engineering Research Council of Canada have initiated a Cybersecurity R&D Challenge to promote industry-academia collaboration on cybersecurity research.[23]

More broadly, this potential strength occurs against the backdrop of steadily decreasing business expenditure on research and development across advanced economies and within Canada.[23] In the recent launch of the Government of Canada's Innovation Agenda, it is recognized that there is a need to "improve in transforming ideas into marketable products, services and business models".[24] One of the six areas of action within Canada's Innovation Agenda includes positioning Canada to "compete in a digital world".[24] We posit that cybersecurity is an area where Ontario's unique strengths can make an impact on this journey.

# Ontario's cybersecurity innovation ecosystem

## Capital

CB Insights highlights Canada as the fourth most active country in the world for cybersecurity deals. When controlled for GDP, Canadian cybersecurity SMEs have attracted a higher ratio of global cybersecurity investment relative to other economies.

### Top countries for cybersecurity deals 2012-2016 YTD

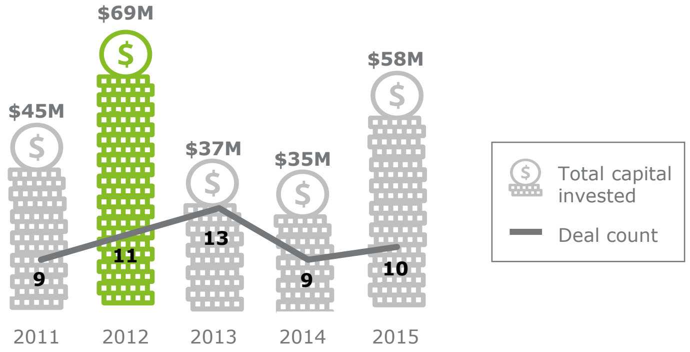
| Rank | Country | Percentage of Deals | GDP Trillion $ |
|---|---|---|---|
| 1 | United States | 75% | 18.0 |
| 2 | Israel | 8% | 0.28 |
| 3 | United Kingdom | 4% | 2.66 |
| 4 | Canada | 2% | 1.63 |
| 5 | China | 1% | 19.5 |
| 6 | Other | 10% | N/A |

Sources: CB Insights & Deloitte analysis[25]

Ontario represents a significant portion of Canada's cybersecurity deal flow with over 52 deals and approximately $244 million in capital invested between 2011 and 2015. The first two quarters of 2016 indicate another strong year with five announced deals worth $38 million.[26]

Deal activity, however, has not grown at the pace of other cybersecurity hubs around the world. Cybersecurity venture capital funding in the UK surpassed Ontario for the first time in 2015, both in terms of total capital invested and deal count. As indicated in the chart opposite, there is a potential plateau of capital flowing into Ontario as other hubs gain momentum.

### Ontario cybersecurity venture capital funding & deal count



Sources: PitchBook & Deloitte analysis[26]

Two other key findings include a lack of institutional investment in Ontario cybersecurity SMEs and a scarcity of late-stage funding forcing Ontario cybersecurity SMEs to look to other regions such as the US.

We found that investment in Ontario cybersecurity SMEs is primarily driven by pure play venture capital firms – where institutional investors are involved, they are typically the venture wings of the large technology, media, and telecommunications firms.

While the level of early-stage capital investment in Ontario cybersecurity SMEs has been steady over the past five years, access to late-stage capital is a perennial problem for Canadian businesses. Ontario cybersecurity SMEs are often driven to the East Coast of the US "by its concentration on security technology for the financial services industry," and the resources to scale a later-stage business.[27]

### Exit trends

While IPOs for cybersecurity businesses in Ontario are rare, we reviewed 15 cybersecurity M&A transactions since 2014.[28] International firms were the buyers in 11 of these transactions and in all but one case the acquired companies retained a significant presence in Ontario post-acquisition. A number of acquirers cited strong talent, innovation, and a strategy to bolster their Canadian and North American market presence through the acquisition.

# Ontario’s cybersecurity innovation ecosystem

## Infrastructure

Ontario’s innovation infrastructure is comprised of incubators, accelerators, industry, and support organizations underpinned by a business, regulatory, and policy environment.

Ontario is home to a network of world-class incubators and accelerators providing space, resources, and commercialization support to Ontario innovators, for example: Communitech in Kitchener-Waterloo, MaRS in Toronto, Invest Ottawa, and VENUS Cybersecurity Corporation in Ottawa.[29] The Ontario Network of Entrepreneurs also works to connect innovators with resources to build and scale business.

Our discussions with these players indicate a number of planned initiatives positioning cybersecurity as an area of focus. However, we did not find widespread and meaningful coordination between actors on promoting cybersecurity innovation. These efforts have created emerging pockets of strong support for cybersecurity innovators, yet there is no primary centre of gravity.

Leading hubs such as Israel, and the United Kingdom have begun moving to create such centres of gravity to bring together relevant ecosystem players and serve as a focal point for cybersecurity innovation. The CyberSpark innovation arena in Be’er Sheva, Israel, was created in 2014 and the Cyber London (CyLon) accelerator was opened in London in 2015.[30] [31]

There is evidence to suggest that this fragmented condition in Ontario is changing. Organizations such as OCE and the TFSA are working to bring together industry, academia, and innovators to solve common problems. Moreover, the rise of cybersecurity Information Sharing and Analysis Centres (ISACs) such as the US-based FSI-ISAC and the Canadian Cyber Threat Exchange indicate that competitive industries such as financial services are willing to collaborate to solve common cybersecurity problems.

Looking to the broader business, regulatory, and policy environment, our analysis similarly identified key strengths and areas to improve. Canada and Ontario have some of the most generous R&D incentives and lowest costs of doing business for digital services, software design, and telecommunications in the G7.[32] Coupled with a low Canadian dollar, these attributes position Ontario as an attractive geography in which to start a cybersecurity business.

At the provincial level, policy support for cybersecurity innovation is growing through Ontario's Innovation Agenda. In 2015, the Premier led a business delegation to Israel that included delegates focused on developing cybersecurity innovation partnerships. Despite this growing support, cybersecurity is not formally identified as an area of focus.[33]

Federally, the Government of Canada’s 2010 Cyber Security Strategy articulates a three-pillared strategy to meet the cyber threat: securing government systems, securing critical private sector systems, and helping Canadian’s be secure online. While a commitment to “provide funding to the innovation system, including academic institutions, to develop new technological solutions for cyber security” is included, the innovation agenda is not a foundational tenet within the strategy.[34] This is in contrast to the Governments of the UK and Singapore whose strategies position cybersecurity innovation as core components of their strategy.[35] [36]

### Regulatory environment

Given the confluence of cybersecurity and the disruptive trends affecting the financial services industry, the regulatory environment is a critical component of Ontario’s cybersecurity innovation ecosystem. While regulators, such as the Office of the Superintendent of Financial Institutions (OSFI), continue to increase scrutiny on cybersecurity within financial services firms, the impacts and expectations of new business models on cybersecurity remain unclear and may hinder innovation in both fintech and cybersecurity. Our discussions with cybersecurity leaders in Ontario’s financial services industry reinforced this point. Regulators around the world have recognized this potential tension and are taking proactive approaches to address it. For example, regulators in the UK and Singapore are working to implement regulatory sandboxes to foster innovation by allowing disruptors and incumbents to test new ideas and technologies “without immediately incurring all the normal regulatory consequences” in a controlled environment.[37]

# Ontario's cybersecurity innovation ecosystem

## Markets

Ontario is regarded as one of the primary economic centres in Canada with clusters of established businesses in the consumer business; technology, media, and telecommunications; government; and financial services industries, representing a significant domestic market for cybersecurity products and services.

### Potentially significant domestic cybersecurity buyers

Financial services
Government
Technology, media, & telecommunications
Consumer business

From an international perspective, there are also a number of factors increasing potential market access for Ontario cybersecurity innovators. Ontario is highly integrated with the global economy and serves as a key hub for cross-border commerce with the US, which is augmented through the North American Free Trade Agreement.

Within the broader context, Canada's positive global reputation as a trusted partner provides the potential for an advantaged springboard to global markets for Ontario cybersecurity innovators. Formal partnerships – including the UK-USA Agreement for Signals Intelligence Cooperation, North Atlantic Treaty Organization, and the alignment of national security interests with other major cybersecurity markets, such as Europe – reinforce this potential. In contrast to other cybersecurity innovation hubs, buying Ontario cybersecurity products and services may be perceived as posing less of a risk of espionage. The global reputation for security that BlackBerry holds is a key example.

Despite being well positioned in terms of potential access to domestic and international markets, we found that a lack of visibility, a culture of "buying Canadian," and a relatively risk-averse domestic client base has historically blocked this potential for cybersecurity innovators in Ontario.

### Spotlight on the financial services industry in Ontario

The financial services industry cluster in Ontario represents a large market opportunity for cybersecurity innovators. The World Economic Forum has rated Canada's banks as the soundest in the world for the past eight years.[38] Canadian banks and regulators are strongly incented to maintain this reputation potentially contributing to a risk-averse approach to innovation.

While financial services firms in Ontario are increasingly interacting with innovation ecosystem players, interactions to date have not been focused on cybersecurity innovation. As part of our interviews with key financial services cybersecurity leaders, we found two pertinent facts that illustrate potential sources of friction within the ecosystem:

- Only 27% of interviewees had interacted with cybersecurity startups in the past 12 months, and only one of these startups was headquartered in Ontario. This suggests a lack of visibility of key market players into the offerings of Ontario cybersecurity innovators.
- The top barriers to adopting innovative Ontario cybersecurity solutions included "not wanting to be the first to adopt" and "vendor scale and solvency". This suggests a potential free-rider dynamic within the ecosystem founded in risk aversion and wanting to see products tested in other markets first.

In addition, we found appetite and incentive for financial services industry players to collaborate on cybersecurity as a shared priority. Our interviews indicated that increased interaction with startups and academia are top of mind for financial services cybersecurity leaders. While strong cybersecurity may be a competitive advantage in the short term, weak cybersecurity may erode trust within the financial services industry as a whole over a longer time horizon, providing a shared interest in collaboration.

**Despite being well positioned in terms of potential access to domestic and international markets, we found that a lack of visibility and a relatively risk-averse domestic client base has historically hindered Ontario cybersecurity innovators.**

# Strategic recommendations

We identified areas of strength and friction through the ecosystem analysis and distilled them into **seven key findings** on which to base recommendations.

## Key findings

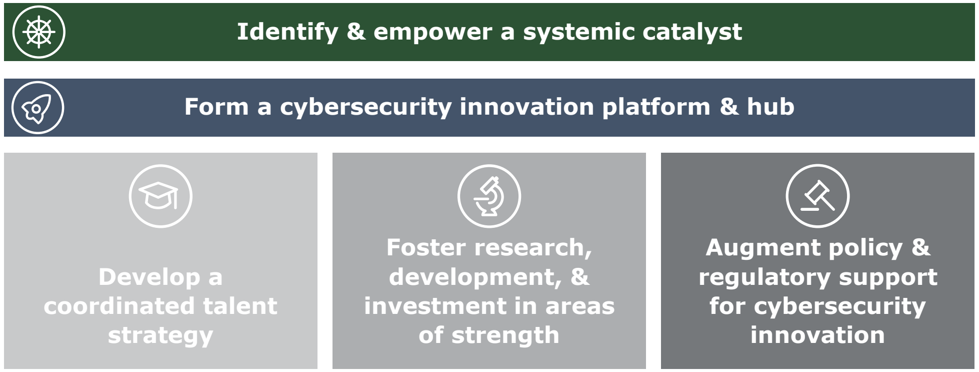
There are a number of dynamics that are affecting growth in positive and negative ways.

1. The future of innovation in the financial services industry is intimately linked to cybersecurity creating opportunities for shared growth.
2. While Ontario has organically developed significant clusters of cybersecurity innovation, there is no single centre of gravity, coordination, or systemic catalyst to bring it all together.
3. There is a cybersecurity talent shortage globally and in Ontario.
4. There is limited collaboration on applying Ontario's R&D strengths in related fields to cybersecurity problems.
5. Ontario is well positioned to access some of the largest domestic and international cybersecurity markets and sources of capital. A lack of visibility, a limited culture of 'buying Canadian,' and a relatively risk-averse domestic market has historically hindered this potential advantage for cybersecurity innovators in Ontario.
6. Cybersecurity is an area of strategic collaboration for financial services and other industries.
7. A historically sound regulatory environment has potentially led to a risk-averse approach to innovation within the financial services industry.

These key findings suggest a hybrid strategy for growth with significant roles for the private, not-for-profit, and public sectors.

Given increasing global competition, Ontario cannot rely on continued organic growth and thus focused and immediate intervention is required. A strong financial services industry with incentive to collaborate as well as robust academic and R&D institutions highlight the potential efficacy of public, private, and not-for-profit sector involvement.

## Strategic recommendations



**Identify & empower a systemic catalyst**

**Form a cybersecurity innovation platform & hub**

**Develop a coordinated talent strategy**

**Foster research, development, & investment in areas of strength**

**Augment policy & regulatory support for cybersecurity innovation**

### Identify & empower a systemic catalyst

Ontario has all the ingredients to become a global hub for cybersecurity innovation but has not yet reached the scale and gravity necessary to compete globally. Given the pace of global competition and the concerted efforts of governments around the world to foster cybersecurity innovation, it is unlikely that purely organic growth will suffice in positioning Ontario as a global cybersecurity innovation hub. Moreover, there is appetite and incentive for the private, not-for-profit, and public sectors to collaborate to accelerate growth in the ecosystem. To initiate this trajectory, a systemic catalyst is required.

We recommend identifying and empowering a systemic catalyst tasked with bringing together the right players, articulating the benefits of collaboration, facilitating strategy development, and tracking progress against strategic objectives.

A potential example of such a catalyst is Innovate Finance in the UK. The organization was created as "a fully independent membership organisation that supports innovators in FinTech and serves as a bridge between…members, regulators and policymakers".[39]

# Strategic recommendations

### Form a cybersecurity innovation platform & hub

Two key findings from the analysis focused on the lack of coordination and visibility into the products and services offered by Ontario's cybersecurity SMEs. We hypothesize that these findings are linked and can be addressed together.

We recommend the formation of a cybersecurity innovation platform to increase the visibility of cybersecurity innovation in Ontario. An associated hub to provide the space and infrastructure for collaboration and innovation activities should be investigated. The functions of a cybersecurity innovation platform are to:

- Connect Ontario cybersecurity SMEs with markets and capital
- Attract talent and innovators to start cybersecurity businesses in Ontario based on strong access to markets and a favourable business environment
- Develop international partnerships
- Provide a central source for information and consistent messaging on cybersecurity innovation in Ontario

The cybersecurity innovation hub need not be a new facility, but is necessary to provide a focal point for cybersecurity innovation activities in Ontario and link the Greater Toronto Area and other natural clusters of innovation in the National Capital Region and Kitchener-Waterloo. The drivers for investigating a cybersecurity innovation hub are to:

- Provide a physical centre of gravity for cybersecurity innovation in Ontario to host events and other programming
- Provide a venue for collaboration with the private sector to foster incumbent innovation, share ideas and space for joint proofs of concepts, cost, and risk sharing
- Provide joint infrastructure and lab space for Ontario cybersecurity innovators

### Develop a coordinated talent strategy

While Ontario boasts a highly educated population and world-class academic institutions, there is a shortage of cybersecurity talent. In collaboration with the province, private sector, and academia, we recommend that a coordinated talent strategy be developed to address this shortage. This strategy should focus on short- and long-term talent imperatives:

In the short term, there is an immediate need to address the talent issue for the private sector. Based on their programmatic agility, the private sector should engage with Ontario colleges to develop programming and augment formal recruitment channels. In parallel, government actors should investigate targeting migrants with cybersecurity skills through the Express Entry program. As precedent, "cyber security specialist" has been listed on the UK's official Shortage Occupation list since 2015.[40]

In the longer term, the strategy could focus on:

- Bolstering cybersecurity programming at the university and graduate levels
- Cross-disciplinary training between STEM and social science fields
- Increasing experiential learning opportunities
- Experimenting with basic cybersecurity awareness content in elementary and secondary education curricula

### Foster research, development, & investment in areas of strength

Ontario has a significant research and development apparatus as well as globally leading expertise in cybersecurity-related fields. We recommend working with academia, the private sector, and thought leaders to develop a research, development, and investment agenda based on Ontario's strengths. This agenda could focus on:

- Applying Ontario's advanced research capabilities in machine learning, artificial intelligence, and quantum computing to cybersecurity problems
- Looking for opportunities for cross pollination between fintech and cybersecurity research and development such as advanced cryptographic protocols
- Continuing to support research into the legal, political, economic, and social implications of cybersecurity

# Strategic recommendations

### Augment policy & regulatory support for cybersecurity innovation

The policy and regulatory environment is a critical facilitator of cybersecurity innovation. From a policy perspective, there are strong incentives for elevating the cybersecurity innovation agenda at the national, provincial, and municipal levels. Outside of the general benefits of an innovative economy, a thriving cybersecurity innovation ecosystem fosters a highly skilled talent pool, a cyber-aware population, and first-mover access to the latest cybersecurity products and services to secure government and private sector systems.

Canada's Cyber Security Strategy is due for renewal in 2016 and Public Safety Canada has recently issued a public consultation notice on the governments approach to cybersecurity. Given the benefits and innovation focus of the current federal government, we recommend that it elevate the cybersecurity innovation agenda as a formal strategic pillar. There is preliminary evidence that this is the case: "Cyber Innovation" is listed as one of three key action areas within the call for consultation.[41] Moreover, we recommend furthering cybersecurity innovation as part of Canada's recently inaugurated Innovation Agenda. At the provincial level, we recommend that cybersecurity continue to be invested in as an area of focus within the digital media and information and communications technology pillar of Ontario's Innovation Agenda.

Specific initiatives in which government can play a unique role include incentivizing "buying Canadian" within the public and private sectors, developing an objective pre-certification service to build trust in Ontario cybersecurity SMEs, and implementing streamlined procurement vehicles to reduce the time and effort required to enter the market which can sink a business trying to scale.

Of equal importance is the regulatory environment. Given the confluence of cybersecurity and the disruptive trends affecting the financial services industry, we recommend that regulators, innovators, and financial services industry players collaborate to better understand the impacts and to clarify expectations. The form which this collaboration takes, whether it be the development of guidelines or a regulatory sandbox, have not been the focus of this study and should be further investigated**.**

### Conclusion

Ontario has all the ingredients to become a global hub for cybersecurity innovation but has not yet reached the scale and gravity necessary to compete at the highest levels. Despite these ingredients and historically strong performance, Ontario risks losing its competitive position through failing to match the concerted efforts of governments and industries around the world that are ramping up investment and coordination in fostering cybersecurity innovation.

Our analysis identified a number of areas of strength and friction within Ontario's cybersecurity innovation ecosystem on which to build and solve. Foremost, the futures of the financial services industry and cybersecurity innovation are inherently linked. Given the strategic importance of the industry to Ontario's economy, fostering a global cybersecurity innovation hub is a shared public-private imperative. Faced with increasing global competition, Ontario cannot rely on continued organic growth. Focused and immediate intervention by public, private actors to *develop cybersecurity talent*, *encourage access to markets*, and *build on Ontario's strengths* to develop next generation cybersecurity products and services is required.

A partnership with the private, not-for-profit, and public sectors to address the findings outlined in this report is required to harness the cybersecurity opportunity and position Ontario as a global cybersecurity innovation hub. Moreover, this analysis has highlighted a number of important areas for further study.

**Ontario must harness the cyber opportunity for growth - the long term security and prosperity of the financial services industry and Ontario's economy may depend on it.**

# Appendices

# Endnotes

1. *The Global Risks Report 2016*. (2016). Available at: http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf. World Economic Forum.

2. Samani, R. (2013). *Cybercrime Exposed: Cybercrime-as-a-Service.* McAfee.

3. *Cyber Security Market by Solution - Global Forecast to 2020.* (June 2015). Available at: http://www.marketsandmarkets.com/PressReleases/cyber-security.asp. Markets and Markets. Charts/graphics created by Deloitte based on Markets and Markets research.

4. Gartner, Inc., Forecast: Information Security, Worldwide, 2014-2020, 2Q16 Update. Contu, R., Canales, C., Deshpande, S., Pingree, L., 2016. Graphic on page 10 combines Gartner's forecasts for "Western Europe" with "Eastern Europe," and "Mature Asia/Pacific" with "Emerging Asia/Pacific" into overall Europe and Asia-Pacific categories. Calculations were performed by Deloitte.

5. *The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation.* (2015). Available at: http://www.juniperresearch.com/researchstore/strategy-competition/cybercrime-security/financial-corporate-threats-mitigation. Juniper Research. Charts/graphics created by Deloitte based on Juniper research.

6. Morgan, S. (2016). *Cybersecurity Market Report: Q2 2016*. Available at: http://cybersecurityventures.com/cybersecurity-market-report/. Cybersecurity Ventures.

7. Hardy, I. (2016). *Rogers Partners with Trustwave, Announces New Suite of Cybersecurity Solutions*. Available at: http://betakit.com/rogers-partners-with-trustwave-announces-new-suite-of-cybersecurity-solutions/. BetaKit.

8. Morgan, S. (December 2015). *J.P. Morgan, Bank of America, Citibank and Wells Fargo Spending $1.5 Billion to Battle Cyber Crime.* Available at: http://www.forbes.com/sites/stevemorgan/2015/12/13/j-p-morgan-boa-citi-and-wells-spending-1-5-billion-to-battle-cyber-crime/#7f6dd91c1112. Forbes.

9. Gartner, Inc., IT Key Metrics Data 2016: Key IT Security Measures: by Industry. Hall, L., Stegman, E., Futela, S., Gupta, D. (2015).

10. IT Security Spending Trends. (February 2016). SANS Institute. Charts/graphics created by Deloitte based on SANS research.

11. Isenberg, D. (June 2010). *The Big Idea: How to Start an Entrepreneurial Revolution.* Harvard Business Review.

12. Jackson, D. (March 2015). *What is an Innovation Ecosystem?* Available at: http://erc-assoc.org/sites/default/files/topics/policy_studies/DJackson_Innovation%20Ecosystem_03-15-11.pdf. National Science Foundation.

13. *Financial Technology.* (2016). Available at: http://www.investinontario.com/financial-technology#IT-spending. Invest in Ontario.

14. Dickson, F., Suby, M. (April 2015). *The 2015 (ISC)2 Global Information Security Workforce Study.* Available at: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf. Frost & Sullivan.

15. *QS World University Rankings by Subject 2015 - Computer Science & Information Systems*. (2015). Available at: http://www.topuniversities.com/university-rankings/university-subject-rankings/2015/computer-science-information-systems#sorting=rank+region=+country=+faculty=+stars=false+search=. QS Top Universities.

16. *Canadian Cybersecurity Course Directory.* (2015). Available at: http://www.serene-risc.ca/fichiers/downloads/1/Course-Directory.pdf?files/prod /downloads/1/Course-Directory.pdf. SERENE-RISC.

17. Bailetti, T., et al. (August 2013). *Developing an Innovation Engine to Make Canada a Global Leader in Cybersecurity.* Available at: http://timreview.ca/sites/default/files/article_PDF/Bailetti_et_al_TIMReview_August2013.pdf. Technology Information Management Review.

18. Magshimim Program. (2016). Available at: http://www.rashi.org.il/magshimim-cyber-program. Rashi Foundation.

19. *Spending on Research and Development, 2015 (intentions)*. (September 2015). Available at: http://www.statcan.gc.ca/daily-quotidien/150923/dq150923b-eng.htm. Statistics Canada.

20. *Submission to the Expert Review Panel on Research and Development.* (February 2011). Available at: http://u15.ca/our-members. U15: Group of Canadian Research Universities.

21. *BlackBerry Launches New Professional Cybersecurity Services Practice to Expand Portfolio.* (February 2016). Available at: http://press.blackberry.com/en/press/2016/blackberry-launches-new-professional-cybersecurity-services-practice-to-expand-portfolio.html. BlackBerry.

22. Lalan, C. (May 2016). *IBM Watson to Tackle Cybercrime*. Available at: https://www-03.ibm.com/press/us/en/pressrelease/49683.wss. IBM.

23. *Cybersecurity R&D Challenge.* (2016). Available at: http://www.oce-ontario.org/programs/industry-academic-collaboration/collaboration-voucher-program/VIA/cybersecurity-r-d-challenge. Ontario Centres of Excellence.

# Endnotes

24. *Positioning Canada to Lead: An Inclusive Innovation Agenda*. (June 2015). Available at: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00009.html. Government of Canada.

25. *Deals To Cybersecurity Startups Are Increasingly Global With Israel In The Lead.* (August 2016). Available at: https://www.cbinsights.com/blog/cybersecurity-funding-geographic-trends/. CB Insights. Charts/graphics created by Deloitte based on CB Insights research.

26. *Ontario Cybersecurity Venture Capital Investments.* (June 2016). PitchBook Data, Inc.

27. Greenberg, A. (June 2015). *Report: Security Incidents in Finance Sector 300 Percent More Frequent than Other Industries.* Available at: http://www.scmagazine.com/financial-services-firms-see-three-times-more-security-incidents-than-other-sectors/article/422655/. SC Magazine.

28. *Ontario Cybersecurity Mergers & Acquisitions and IPOs*. (June 2016). PitchBook Data, Inc.

29. *From Concept to Commercialization: A Startup Eco-system Strategy for the City of Toronto*. (2015). Available at: http://www.toronto.ca/legdocs/mmis/2015/ed/bgrd/backgroundfile-78748.pdf. City of Toronto.

30. *CyberSpark – the Israeli Cyber Innovation Arena*. (2014). Available at: http://in.bgu.ac.il/en/cyber/Pages/Innovation-Arena.aspx. Ben-Gurion University of the Negev.

31. *Cyber London is Europe's First Cyber Security Accelerator and Incubator* Space. (2016). Available at: https://cylonlab.com/. CyLon.

32. *Competitive Alternatives: KPMG's Guide to International Business Location Costs*. (2014). Available at: https://www.competitivealternatives.com/reports/2014_compalt_report_vol1_en.pdf. KPMG.

33. Office of the Premier. (May 2016). *Business Mission Promotes Ontario's Tech and Financial Sectors*. Available at: https://news.ontario.ca/opo/en/2016/05/business-mission-promotes-ontarios-tech-and-financial-sectors.html. Ontario Government.

34. Public Safety Canada. (2015). *Action Plan 2010-2015 for Canada's Cyber Security Strategy*. Available at: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-en.aspx. Government of Canada.

35. *The UK Cyber Security Strategy 2011-2016: Annual Report.* (April 2016). Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf. UK Cabinet Office.

36. *National Cyber Security Masterplan 2018.* (2014). Available at: https://www.ida.gov.sg/~/media/Files/Programmes%20and%20Partnership/Initiatives/2014/ncsm2018/NationalCyberSecurityMasterplan%202018.pdf. Infocomm Development Authority of Singapore.

37. *Regulatory Sandbox*. (November 2015). Available at: https://www.fca.org.uk/your-fca/documents/regulatory-sandbox. Financial Conduct Authority.

38. Schwab, K. (2016). *The Global Competitiveness Report 2015–2016*. Available at: http://www3.weforum.org/docs/gcr/2015-2016/Global_Competitiveness_Report_2015-2016.pdf. World Economic Forum.

39. *What is Innovate Finance?* (2016). Available at: http://innovatefinance.com/ membership. Innovate Finance.

40. *Tier 2 Shortage Occupation List.* (November 2015). Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/486107/Shortage_Occupation_List_-_November_2015.pdf. UK Government.

41. Public Safety Canada. (2016). *Security and Prosperity in the Digital Age: Consulting on Canada's Approach to Cyber Security*. Available at: http://www.publicsafety.gc.ca/cnt/cnslttns/cbr-scrt/cbr-scrt-en.pdf. Government of Canada.

# About the authors

**Jeremy Hurst**
Senior Manager – Cyber Risk Services
jhurst@deloitte.ca

Jeremy is a seasoned risk and technology professional with over 15 years of international experience ranging from technology startups to global financial institutions. He holds a Bachelor of Mathematics from the University of Waterloo, a Bachelor of Arts from the University of Toronto, and an MBA from the Rotman School of Management where he graduated as a Bregman Scholar. He also maintains CISSP and CPA designations.

**Victor Platt**
Senior Consultant – Cyber Risk Services
vplatt@deloitte.ca

Victor focuses on helping large financial services and retail organizations develop cybersecurity strategies which support business objectives and enable innovation. An active researcher, Victor's analysis of Canada's cybersecurity strategy was published in *International Journal* and cited by Parliament. Victor holds a Bachelor of Arts from the University of Toronto and a Master of Infrastructure Protection and International Security from the Norman Paterson School of International Affairs.

## Advisers

**Steve Rampado**
Partner – Cyber Risk Services
srampado@deloitte.ca

Steve Rampado has over 20 years of experience in cybersecurity, technology risk, and regulatory management within the financial services industry. Steve previously lead Deloitte's Enterprise Risk Services in Toronto, holds an MBA and P.Eng designation.

**Terry Stuart**
Chief Innovation Officer – Deloitte Canada
testuart@deloitte.ca

Terry's job is to be a "constructive disruptor", helping both the firm and clients thrive in a world where exponential change is in the driver's seat and is not obeying the speed limit. Terry leads Deloitte's ecosystem strategy in Canada. He drives our D{ } initiative at Communitech and Deloitte's participation at OneEleven, MaRS, and the Ryerson DMZ.

## Acknowledgements

This report was prepared by Deloitte LLP with funding and support from Ontario Centres of Excellence and the Toronto Financial Services Alliance. The authors would like to acknowledge the invaluable contributions of Blaine Woodcock, Dina Kamal, Duncan Stewart, Fraser Gibson, Marc MacKinnon, Nick Galletto (alphabetical) as well as the OCE and TFSA teams. We would also like to thank the interviewees who took the time speak to us and share their insights, as well as Andrew McFarlane and Mary Chestak for their research support.

# Ontario cybersecurity SMEs

**10SCAPE** (Toronto) - Founded in 2013

**AFORE Solutions (CloudLink)** (Ottawa) - Founded in 2003
Acquired by EMC in 2015

**Airpost** (Toronto) - Founded in 2012
Acquired by Box in 2015

**Applied Recognition** (Burlington) - Founded in 2005

**Aprivacy (I Think Security)** (Waterloo) - Founded in 2010

**AssetMetrix** (Ottawa) - Founded in 2000
Acquired by Microsoft in 2006

**Barricode** (Richmond Hill) - Founded in 2006
Acquired by Polar Wireless Corp. in 2006

**Bioscrypt** (Markham) - Founded in 1987
Acquired by L-1 Identity Solutions in 2008

**Blacksumac** (Ottawa) - Founded in 2012
Acquired by iControl Networks in 2014

**BorderWare Technologies** (Mississauga) - Founded in 1994
Acquired by WatchGuard Technologies in 2009

**BrandProtect** (Toronto) - Founded in 2001

**Certicom** (Mississauga) - Founded in 1985
Acquired by RIM in 2009

**Chrysalis-ITS** (Ottawa) - Founded in 1994
Acquired by Rainbow Technologies in 2003

**CloudMask** (Ottawa) - Founded in 2012

**Cognitive Systems Corp.** (Waterloo) - Founded in 2014

**Crack Semiconductor** (Ottawa) - Founded in 2002

**Cryptomill Technology** (Toronto) - Founded in 2005

**Cycura** (Toronto) - Founded in 2013

**Defence Intelligence** (Ottawa) - Founded in 2008

**Devera Logic** (Ottawa) - Founded in 2007

**Digital Wyzdom** (Toronto) - Founded in 2005
Acquired by Telus in 2013

**DLS Technologies** (Ottawa) - Founded in 2000

**Echoworx** (Toronto) - Founded in 2000

**Elliptic Technologies** (Ottawa) - Founded in 2001
Acquired by Synopsis in 2015

**eSentire** (Cambridge) - Founded in 2001

**Firemex** (Toronto) - Founded in 2006

**Fixmo** (Toronto) - Founded in 2009
Acquired by Good Technology in 2014

**Graphite Software** (Ottawa) - Founded in 2012

**Guardly** (Toronto) - Founded in 2010

**Hackjacket Inc.** (Toronto) - Founded in 2014

**IAmI Authentications INC.** (Toronto) - Founded in 2015

**idAlerts** (Oakville) - Founded in 2005
Acquired by Collinson Group in 2015

**IDENTOS** (Toronto) - Founded in 2014

**InBay** (Ottawa) - Founded in 2009

**Industrial Cyber Sensing Inc.** (Kitchener) - Founded in 2013

**IntelliGO** (Toronto) - Founded in 2012

**Interset** (Ottawa) - Founded in 2002

**Invixium** (Markham) - Founded in 2012

**Iota Security** (Toronto) - Founded in 2013

**IPSS** (Ottawa) - Founded in 2002

**ISARA Corporation** (Waterloo) - Founded in 2015

**IT Weapons** (Brampton) - Founded in 2000
Acquired by Konica Minolta Business Solutions (Canada) Ltd. in 2015

**KoreConx** (Toronto) - Founded in 2013

**KTS Global** (Waterloo) - Founded in 2011

**KyberPass** (Ottawa) - Founded in 1995

**Layer7 Networks** (Pickering) - Founded in 2012

**Magnet Forensics** (Waterloo) - Founded in 2009

**MessageWare** (Mississauga) - Founded in 1993

**Nakina** (Richmond Hill) - Founded in 2001
Acquired by Nokia in 2016

**N-Dimension** (Richmond Hill) - Founded in 2001

**Nymi** (Toronto) - Founded in 2011

**OnPar Solutions** (Ottawa) - Founded in 2013

**OnTab** (Toronto) - Founded in 2012
Acquired by Ackroo in 2016

**Per Vices** (Toronto) - Founded in 2006

**Perspecsys** (Mississauga) - Founded in 1996
Acquired by Blue Coat Systems in 2015

**Phirelight** (Ottawa) - Founded in 2001

**Plainmark** (Richmond Hill) - Founded in 2012

**Privacy Analytics** (Ottawa) - Founded in 2007
Acquired by IMS Health in 2016

**QKD Corp** (Toronto) - Founded in 2013

**RedWolf Security** (Waterloo) - Founded in 2005

**Resolver** (Toronto) - Founded in 2000
Acquired by Klass Capital in 2015

**SAPSOL Technologies** (Mississauga) - Founded in 2006

**SecureKey** (Toronto) - Founded in 2008

**SecurifyLabs** (Orleans) - Founded in 2014

**Securit Records Management** (Oakville) - Founded in 1988
Acquired by Iron Mountain in 2014

**Security Compass** (Toronto) - Founded in 2005

**Sensoraxis Inc.** (Ottawa) - Founded in 2015

**Sentry Metrics** (Toronto) - Founded in 1997
Acquired by Herjavec Group in 2014

**SoftwareSecured** (Ottawa) - Founded in 2009

**Solana Networks** (Ottawa) - Founded in 2003

**SOTI** (Mississauga) - Founded in 1995

**SPE Mail** (Toronto) - Founded in 2014

**Spyders** (Toronto) - Founded in 2005

**Squanto** (Ottawa) - Founded in 2015

**SurfEasy** (Toronto) - Founded in 2011
Acquired by Opera in 2015

**Symple ID Inc.** (Waterloo) - Founded in 2013

**Systematics Consulting Inc.** (Toronto) - Founded in 2009

**The SecDev Group** (Ottawa) - Founded in 2009

**Third Brigade** (Ottawa) - Founded in 2004
Acquired by Trend Micro in 2009

**TitanFile** (Waterloo) - Founded in 2011

**TITUS** (Ottawa) - Founded in 2005

**Touch N Go** (Waterloo) - Founded in 2007

**TrustPoint Innovation Technologies, Inc.** (Waterloo) - Founded in 2012

**uConekt Inc.** (Pickering) - Founded in 2015

**VoIPShield Systems** (Ottawa) - Founded in 2005

**VOR Security** (Ottawa) - Founded in 2012

**WAW Technologies** (Ottawa) - Founded in 2014

**WinMagic Data Security** (Mississauga) - Founded in 1997

**XAHIVE** (Ottawa) - Founded in 2013

**Zighra** (Ottawa) - Founded in 2009

Deloitte.

### About Ontario Centres of Excellence

Ontario Centres of Excellence (OCE) Inc. drives the commercialization of cutting-edge research across key market sectors to build the economy of tomorrow and secure Ontario’s global competitiveness. In doing this, OCE fosters the training and development of the next generation of innovators and entrepreneurs and is a key partner with Ontario’s industry, universities, colleges, research hospitals, investors, and governments.

### About the Toronto Financial Services Alliance

The Toronto Financial Services Alliance (TFSA) is a unique, public-private partnership dedicated to growing Toronto region’s financial services cluster and building it as a global financial services centre. Established in 2001, TFSA is a collaboration involving three levels of government, the financial services industry, and academia.

### About this publication

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

### About Deloitte

Deloitte, one of Canada’s leading professional services firms, provides audit, tax, consulting, and financial advisory services. 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 for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte.