



# International Business Development Strategy

May 2024



*Explore how to  
diversify  
Canada's export  
of cybersecurity  
products and  
services to  
international  
markets.*

# Disclaimer

This report was provided to inform and assist In-Sec-M with developing its International Business Development Strategy.

Deloitte does not assume any responsibility or liability for losses incurred by any party because of the circulation, publication, reproduction, or use of this report contrary to its intended purpose. This report has been made only for the purpose stated and shall not be used for any other purpose. Neither this report (including references to it) nor any portions thereof (including without limitation the identity of Deloitte or any individuals signing or associated with this report, or the professional associations or organizations with which they are affiliated) shall be disseminated to third parties by any means or included in any document without the prior written consent and approval of Deloitte.

Our report and work product cannot be included, or referred to, in any public or investment document without the prior consent of Deloitte LLP. The analyses are provided as of May 2024, and we disclaim any undertaking or obligation to advise any person of any change in any fact or matter affecting this analysis, which may come or be brought to our attention after the date hereof. Without limiting the foregoing, if there is any material change in any fact or matter affecting the analyses after the date hereof, we reserve the right to change, modify or withdraw the analysis.

Observations are made based on economic, industrial, competitive and general business conditions prevailing as at the date hereof. In the analyses, we may have made assumptions with respect to the industry performance, general business and economic conditions and other matters, many of which are beyond our control, including government and industry regulation. No opinion, counsel, or interpretation is intended in matters that require legal or other appropriate professional advice. It is assumed that such opinion, counsel, or interpretations have been, or will be, obtained from the appropriate professional sources. To the extent that there are legal issues relating to compliance with applicable laws, regulations and policies, we assume no responsibility, therefore. We believe that our analyses must be considered as a whole and that selecting portions of the analyses, or the factors considered by it, without considering all factors and analyses together, could create a misleading view of the issues related to the report. Amendment of any of the assumptions identified throughout this report could have a material impact on our analysis contained herein. Should any of the major assumptions not be accurate or should any of the information provided to us not be factual or correct, our analyses, as expressed in this report, could be significantly different.

**Deloitte.**

# Contents

## **Sector Analysis** **7**

---

Overview of In-Sec-M **8**

---

Sector Overview **10**

---

International Activities **17**

---

## **International Business Development Targets** **21**

---

Sector Trends and Market Outlook **22**

---

In-Sec-M Member Coverages **27**

---

Target Market Analysis **32**

---

## **International Business Strategy Development** **50**

---

SWOT Analysis **51**

---

Strategic Objectives **53**

---

Tactical Action Plan **56**

---

# List of Acronyms

<b>AI</b>	Artificial Intelligence
<b>CAGR</b>	Compound Annual Growth Rate
<b>CUSMA</b>	Canada-United States-Mexico Agreement
<b>D&amp;S</b>	Defense and Security
<b>EBIT</b>	Earnings Before Interest and Taxes
<b>ECG</b>	Export Controls Guide
<b>EIPA</b>	Exports and Imports Permits Act
<b>EMBRAPII</b>	Canada-Brazil Calls for Proposals
<b>GDP</b>	Gross Domestic Product
<b>GDPR</b>	General Data Protection Regulation
<b>GIC</b>	Government in Council
<b>IAM</b>	Identity and Access Management
<b>ICS</b>	Industrial Control Systems
<b>ICT</b>	Information and Communications
<b>IP</b>	Internet Protocol
<b>IRAP</b>	Industrial Research Assistance Program
<b>IT</b>	Information Technology
<b>NRCC</b>	National Research Council Canada
<b>OT</b>	Operation Technology
<b>SCADA</b>	Supervisory Control and Data Acquisition
<b>SME</b>	Small to Medium Enterprise
<b>USD</b>	U.S. Dollar

# Purpose of the Study

The primary objective of this International Business Strategy (the “Strategy”) is to explore how to diversify Canada’s export of cybersecurity products and services to international markets.

The study was conducted in three distinct phases. The first phase involved conducting a comprehensive sector overview to gain insights into the economic footprint, industry characteristics, industry segments, and capabilities of the Canadian cybersecurity sector. Additionally, this report section examined In-Sec-M’s services and past international activities. Furthermore, a list of major international conferences that can facilitate export diversification for Canadian companies was compiled for future considerations.

The second phase of the study focused on analyzing global trends that impact the demand and supply of Canadian cybersecurity offerings. Information from various sources, including In-Sec-M’s industry survey, past mission reports, stakeholder engage-

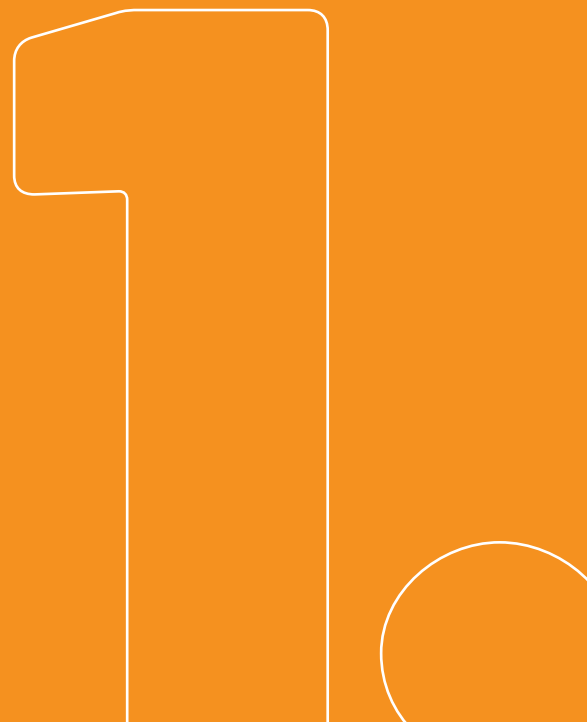
ments, market research, and expert opinions, was gathered to identify markets with potential for export diversification. This analysis also explored specific areas within those sectors that present potential opportunities.

The third phase of the study involved developing strategic objectives and actions for In-Sec-M and the Canadian cybersecurity sector to consider for future implementation.

It is important to note that this study aims to explore opportunities for export diversification. Consequently, markets such as the United States, where strong trading activities already exist, were not included in this study. However, it should also be emphasized that this study does not limit the future international engagement activities of In-Sec-M and Canadian cybersecurity companies. Exploring new markets and opportunities remains a priority for market development and should continue to be pursued.



# Sector Analysis



# Overview of In-Sec-M

In-Sec-M is the national cybersecurity cluster in Canada. Founded in 2017 with the support of the National Research Council Canada (NRCC), In-Sec-M aims to bring together Canadian companies specializing in cybersecurity to help them establish a strong presence in national and international cybersecurity markets. As a non-profit organization, In-Sec-M acts as a bridge between organizations with cybersecurity needs and those that provide solutions. With a network of more than 200 cybersecurity solution and service providers, independent experts, research centres, educational institutions and government agencies, In-Sec-M facilitates connections and promotes Canadian cybersecurity services and solutions to major decision-makers. Additionally, In-Sec-M collaborates with provincial and federal departments to develop and deliver tailor-made services and training courses, leveraging the expertise of experienced Canadian companies in the field.

## Organizational Goals

In-Sec-M has set ambitious organizational goals to establish a competitive and internationally recognized Canadian cybersecurity industry. With the increasing prevalence of cyber threats and their detrimental impact on various aspects of society, In-Sec-M recognizes the urgent need for a robust cybersecurity framework. The organization acknowledges that cyberattacks are becoming more frequent, sophisticated, and costly, affecting the democratic space, essential services, and the intellectual property of Canadian innovators. However, In-Sec-M also sees cybersecurity as an opportunity for economic growth and job creation. By fostering a dynamic ecosystem and promoting the development of first-class solutions, In-Sec-M aims to ensure that the Canadian cybersecurity industry remains agile, competitive, and capable of addressing both national and international cybersecurity challenges effectively.

## In-Sec-M Capabilities

**In-Sec-M's strategy stands on three intertwined axes:**



**Innovation:** In-Sec-M supports initiatives to strengthen the cybersecurity innovation ecosystem in Canada, while fostering innovation partnerships with foreign organizations to address the most complex needs of organizations, strategic sectors, and territories.



**Security:** In-Sec-M, in collaboration with the federal and provincial governments, designs and implements various programs and initiatives to assist and support cyber resilience, making the expertise of the ecosystem available to organizations wishing to strengthen their cybersecurity.



**Market:** In-Sec-M designs and implements projects that strategically position the Canadian cybersecurity industry, acting as a cohesive platform to ensure the penetration of major national and international markets for the various players in the ecosystem.



## International Trade Missions

To increase Canadian exports of cybersecurity products and services to global markets, In-Sec-M organizes strategic trade missions. Each year, these trade missions allow Canadian enterprises, especially small and medium-sized enterprises (SMEs), representatives of research centers, sector support organizations, and various government organizations to expand their activities internationally, develop strategic partnerships, and promote Canadian expertise on an international scale, while increasing investment opportunities in Canada.



## Assistance Programs

To strengthen the cybersecurity capabilities of Canada's economy, In-Sec-M, in collaboration with the federal and provincial governments, provides organizations with a variety of assistance programs. Two of the programs currently available are described below.

**Assistance Program MaLoi25:** In-Sec-M has designed an assistance program, with the financial support of the government of Québec, to help any organization, for-profit or not, who has its head office in Quebec and fewer than 500 employees to comply with Act 25 for the protection of personal information and enhance their cybersecurity. This program includes access to a self-diagnosis tool as well as awareness, training, and coaching services.

**SME Cyber Security Support Program:** This is a program that supports innovative Canadian SMEs by providing cybersecurity consulting services through the National Research Council's (NRC) Industrial Research Assistance Program (IRAP). This program provides customized support in the form of consulting services, particularly in the areas of information systems protection or compliance with specific practices, laws, regulations, standards or certifications, or for the development of new solutions in cybersecurity.

# Sector Overview

The Canadian cybersecurity sector has become increasingly important, reflecting the global rise of cyber threats alongside the rapid digital transformation across many industries in Canada. This section provides an overview of the Canadian sector and highlights its importance.

## Economic Footprint

Canada has established itself as a global leader in the field of cybersecurity, evident through its commitment and capabilities. The Global Cybersecurity Index (GCI)<sup>1</sup> of 2020, published by the International Telecommunication Union (ITU), serves as a comprehensive measure of countries' dedication to cybersecurity on a global scale. Out of the 194 countries assessed, Canada secured an impressive 8th position in terms of its commitment to cybersecurity. The economic footprint of Canada's cybersecurity industry and its value chain is significant, contributing over \$3.2 billion to the national GDP according to Statistics Canada's 2020 survey<sup>2</sup>. Half of the GDP contribution was directly attributed to the industry's economic activities, while 25% (\$0.8 billion) was attributed to Canadian suppliers to the industry and the 25% (\$0.8 billion) was from consumer spending by associated employees.<sup>3</sup>

The Canadian cybersecurity industry directly employs more than 14,100 people (as at 2020), and in total contributes to more than 29,400 jobs national-wide (including indirect and induced jobs). From 2018 to 2020, the industry experienced high growth demonstrated by an increase of \$860 million in GDP and 6,900 total new jobs created. In addition, the industry also experienced significant growth during the pandemic. For example, from 2020 to 2022, the industry's sales of goods and services had grown by 49%.

## Industry Characteristics

The 2022 Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey revealed that there are 463 businesses operating in the cybersecurity industry. The industry is predominantly composed of SMEs, with 90% of the firms employing fewer than 250 people. These SMEs contribute to approximately 39% of the industry's revenues, 37% of its employees, 22% of its research and development (R&D) efforts, and 18% of its exports.

In terms of ownership, the majority of the businesses in the Canadian cybersecurity industry (81%, or 374 businesses) are Canadian-owned or have their parent company located in Canada. These Canadian companies account for 71% of the industry's total revenues. Among the Canadian companies, three quarters (339 businesses) are Canadian-controlled private corporations. However, these private corporations only contribute to 28% of the industry's sales. There are 56 businesses (12% of total businesses) operating in Canada that are owned by parent companies located in the United States. Despite their small number, these businesses contribute to almost 22% of the industry's revenues.

The Canadian cybersecurity industry is renowned for its high intensity of R&D activities. According to Statistics Canada data, the sector's R&D activities in 2020 were nearly 2.5 times greater than the Canadian information and communications technology (ICT) industry average.

1. [ITU Publications](#)
2. Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey, Statistics Canada, 2022
3. Total sales of the industry, as reported later in the document, exceed its contribution to GDP. This discrepancy arises due to the treatment of intermediate inputs, with total sales representing the full value of goods and services sold, while GDP contribution focuses on value added after subtracting the cost of inputs. Factors such as reliance on imports or low value-added activities can contribute to the higher total sales compared to GDP contribution.

## Industry Segments

The cybersecurity industry can be further segmented into the following business activities<sup>4</sup>, based on the types of goods and services that each segment produces:

- › **Compliance Audits and Program Development:** This segment encompasses the provision of compliance audits, program development, strategy development and risk management and consulting services, including cybersecurity audits, strategy development, compliance program development and other related consulting services.
- › **Industrial Control Systems (ICS):** This segment focuses on cybersecurity solutions and services aimed at safeguarding industrial control systems, supervisory control and data acquisition (SCADA), and operation technology (OT), including products like Hardware Security Modules and Hardware Cryptographic Modules, while excluding protection for enterprise information technology (IT) networks.
- › **Encryption:** This segment encompasses sales related to hardware or software-based encryption, as well as services for developing or implementing encryption, including activities related to quantum-proof algorithms and encryption, excluding the integration or resale of commercial encryption and encryption primarily included under another goods and services category.
- › **Infrastructure Solutions:** This segment focuses on sales of services for cybersecurity infrastructure, including the establishment of ongoing protection for networks and data. This includes services and solutions such as firewalls, intrusion detection and prevention systems, managed security service providers, web application firewalls, secure email gateways, endpoint security, detection and response, insider threat detection, identity and access management/control, application security tools, security system design and integration, cybersecurity orchestration and automation, cloud-based cybersecurity solutions, and other technologies designed to protect against attacks using cryptanalytic techniques.
- › **Penetration Testing and Threat Monitoring:** This segment involves sales related to penetration testing, vulnerability assessments, and activities in the cyber domain aimed at detecting, monitoring, analyzing, understanding, and predicting cyber threats to improve situational awareness and strengthen cyber defenses, including the conduct of active cyber defense measures to protect data, networks, infrastructure, and other systems from offensive and exploitative cyber capabilities and actions.
- › **Forensics and Investigation:** This segment involves sales related to the production of goods and/or provision of services for identifying, assessing, and responding to cyber-attacks and incidents, including services and software tools for network forensics, hunt services, fraud analytics, identification of inside perpetrators, and other incident response services.
- › **Training:** This segment encompasses sales related to the production of goods and/or provision of services for cybersecurity training, workforce development, and educational services or solutions, catering to all levels from basic users to advanced practitioners, and utilizing various delivery mechanisms such as services, courseware, software, and more.

4. Ibid.

## Canadian Capabilities

When looking at the sales of different categories in the Canadian cybersecurity industry, it is found that the significant strength of the Canadian cybersecurity industry lies in providing cybersecurity infrastructure services and solutions for the ongoing protection of networks and data. In 2022, this category has the highest total sales, amounting to \$3.7 billion, and also the highest sales in software and/or hardware<sup>5</sup>, with \$1.5 billion. This indicates a strong capability and demand in providing comprehensive cybersecurity solutions to protect networks and data.

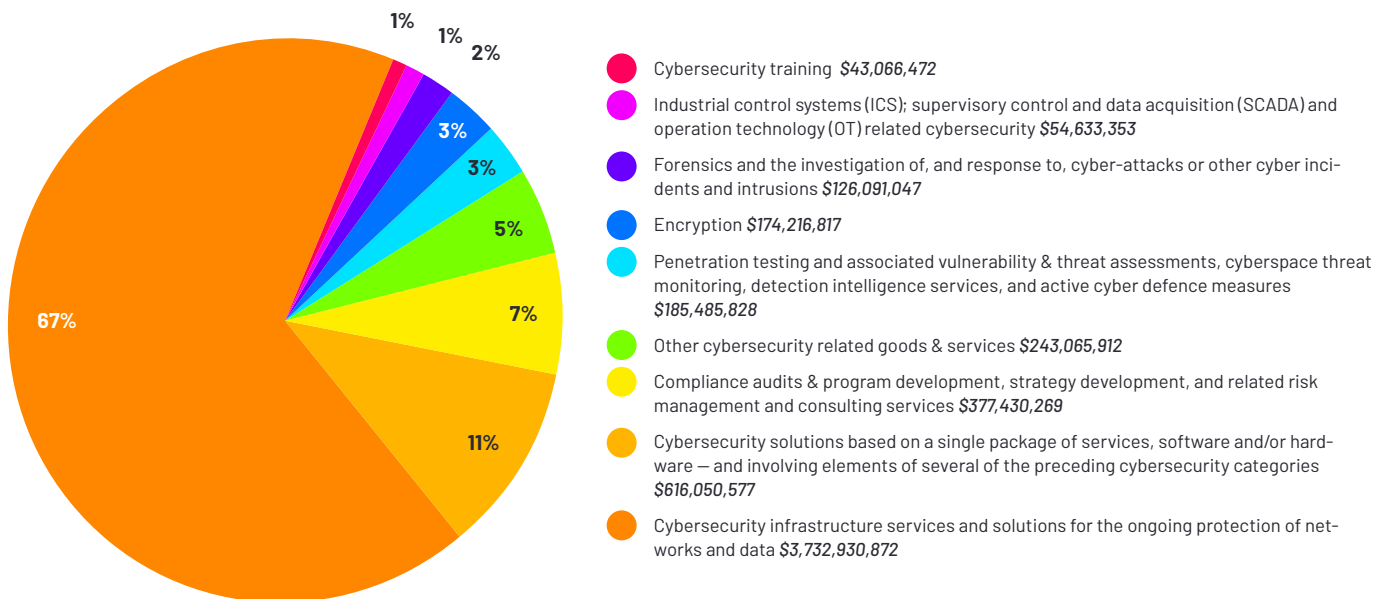
The industry also shows a strong capability in compliance audits, program development, strategy development, and related risk management and consulting services. This category has the second-highest total sales (excluding the category of cybersecurity solutions based on a single package of services, software and/or hardware), amounting to \$377 million, and also significant sales in software and/or hardware, with \$116 million. This

suggests that Canadian cybersecurity companies are proficient in helping businesses comply with cybersecurity regulations and develop effective strategies.

The category of “penetration testing and associated vulnerability and threat assessments, cyberspace threat monitoring, detection, intelligence services, and active cyber defence measures” is another crucial aspect of the Canadian cybersecurity industry. With total sales of \$185 million it represents a significant portion of the industry’s revenue. However, the sales of software and/or hardware in this category is low, compared with other categories with high overall sales.

Encryption also stands out as a strong capability, with total sales of \$174 million and software and/or hardware sales of \$100,260,274. This indicates that the industry is investing significantly in encryption technologies, which are crucial for securing data.

**Figure 1 Sales of Cybersecurity Goods and Services, by Goods and Services Categories, Canada, 2022**



5. The difference between an industry’s total sales and its sales of hardware and software may include revenues generated from billable hours of the workforce through services provided.

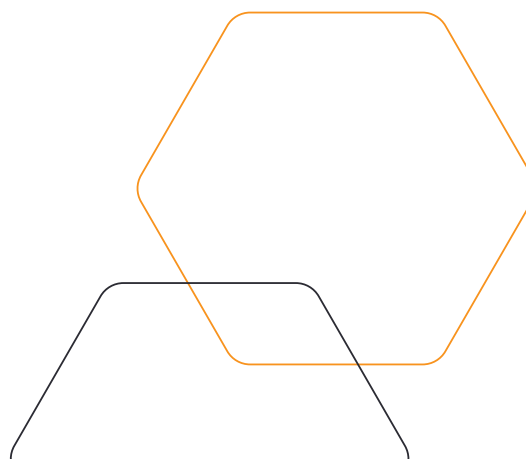
**Table 1 Sales of Cybersecurity Goods and Services, by Software and/or Hardware, Canada, 2022**

Goods and Services Category	Total Category Sales (\$)	Sales (\$) of: Software and/or Hardware
Cybersecurity infrastructure services and solutions for the ongoing protection of networks and data	3,732,930,872	1,509,967,917
Cybersecurity solutions based on a single package of services, software and/or hardware—and involving elements of several of the preceding cybersecurity categories.	616,050,577	325,522,053
Compliance audits and program development, strategy development, and related risk management and consulting services	377,430,269	116,890,323
Other cybersecurity related goods and services	243,065,912	152,740,766
Penetration testing and associated vulnerability & threat assessments, cyberspace threat monitoring, detection, intelligence services, and active cyber defence measures	185,485,828	29,286,658
Encryption	174,216,817	100,260,274
Forensics and the investigation of, and response to, cyber-attacks or other cyber incidents and intrusions	126,091,047	15,437,997
Industrial control systems (ICS); supervisory control and data acquisition (SCADA) and operation technology (OT) related cybersecurity	54,633,353	6,086,022
Cybersecurity training	43,066,472	6,310,658
<b>Total Cybersecurity Industry</b>	<b>5,552,971,147</b>	<b>2,262,502,669</b>

(Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey, Statistics Canada)

During the period from 2020 to 2022, the sales of cybersecurity infrastructure services showed the highest growth in sales volume, experiencing a significant increase of 70%, resulting in a sales boost of approximately \$1.54 billion. The segment of compliance audits and program development, strategy development, and related risk management and consulting services also experienced a sales boost of about \$114 million. Additionally, there was a notable increase of \$54 million in the sales of services related to forensics, cyber-attacks, and intrusion investigations.

However, certain categories witnessed a decline in sales from 2020 to 2022, particularly Encryption and the ICS, SCADA, and OT related categories. The Encryption category experienced a 29% decrease (equivalent to \$73 million) in sales in 2022 compared to 2020, while the ICS; SCADA and OT category saw a significant 68% decline (equivalent to \$116 million) during the same period.



**Table 2 Composition of Industry Revenues and Changes Between 2020 and 2022 by Goods and Services Type**

Goods and Services Category	Total Category Sales (\$) (2020)	Total Category Sales (\$) (2022)	Growth of Sales (%) (2020 - 2022)	Total Category Percentages (%) (2022)
Cybersecurity infrastructure services and solutions for the ongoing protection of networks and data	\$2,192,703,687	\$3,732,930,872	70%	67.2%
Cybersecurity solutions based on a single package of services, software and/or hardware—and involving elements of several of the preceding cybersecurity categories.	\$402,764,728	\$616,050,577	53%	11.1%
Compliance audits and program development, strategy development, and related risk management and consulting services	\$263,543,386	\$377,430,269	43%	6.8%
Other cybersecurity related goods and services	\$187,580,158	\$243,065,912	30%	4.4%
Penetration testing and associated vulnerability and threat assessments, cyberspace threat monitoring, detection, intelligence services, and active cyber defence measures	\$174,023,686	\$185,485,828	7%	3.3%
Encryption	\$246,812,300	\$174,216,817	-29%	3.1%
Forensics and the investigation of, and response to, cyber-attacks or other cyber incidents and intrusions	\$72,238,812	\$126,091,047	75%	2.3%
Industrial control systems (ICS); supervisory control and data acquisition (SCADA) and operation technology (OT) related cybersecurity	\$170,577,097	\$54,633,353	-68%	1.0%
Cybersecurity training	\$26,443,076	\$43,066,472	63%	0.8%
<b>Total Cybersecurity Industry</b>	<b>\$3,736,686,930</b>	<b>\$5,552,971,147</b>	<b>49%</b>	<b>-</b>

(Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey, Statistics Canada)

(Note: The data reported by Statistics Canada indicates a significant decline in sales of ICS, SCADA, and OT related cybersecurity products and services from 2020 to 2022. However, the data does not provide any explanation for this decline. Despite conducting additional research to seek an explanation, no relevant information could be found.)

**According to the survey results from Statistics Canada, each region possesses specific areas of strengths in the cyber security industry.**

## Geographic Strengths

According to the survey results from Statistics Canada, each region possesses specific areas of strengths in the cyber security industry. Ontario accounted for the largest share of employment in the cybersecurity sector at 48%. The top regional specializations in Ontario included cybersecurity infrastructure solutions, bundled solutions, compliance audits and program development, penetration testing and threat monitoring, and encryption.

Quebec followed with a 15% share of employment, with a focus on cybersecurity infrastructure solutions, compliance audits and program development, bundled solutions, penetration testing and threat monitoring, and training.

Atlantic Canada accounted for 4% of employment and specialized in industrial control systems, bundled solutions, cybersecurity infrastructure solutions, compliance audits and program development, and training.

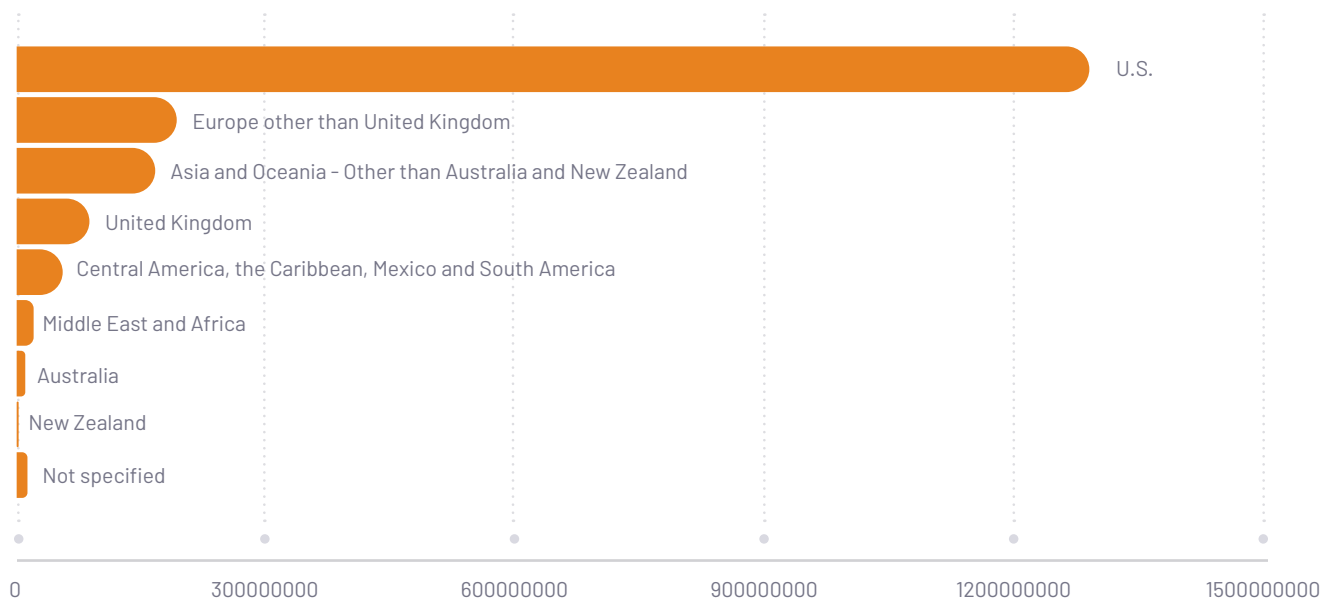
Lastly, Western and Northern Canada represented 33% of employment and had specializations in

cybersecurity infrastructure solutions, bundled solutions, compliance audits and program development, encryption, and industrial control systems. In particular, the province of British Columbia in Western Canada has emerged as a hub for cybersecurity, housing more than 11,000 technology companies, tech giants such as Amazon, Salesforce, Samsung and Microsoft, and global leading cybersecurity providers such as Fortinet, Splunk, IBM and the Mastercard's Global Intelligence. Local entities like Trade and Invest B.C. and Cyber Centre of Excellence actively contribute to the advancement of the cybersecurity sector in British Columbia.

## Exports

In 2022, the exports of cybersecurity products and services accounted for 33% of the industry's total revenue<sup>6</sup>. The Canadian cybersecurity industry exported \$1.83 billion of products and services, and almost 70% (\$1.29 billion) to the U.S. Other major export markets include Europe, Asia, Australia and New Zealand.

**Figure 2 Export of Cybersecurity Goods and Services, by Type of Customer and Countries, Canada, 2022**



6. Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey (2022), Statistics Canada

**Figure 3 Export of Cybersecurity Goods and Services, by Type of Customer and Countries, Canada, 2022**

Total export sales	Export Sales (\$)(2022)
Sales to U.S. federal government	\$8,835,928
Sales to non-government entities in U.S. defence, cybersecurity or commercial and civil marine sectors (including subcontracts)	\$113,772,181
Sales to other U.S. customers	\$1,162,879,378
Breakdown not specified	\$3,800,758
<b>Total sales to U.S.</b>	<b>\$1,289,288,246</b>
Sales to Europe other than United Kingdom	\$192,397,638
Sales to Asia and Oceania - Other than Australia and New Zealand	\$166,533,552
Sales to United Kingdom	\$87,468,734
Sales to Central America, the Caribbean, Mexico and South America	\$55,325,559
Sales to Middle East and Africa	\$20,390,194
Sales to Australia	\$10,345,469
Sales to New Zealand	\$2,160,609
Breakdown not specified	\$12,973,330
<b>Total export sales</b>	<b>\$1,836,883,330</b>

(Source: Canadian Defence, Aerospace, Marine and Cybersecurity Industries Survey, Statistics Canada)





# 13 International Activities

## International Engagement

In recent years, In-Sec-M has significantly expanded its international engagement efforts to foster relationships with prominent global cybersecurity ecosystems and facilitate the entry of Canadian cybersecurity solutions and service providers into international markets.

To accomplish this, In-Sec-M has organized nearly 20 market exploration and development missions across Asia, North and South America, Europe, Middle East and Africa. In addition, the organization has actively participated in over 20 international events. These initiatives have enabled In-Sec-M to showcase the capabilities of Canadian companies with export potential, as well as engage university researchers, experts, and government representatives.

Through these endeavours, In-Sec-M has successfully established strategic alliances with various global ecosystems. A notable example is the recent partnership agreement with the Pôle d'excellence Cyber in France. This collaboration aims to enhance dynamism, innovation, and the promotion of joint projects within the French and Canadian cybersecurity ecosystems.

In-Sec-M is committed to further expanding its international reach in the upcoming years. The organization plans to conduct exploratory missions targeting new countries, as well as market development missions, thereby continuing its efforts to support Canadian cybersecurity businesses with their global expansion.

## International Conferences

The following table provides a comprehensive list of major international cybersecurity conferences across various markets. This valuable information is essential for future business development activities, as attending conferences plays a crucial role in fostering industry connections, staying updated on the latest trends, and showcasing the expertise of Canadian cybersecurity solutions and service providers. The table includes the names, descriptions, locations, sizes, and dates of these conferences, offering a comprehensive overview of the key events in the global cybersecurity landscape.



## North America Conferences

Conference Name	Description	Location	Size of Conference	Date
<a href="#">RSA Conference</a>	Brings together experts, professionals, and global thought leaders to discuss trends, challenges, and solutions in cybersecurity. RSA offers a variety of activities, including keynote speeches, panel discussions, technical sessions, hands-on labs, workshops, and networking events. It covers topics such as cloud security, AI, data privacy, threat intelligence, and cryptography. The conference also features an Expo where exhibitors showcase their latest products and services.	San Francisco, U.S.	<ul style="list-style-type: none"> <li>› 40,000 attendees</li> <li>› 650 speakers</li> <li>› Over 500 exhibitors</li> </ul>	May 6 to 9 2024
<a href="#">Cyber Security &amp; Cloud Expo (Congress North America)</a>	Cyber Security & Cloud Expo is the leading event covering Zero-Day Vigilance, Threat Detection, Global Cyber Conflicts, Generative AI, Quantum Computing, Risk Management, Cloud Transformation, Hybrid Cloud strategies, DevSecOps Integration and Artificial Intelligence (AI) & Machine Learning (ML) in Infrastructure.	Santa Clara, U.S.	<ul style="list-style-type: none"> <li>› 7,000 attendees</li> <li>› 250 speakers</li> </ul>	June 5 to 6 2024
<a href="#">SecTor</a>	SecTor has built a reputation of bringing together experts from around the world to share their latest research and techniques. In a non-threatening and productive way, SecTor sheds light on the underground threats and mischief that threaten corporate and personal IT systems.	Toronto, Canada	› Not known	October 22 to 24 2024
<a href="#">Infosecurity Mexico</a>	Infosecurity Mexico is one of the leading cybersecurity events in Mexico and Latin America. It is an annual conference and exhibition that focuses on bringing together cybersecurity professionals, experts, and industry leaders to discuss and address the latest trends, challenges, and solutions in the field	Mexico City, Mexico	<ul style="list-style-type: none"> <li>› 1,600+ attendees</li> <li>› 60+ business meetings</li> </ul>	October 22 to 23 2024

## South America Conferences

Conference Name	Description	Location	Size of Conference	Date
<a href="#">Cybertech Latin America</a>	Cybertech Latin America has been the conduit connecting the region's foremost cyber, business, and innovation ecosystems. The conference will include sessions on innovative technologies, collaboration, data and more.	Panama City, Panama	› Not known	March 13 to 14 2024
<a href="#">Cyber Security Summit Brazil</a>	This is annual event brings together industry experts, thought leaders, and professionals in the field of cybersecurity to discuss emerging trends, share knowledge, and explore solutions to the challenges faced in the digital world. The Security Leaders Brazil Summit focuses on SMEs embracing technologies, regulations, cyber threats and more.	Sao Paulo, Brazil	› Not known	October 28 to 29 2024

## Europe Conferences

Conference Name	Description	Location	Size of Conference	Date
<a href="#">CyberSecurity Conference</a>	This conference examines how Europe can stay at the forefront of cybersecurity advancements and contribute to global collective efforts in securing our digital future. Key topics include European cybersecurity policy framework in safeguarding the continent's digital economy, supply chain integrity, and the transformative impact that AI and collaboration.	Brussels, Belgium	<ul style="list-style-type: none"> <li>› Over 200 participants</li> <li>› 5 sessions</li> </ul>	March 19 2024
<a href="#">InfoSecurity Europe</a>	InfoSecurity Europe is one of the leading gatherings of the information security industry in Europe. Each year, we bring the community together to share innovation, learn from each other, test and benchmark solutions, build relationships, drive new business and connect with colleagues. The leading suppliers choose InfoSecurity Europe as an opportunity to launch new technologies, products and services.	London, United Kingdom	<ul style="list-style-type: none"> <li>› 13,800 plus attendees</li> <li>› 380 plus exhibitors</li> </ul>	June 4 to 6 2024
<a href="#">Cybersec Expo &amp; Forum</a>	Cybersec Expo is a leading cybersecurity conference. It focuses on emerging technologies, cybersecurity trends, and export opportunities for companies in the cybersecurity sector as well as Venture Capital investments in the region.	Katowice, Poland	<ul style="list-style-type: none"> <li>› Not known</li> </ul>	June 19 to 20 2024
<a href="#">Connect at Tech Show London</a>	Technology exhibition and conference held annually. It brings together industry professionals, innovators, and technology enthusiasts from around the world to showcase the latest advancements in various fields such as cybersecurity.	London, United Kingdom	<ul style="list-style-type: none"> <li>› 14,850+ plus attendees</li> <li>› 71 exhibitors</li> </ul>	March 12 to 13 2024
<a href="#">National Cyber Security Show</a>	The National Cyber Security Show in Birmingham offers two main components: the Solutions Theatre and the Leaders' Summit. The Solutions Theatre provides an excellent platform for exhibitors to showcase their product capabilities, technological advancements, and key cyber solutions to an engaged audience. This audience consists of individuals with active projects and buying power, making it a valuable opportunity for companies to demonstrate their offerings and attract potential customers.	Birmingham, United Kingdom	<ul style="list-style-type: none"> <li>› Not known</li> </ul>	April 30 to May 2 2024
<a href="#">CyberWiseCon Europe</a>	CyberWiseCon is a premier IT security conference that brings together cybersecurity experts, industry leaders, and IT professionals from around the Europe. Provides a platform for cybersecurity companies to showcase their latest productions, services and innovations.	Lithuania (available online as well)	<ul style="list-style-type: none"> <li>› 700 + attendees</li> <li>› 130+ speakers</li> <li>› 35+ countries</li> </ul>	May 20 to 24 2024
<a href="#">Les Assises de la cybersécurité</a>	Les Assises de la cybersécurité is one of the most prominent cybersecurity conferences in France. It is an annual event that brings together cybersecurity professionals, experts, and industry leaders to discuss and address the challenges and solutions in the field.	Monaco	<ul style="list-style-type: none"> <li>› 1400+ guests</li> <li>› 170+ partner companies</li> <li>› 120+ experts and journalists</li> </ul>	October 9 to 12 2024

<a href="#">InCyber Forum Europe</a>	The InCyber Forum is Europe's leading event for digital security and trust. Its unique feature is that it brings together the entire cybersecurity and "trusted digital" ecosystem: end-customers, service providers, solution vendors, consultants, law enforcement and government agencies, schools and universities.	Lille, France	<ul style="list-style-type: none"> <li>› 20,000+ visitors</li> <li>› 700+ partners</li> <li>› 103 represented countries</li> </ul>	April 1 to 3 2025
<a href="#">Cloud Expo Europe Frankfurt</a>	Cloud & Cyber Security Expo is a prominent cybersecurity event held in Germany. It is a part of Tech Show Frankfurt, presented by CloserStill Media. The event focuses on bringing together industry professionals, experts, and leading vendors to discuss and showcase the latest developments, challenges, and solutions in cloud computing and cybersecurity.	Frankfurt, Germany	<ul style="list-style-type: none"> <li>› 6,200+ attendees</li> <li>› 300+ sessions</li> <li>› 1,100+ meetings arranged</li> </ul>	May 22 to 23 2024
<a href="#">Global Cyber Conference</a>	The Global Cyber Conference is an international cybersecurity event in Switzerland gathering an audience of senior cybersecurity stakeholders, decision-makers, public authorities, and academia from all around the globe. It provides key decision-makers a networking and learning platform to gain a shared understanding of what needs to be done to strengthen cyber resilience.	Zurich, Switzerland	<ul style="list-style-type: none"> <li>› 350+ attendees from 30+ countries</li> </ul>	November 26 to 27 2024
<a href="#">ItaliaSec Cyber Summit</a>	ItaliaSec is a CPE certified IT security conference, uniting 150+ senior security leaders from Italy's public and private sectors.	Rome, Italy	<ul style="list-style-type: none"> <li>› 150+ cybersecurity leaders</li> </ul>	May 13 to 14 2025

## Asia Conferences

Conference Name	Description	Location	Size of Conference	Date
<a href="#">Cyber Security World Asia</a>	Annual event that takes place in Singapore, focusing on the latest trends, challenges, and solutions in the field of cybersecurity. The event features a range of activities including keynote speeches, panel discussions, workshops, and exhibitions topics include lead generation.	Singapore	<ul style="list-style-type: none"> <li>› 23,864 attendees visited Tech week in 2023 (Cyber Security World Asia is part of the Tech Week Singapore event)</li> </ul>	October 9 to 10 2024
<a href="#">GovernmentWare (GovWare)</a>	GovWare is Singapore's largest cybersecurity conference and exhibition. GovWare unites policymakers, tech innovators and end-users across Asia and beyond, driving pertinent dialogues on the latest trends and critical information flow.	Singapore	<ul style="list-style-type: none"> <li>› 12,000 plus attendees</li> </ul>	October 15 to 17 2024
<a href="#">CODE BLUE</a>	The conference offers cutting-edge lectures by cybersecurity professionals and opportunities for information exchange and collaboration across borders. By uniting experts from various fields, the conference aims to enhance cybersecurity cooperation in Asia and cultivate talented researchers in Japan and Asia. CODE BLUE 2024, is in its 12th year.	Tokyo, Japan	<ul style="list-style-type: none"> <li>› Not known</li> </ul>	November 9 to 15 2024

# International Business Development Targets

This report section examines socio-economic and sector-specific trends affecting the cybersecurity industry globally. It then presents thorough research on potential markets for diversifying Canada's exports. Each selected market comes with a profile that outlines the opportunities and challenges that were informed by market research, stakeholder engagement, and previous In-Sec-M mission reports.



# Sector Trends and Market Outlook

## Trends Impacting Cybersecurity Demand

The following global trends are impacting the demand for cybersecurity products and services. For Canadian cybersecurity industry aiming to diversify its export of goods and services to international markets, they face implications from these industry trends such as increasing digitalization, the impact of the COVID-19 pandemic, the adoption of AI, and stringent cybersecurity regulations. These trends create opportunities for Canadian cybersecurity firms to provide support in areas such as securing digital transformations, protecting against remote working cyber risks, leveraging AI technology, and meeting regulatory requirements. By addressing these trends and offering solutions that align with the evolving needs of organizations worldwide, Canadian firms can position themselves as reliable partners in the global cybersecurity market.

## *Increasing Digitalization Across All Sectors*

As technology continues to advance and companies recognize the advantages of digitalization, there is a noticeable trend in industries adopting Internet of Things (IoT) technologies. Whether it is for business-to-business operations or business-to-consumer interactions, organizations are increasingly incorporating IoT into their activities. One of the key considerations when it comes to digital trans-

formation is the financial impact, specifically the cost-benefit analysis – the potential for cost reduction and, ultimately, the generation of increased revenue.

Many organizations perceive digitalization as a costly endeavor. However, extensive research indicates that the expenses incurred by being disrupted and eventually phased out of the market are often more significant than the investments required to upgrade operations. In today's global economy, traditional methods are frequently inadequate in addressing the rapid pace and scale of challenges. A study conducted by McKinsey & Company in 2020 specifically addressed this concern in the manufacturing sector<sup>7</sup>, demonstrating how companies can enhance both efficiency and productivity by streamlining steps in the value chain through IoT products.

Furthermore, a separate study conducted by Boston Consulting Group revealed that organizations that undergo digital transformations experience a significant increase in EBIT (earnings before interest and taxes). On average, these organizations saw a 21% increase in EBIT, compared to a 10% increase for organizations that did not undergo digital transformations<sup>8</sup>. Additionally, when examining industries such as the Financial Industry, Consumer, Energy, Health care, Industrial Goods, Insurance, and Tech, it was found that 71% of organizations (that had undergone digital transformation) experienced sales and market acceleration<sup>9</sup>.

7. Industrial IoT generates real value, McKinsey & Company, 2020

8. Performance and Innovation Are the Rewards of Digital Transformation, Boston Consulting Group, 2021

9. Ibid.

Canadian cybersecurity firms have a significant opportunity to provide support to organizations that are embarking on infrastructure updates through digitalization. In order to capitalize on this opportunity, it is crucial for the Canadian market to operate efficiently and effectively promote its solutions as a viable option for these organizations with increasing foreign competition.

### *The Pandemic Has Created New Challenges*

The COVID-19 pandemic had a significant impact on the cybersecurity industry globally. As organizations shifted to remote working, there was an increased reliance on technology and digital platforms. However, many organizations were unable to provide a secure remote-working environment, leaving employees vulnerable to cyber risks. This has created a greater need for cybersecurity measures to protect sensitive data and prevent cyberattacks. The rise in remote working has also led to an increase in cyberattacks, with hackers exploiting the vulnerabilities of employees working from home<sup>10</sup>. Phishing scams, fraudulent websites, and direct attacks on companies have become more prevalent. Video conferencing services have been targeted, with hackers stealing personal data and disrupting businesses. The cyber threat landscape has become more diverse and intensified, with malicious employees, cybercriminals, hacktivists<sup>11</sup>, and script kiddies<sup>12</sup> contributing to increased cybersecurity threats. Enhanced detection mechanisms, such as user and entity behavior analysis (UEBA), are needed to identify anomalous activities and prevent cyberattacks. Addressing human error and adapting IT systems to remote working environments are crucial for maintaining cybersecurity. The pandemic has highlighted the need for organizations to prioritize cybersecurity and invest in robust measures to mitigate risks.

### *Adoption of Artificial Intelligence (AI)*

The increasing need for advanced cybersecurity solutions is the primary trend driving the growth of AI in cybersecurity market. This surge in demand is significantly boosting the industry's overall demand. A recent report by Acumen Research and Consulting estimated that the global market for AI-based cybersecurity products was \$15 billion in 2021 and is estimated to reach \$135 billion by 2023 at a CAGR of 27.8%<sup>13</sup>.

The use of AI technology is becoming more prevalent in cybersecurity organizations. This trend is motivated by the recognition that AI can play a crucial role in detecting and addressing security threats. By simulating different attack scenarios, AI can effectively identify vulnerabilities and flag potential security issues. This integration of AI intelligence offers significant advantages to cybersecurity organizations, as it enables them to proactively prevent future attacks. By stopping breaches before they happen, not only can the data of individuals and companies be safeguarded, but businesses can also reduce their IT costs.

Furthermore, the 2024 federal government budget introduced several initiatives aimed at advancing AI in Canada. One of these initiatives is the Canadian AI Sovereign Compute Strategy, which aims to promote the development of AI infrastructure that is owned and located in Canada<sup>14</sup>. Additionally, the budget allocated \$2 billion to build and provide access to technological infrastructure for AI researchers, start-ups, and scale-ups in Canada<sup>15</sup>.

In addition to infrastructure development, the federal government plans to establish the Canadian AI Safety Institute. With a budget of \$50 million, this institute will focus on ensuring the safe development and deployment of AI systems. It will collaborate

10. [Impact of COVID-19 on Cybersecurity \(deloitte.com\)](#)

11. Hacktivists are individuals or groups who engage in hacking activities with the aim of promoting a social or political agenda.

12. Script kiddies are individuals with limited technical skills who rely on pre-existing hacking tools, scripts, or software to carry out cyber attacks.

13. [AI and Cybersecurity: A New Era, Morgan Stanley, 2023](#)

14. [Securing Canada's AI advantage, Canada, 2024](#)

15. Ibid.

with stakeholders and international partners to gain insights and protect against the risks associated with advanced or malicious AI systems.

In summary, the Canadian government is fostering an ecosystem that supports and accelerates the growth of the AI industry. By providing resources and infrastructure, it aims to cultivate a domestic supply of AI solutions that can meet both domestic and international demand. This strategic approach will help position Canada as a leader in the field of AI and ensure the country's competitiveness in the global market.

### *Stringent Cybersecurity Regulations*

With the advancement of digital infrastructure, the risk of cybercrimes targeting governments, organizations, and communities has increased significantly<sup>16</sup>. Consequently, governments worldwide are actively mobilizing their efforts to combat, minimize, and ultimately prevent cyber-attacks.

In Canada, the Federal government has recently introduced several new pieces of legislation aimed at enhancing security measures for federally regulated industries and the private sector. One notable development is Bill C-26, which specifically focuses on bolstering security across key sectors such as finance, telecommunications, energy, and transportation.

Part 2 of Bill C-26, known as the Critical Cyber Systems Protection Act, is particularly significant. This Act aims to improve cyber threat information sharing and grants the Governor in Council (GIC)<sup>17</sup> the authority to issue Cyber Security Directions (CSDs)<sup>18</sup>. Under the legislation, designated operators are required to act based on the measures specified in the

CSD within a specified timeframe. Non-compliance with a CSD can result in consequences such as administrative monetary penalties or facing regulatory offenses, which may lead to fines or imprisonment.

In addition, it is important to note that private sector enterprises operating outside of federally regulated industries are bound by the Personal Information Protection and Electronic Documents Act (PIPEDA). This legislation establishes a comprehensive set of rules and principles that organizations must follow to safeguard individuals' personal information<sup>19</sup>. One of the primary objectives of PIPEDA is to prioritize the security of personal information. To meet the requirements of PIPEDA, organizations are obligated to implement a variety of safeguards to mitigate potential risks associated with personal data. These risks include the possibility of loss, theft, unauthorized access, disclosure, copying, use, or modification of personal information.

In 2022, the Government of Canada has tabled Bill C-27, the Digital Charter Implementation Act, 2022 to strengthen Canada's private sector privacy law, create new rules for the responsible development and deployment of artificial intelligence (AI), and continue advancing the implementation of Canada's Digital Charter. As such, the Digital Charter Implementation Act, 2022 introduces three proposed acts: the Consumer Privacy Protection Act, the Artificial Intelligence and Data Act, and the Personal Information and Data Protection Tribunal Act. The proposed Consumer Privacy Protection Act will address the needs of Canadians who rely on digital technology and respond to feedback received on previous proposed legislation. This law will ensure that the privacy of Canadians will be protected and that innovative businesses can benefit from clear rules as technology continues to evolve.

16. [National cyber threat assessment 2023-2024](#)

17. A [Governor-in-Council appointment](#) is one made by the Governor General, on the advice of the Queen's Privy Council of Canada (i.e., the Cabinet). The responsibilities of Governor in Council appointees range from making quasi-judicial decisions, to providing advice and recommendations on socio-economic development issues, to managing Crown corporations.

18. [Protecting Critical Cyber Systems, Government of Canada, 2022](#)

19. [The Personal Information Protection and Electronic Documents Act \(PIPEDA\)](#)



Provincial legislations in Canada are also imposing more stringent rules on cybersecurity of information collection, communication, and storage. In Québec, enactment of An Act to modernize legislative provisions as regards the protection of personal information (hereinafter called “Act 25”), formerly known as Bill 64, has led to significant changes for organizations in that collect, communicate, and use personal information. Based in large part on Europe’s “General Data Protection Regulation” (GDPR), this new provincial law is intended to give more rights to individuals who share their personal information, and, at the same time, it institutes a general principle of transparency.

On the international stage, countries are increasingly focusing on cybersecurity-related rules and regulations, such as the GDPR, Cyber Resilience Act, and NIS Directives in the EU, as well as the General Data Protection Law in Brazil. These regulations present new opportunities for the Canadian cybersecurity industry to provide products and services that meet the demands of these markets. Additionally, globally recognized industry certifications and standards, such as the ISO 27001 standard, the Cyber Essential scheme in the UK, and the Cybersecurity Maturity Model Certification (CMMC) in the US, create further opportunities for Canadian companies to support organizations in obtaining these certifications. In conclusion, the current climate of cyber regulations presents significant opportunities for cybersecurity firms. These regulations mandate that certain classifications of organizations must implement measures to protect specific types of data and other information collected, communicated, and stored. This requirement creates a demand for cybersecurity firms, as they are well-positioned to provide the necessary solutions and expertise in data protection. By offering products and services that align with regulatory requirements, cybersecurity firms can capitalize on this opportunity and thrive in the market.

## Trends Impacting Cybersecurity Supply

The following sector trends are impacting the supply for cybersecurity products and services. These trends, including technological advances and evolving cyber threats, have implications for Canadian companies exporting cybersecurity products. Companies must stay updated on advancements like AI and cloud computing to offer cutting-edge solutions. The growing cyber threats landscape presents opportunities for export, but competition is increasing. Compliance with export controls is also crucial. Canadian firms should ensure they meet regulations to succeed in the global market.

### *Technological Advances*

The field of cybersecurity began to emerge in the 1980s and gained significance alongside the widespread adoption of personal computers. During this era, the technological landscape lacked the presence of cloud computing and the IoTs. Cybersecurity primarily revolved around antivirus software and physical firewalls that were installed directly on computers.

Antivirus programs were originally developed to identify and eliminate computer viruses. However, traditional antivirus software was only programmed to target specific viruses, rendering them ineffective against new and emerging threats until the software was updated. Firewalls acted as a protective shield between internal and external networks, overseeing and managing incoming and outgoing network traffic. Nevertheless, early firewalls had limited capabilities and primarily focused on filtering network traffic based on Internet Protocol (IP) addresses and port numbers.

Today, technological advancements have revolutionized the field of cybersecurity, leading to signifi-

cant changes in the typology of cybersecurity solutions and its sophistication. One notable example is the integration of AI into cybersecurity tools. AI-powered solutions can analyze vast amounts of data and identify patterns, enabling them to detect and respond to threats in real-time. These tools can continuously learn from new threats and adapt their defense mechanisms, accordingly, making them highly effective in combating evolving cyber threats than early renderings of antivirus programs. Additionally, advancements in cloud computing have greatly influenced the type of cybersecurity solutions available. Cloud-based security solutions provide organizations with the flexibility to scale their security measures according to their needs. This eliminates the need for on-premises infrastructure and allows for more efficient and cost-effective security management.

### *Evolving Cyber Threats Landscape*

The growing trend of digitalization has brought about numerous benefits, such as improved efficiency and faster response times as described. However, digital transformation has also expanded the opportunities for cyber criminals to launch attacks. With the increasing interconnectedness of devices and systems, the potential targets for cyber-attacks have multiplied exponentially. To illustrate, the World Economic Forum reports that cybercrime cost organizations and governments a staggering \$11.50 trillion USD globally in 2023<sup>20</sup>. Shockingly, this figure is projected to double to \$23 trillion USD by 2027<sup>21</sup>.

The rising threat landscape has resulted in a significant increase in the deployment of cybersecurity products in the market. According to Mordor Intelligence, the cybersecurity market is projected to reach a value of \$182.84 billion USD by 2024<sup>22</sup>. This growth is primarily fueled by the abundance of

opportunities and ongoing transactions on a global scale. While large corporations have had the advantage of investing in cybersecurity early due to their resources, SMEs are also beginning to acknowledge the associated benefits of preventative security measures and as a result the market for cybersecurity will continue to grow.

### *Cybersecurity and Export Controls*

The Exports and Imports Permits Act (EIPA) is a crucial piece of legislation in Canada that governs the movement of goods and technologies both within and outside the country<sup>23</sup>. Its primary objective is to ensure that Canadian companies are compliant with international agreements, national security measures, and foreign policy objectives. By effectively regulating the export and import processes, the EIPA plays a vital role in safeguarding Canada's interests and maintaining a secure and prosperous economy. The EIPA establishes a permit system that details which items are subject to receive permit approval before engaging in export activity – these items are listed within the Export Controls Guide (ECG).

The ECG does not specifically mention cybersecurity products. However, it is important to note that Category 5 – Part 2 of the Export Control Guide Canada is dedicated to Information Security<sup>24</sup>. This category encompasses a wide range of items related to information security, including cryptographic systems, secure communication systems, intrusion detection systems, and software tools for information security. Additionally, it covers technologies used for information security testing, such as penetration testing tools and vulnerability assessment tools. It is essential for Canadian cybersecurity firms to determine whether they are subject to these regulations and to ensure that they do not face any penalties for non-compliance.

20. [2023 was a big year for cybercrime, World Economic Forum, 2024](#)

21. [Ibid.](#)

22. [Cybersecurity Market Size & Share Analysis - Growth Trends & Forecasts \(2024 - 2029\), Mordor Intelligence](#)

23. [Export and Import Permits Act, Government of Canada](#)

24. [A Guide to Canada's Export Control List, Government of Canada](#)

# In-Sec-M Member Coverages

In 2024, In-Sec-M conducted a survey to gather information about Canadian cybersecurity businesses including capabilities and sector of focus. The survey was distributed to In-Sec-M's members as well as non-member companies across Canada.

---

## Sectors of Activities

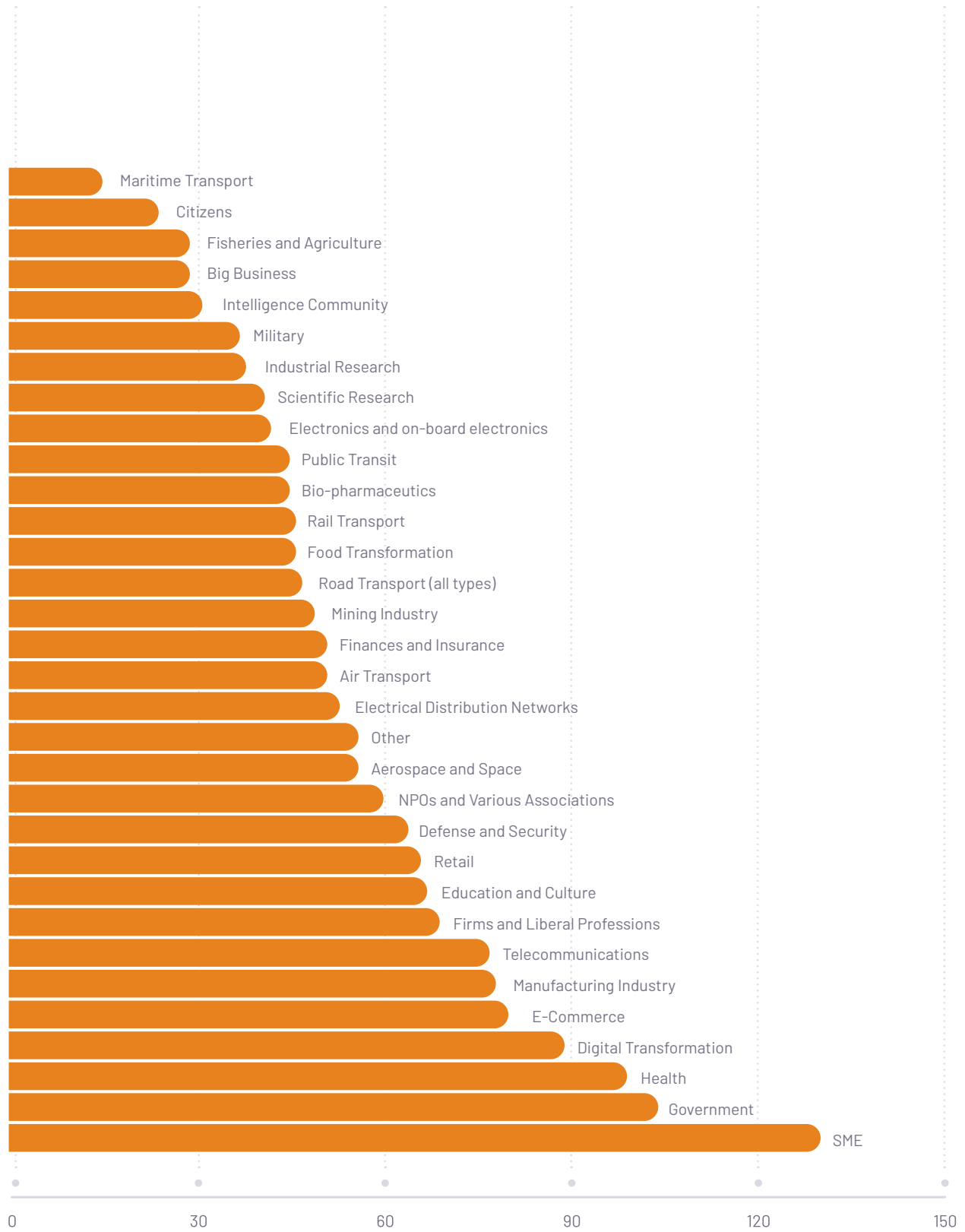
Out of the 148 participants, a significant majority of 130 (88%) indicated that SMEs formed a key focus area for their operations. This finding highlights the sustained demand for cybersecurity products and services within the SME sector and underscores the strong capabilities of In-Sec-M members in meeting these needs.

The public sector emerged as another significant customer base, with over 70% of respondents indicating their provision of cybersecurity products and/or services to governments. Additionally, the Health, Digital Transformation, E-commerce, and Manufacturing industries were identified as prominent sectors by a majority of respondents.

However, the survey results also revealed relatively low attention given to Maritime Transportation, Citizens, Fisheries, and Agriculture. These sectors garnered less interest among the respondents in terms of their business focus.



Figure 4 Main Sectors of Activities, In-Sec-M Canadian Cybersecurity Ecosystem Survey, 2024



**Table 4 Main Sectors of Activities, In-Sec-M Canadian Cybersecurity Ecosystem Survey, 2024**

Main sectors of activities	Number of Survey Response Selections	% of Total Respondents
SME	130	88%
Government	104	70%
Health	99	67%
Digital transformation	89	60%
E-commerce	80	54%
Manufacturing industry	78	53%
Telecommunications	77	52%
Firms and liberal professions	69	47%
Education and culture	67	45%
Retail	66	45%
Defense and security	64	43%
NPOs and various associations	60	41%
Aerospace and space	56	38%
Other	56	38%
Electrical distribution networks	53	36%
Air transport	51	34%
Finances and insurance	51	34%
Mining industry	49	33%
Road transport (all types)	47	32%
Food transformation	46	31%
Rail transport	46	31%
Biopharmaceutics	45	30%
Public transit	45	30%
Electronics and on-board electronics	42	28%
Scientific research	41	28%
Industrial research	38	26%
Military	37	25%
Intelligence Community	31	21%
Large Enterprise	29	20%
Fisheries and agriculture	29	20%
Citizens (Customers)	24	16%
Maritime transport	15	10%

## Market Coverage

The survey included questions about the market coverage<sup>25</sup> of the respondents. When examining the North, Central, and South American markets, it was observed that more than half of the survey respondents exported their products and/or services to the United States. Specifically, 31% (46 respondents) exported to Mexico and the Caribbean, while 24% (36 respondents) exported to Central and South America.

**Table 5 North, Central and South American Market Coverages, In-Sec-M Canadian Cybersecurity Ecosystem Survey, 2024**

Market	Number of Survey Response Selections	% of Total Respondents
United States	88	59%
Mexico and Caribbean/Antilles	46	31%
Central and South America	36	24%

Europe emerged as a strong market for In-Sec-M members. Nearly half of the respondents (72 respondents, 49%) stated that they exported their products and/or services to France. The United Kingdom was the second largest European market among the survey respondents, with 49 companies selecting it as a market. Other European markets mentioned included Italy, Spain, Benelux and Scandinavia.

**Table 6 Europe Market Coverages, In-Sec-M Canadian Cybersecurity Ecosystem Survey, 2024**

Market	Number of Survey Response Selections	Percentage of Total Respondents
Europe - France	72	49%
Europe - United Kingdom	49	33%
Europe - Benelux	38	26%
Europe - Spain	37	25%
Elsewhere in Europe	37	25%
Europe - Italy	35	24%
Europe - Scandinavia	30	20%

In addition to these regions, other international markets also received attention. It was found that 19% (28 respondents) of the survey respondents exported to Israel, while 18% (27 respondents) exported to markets in the Middle East. Africa and Asia were also significant markets, with 24% and 20% of respondents exporting to these regions, respectively.

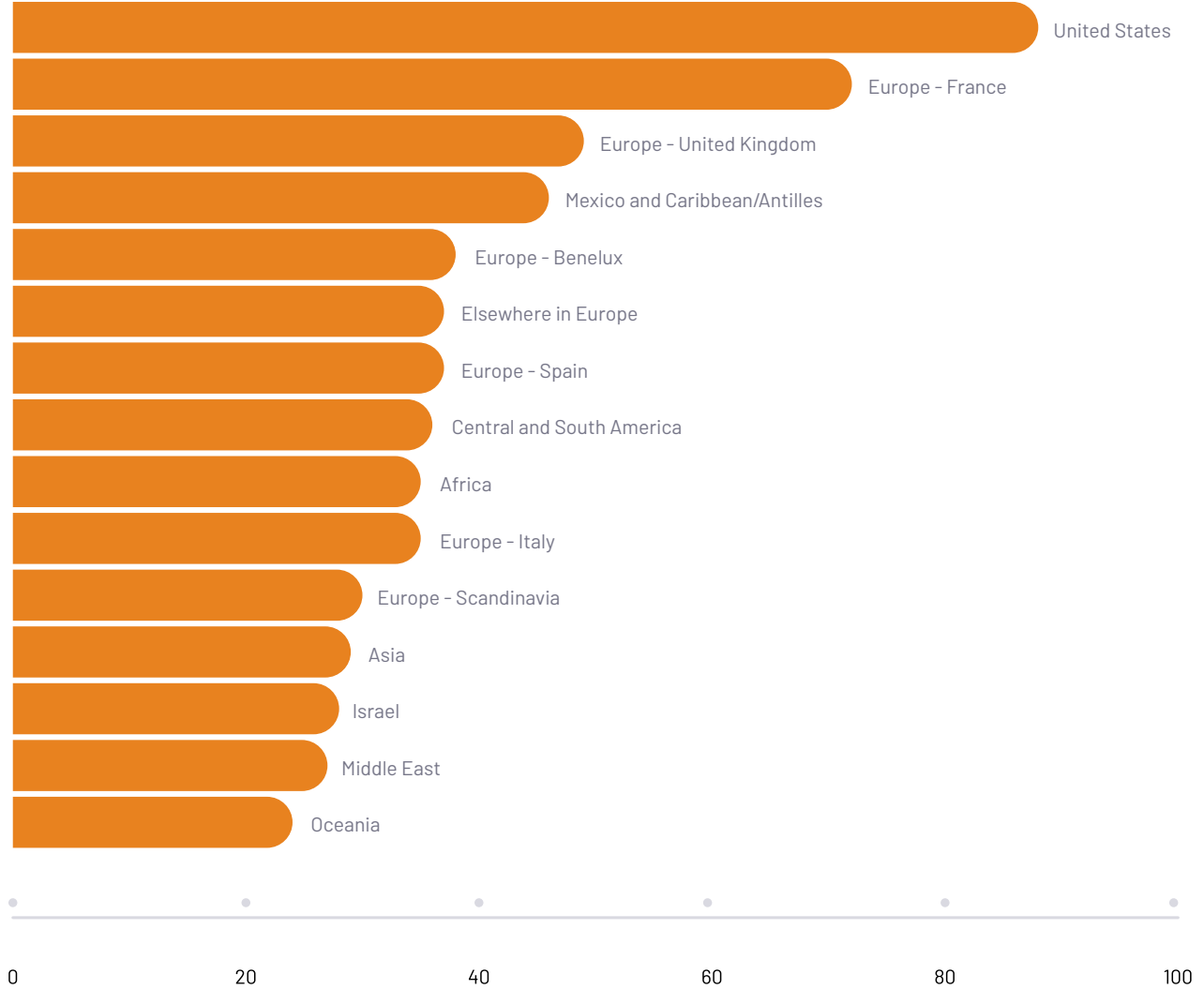
25. It is important to note that survey respondents have the option to select multiple answers for this survey question. Respondents were asked to indicate their market coverage. However, market coverage does not necessarily imply physical presence or location of the company in that market.

**Table 7 Other Market Coverages, In-Sec-M Canadian Cybersecurity Ecosystem Survey, 2024**

Market	Number of Survey Response Selections	% of Total Respondents
Africa	35	24%
Asia	29	20%
Israel	28	19%
Middle East	27	18%
Oceania	24	16%

The following chart presents the percentage of market coverage among survey respondents.

**Figure 5 Market Coverages, In-Sec-M Canadian Cybersecurity Ecosystem Survey, 2024**



# Target Market Analysis

The development of the international business strategy starts with the evaluation and selection of target markets. The following section presents the methodology and research insights from the selection and evaluation process.

## Methodology

Based on sector research, stakeholder interviews, In-Sec-M's past mission reports, and survey results from In-Sec-M's members, a comprehensive list of countries has been compiled to be considered for the Target Market Analysis. These countries have been mentioned in multiple information sources and are deemed potential target markets. The initial list includes:

- › **North, Central and South American Market:** Mexico and Brazil
- › **European Market:** United Kingdom, Germany, France, Benelux (Belgium, Netherlands, and Luxembourg), Spain, Italy, and Switzerland
- › **Asian Market:** Singapore

It is important to note that while other countries and regions were mentioned in the sources, they were not considered due to a general lack of information and comparative data. These countries included India, Malaysia, Japan, and South Africa. This does not imply that they do not present opportunities for Canadian exports of cybersecurity products and services. The rapidly growing cybersecurity sector may lead to emerging opportunities in these countries in the future. Therefore, it is recommended for In-Sec-M and its members to continue monitoring export opportunities to these countries and regions.

It should be noted that the purpose of this international strategy is to diversify Canada's export of cybersecurity products and services. As a result, the United States, which is Canada's largest trading partner in this sector, was excluded from the selection of potential target markets. However, the data and many stakeholders highlighted opportunities to strengthen trading relationships with the U.S., leveraging the existing strong ties between the two countries. Therefore, although the U.S. is not included in this analysis, it is recommended that Canadian companies and In-Sec-M continue to explore and capture new international business opportunities between Canada and the U.S.



The shortlisted countries and regions were assessed to understand their market characteristics and opportunities for the future Canadian exports. The analysis focused on the following areas:

- › **Market Size and Growth:** Information on the potential target market's economic size, size of their ICT and/or cybersecurity sector, and any major cybersecurity-related initiatives.
- › **Market Entry:** Assessment of the ease and cost of doing business, including ways of market entry and the cost of market entry in potential target markets.
- › **Market Competition:** Evaluation of competition in potential markets to identify opportunities for Canadian exports. Higher competition may result in fewer opportunities for new entrants.
- › **Opportunities:** Identification of specific target sectors and types of businesses in potential target markets that are actively seeking cybersecurity products and services. These opportunities can serve as market entry points for Canadian companies.
- › **Risks and Challenges:** Examination of potential risks for Canadian exports, including regulatory risks and political sensitivity around cybersecurity.
- › **Stakeholder Interview Insights:** Inclusion of additional insights gathered from stakeholder interviews.
- › **In-Sec-M Mission Insights:** Inclusion of additional insights gathered from In-Sec-M's past international missions.

## Assumptions and Limitations

The selection of target markets in this study is based on a combination of primary and secondary research sources.

Primary research involved stakeholder engagement and expert opinions from Deloitte. Secondary research included online research, past mission reports from In-Sec-M, and survey results. It is assumed that these sources provide a comprehensive overview of the potential target markets and their opportunities and challenges.

However, there may be limitations in certain cases where information is limited or missing. This could be due to incomplete primary research, such as interview request being declined by stakeholders, or limited information in secondary research. The following section highlights these limitations.



## Potential Target Markets

The information gathered for each of the ten potential target markets was aggregated. Key findings and summaries for each market are provided below.

### Mexico

#### MARKET SUMMARY

Mexico is the second largest economy in Latin America and ranks 15th worldwide. Despite challenges such as the 2019 oil crisis and the 2020 global recession caused by COVID-19, Mexico has shown stable economic growth with a recovery trend after the pandemic. In 2022 and 2023, Mexico's economic growth exceeded 3%. The country has experienced significant digitization growth, making it more vulnerable to cyber-attacks. Mexico is the most attacked country in Latin America by ransomware and saw a 93% increase in malware attacks in 2020. The Mexican financial sector, in particular, has been targeted, with 56% of malware attacks and 47% of phishing attacks.<sup>26</sup>

In the last In-Sec-M survey to cybersecurity businesses, out of 148 respondents, 46 (31%) of them export cybersecurity products and services to Mexico and Caribbean/Antilles.

#### MARKET ENTRY AND COMPETITION

Mexican business culture values face-to-face communication for assessing potential partners' character, trustworthiness, and compatibility. The Canada-United States-Mexico Agreement (CUSMA) strengthens Canada's economic ties with the United States and Mexico. In the past five years, Mexican companies have become significant players in the IT industry, ranking among the top 20 service providers globally. The Mexican cybersecurity industry focuses on Data Security, Governance and Compliance, Cloud Security, Detection and Prevention, as well as Incident Response and Forensics. Major cybersecurity companies in Mexico include Scitum, Arame, and KUI Networks.<sup>27</sup>

#### OPPORTUNITIES

The banking and finance sector in Mexico presents opportunities for cybersecurity products and services. Financial institutions are investing more in technology and innovation to prevent and respond to fraudulent activities. In 2021, Mexican banks increased their investment in technology and innovation by 20.8% compared to 2020 and 35% compared to pre-pandemic times.<sup>28</sup>

#### RISKS AND CHALLENGES

A significant challenge in the ICT sector in Mexico is the influence of monopolistic entities that impede necessary reforms. Perceived corruption within government procurement in the ICT sector at the federal, state, and municipal levels is also a barrier for foreign firms. Mexico lacks a specific law focused on cybersecurity, although there are regulations on financial crimes, information security, and technology-related crimes.<sup>29 30</sup>

#### STAKEHOLDER INTERVIEW INSIGHTS

Stakeholder interviews confirm that Mexico presents a significant opportunity due to its vulnerability to cybersecurity attacks in recent years. Mexican enterprises are actively seeking cybersecurity services and solutions to address and prevent further attacks.

26. Cybersecurity Overview in Mexico, Israel's Economic Office to Mexico

27. Ibid.

28. Ibid.

29. Ibid.

30. [The Development of the ICT Landscape in Mexico: Cybersecurity and Opportunities for Investment \(csis.org\)](https://www.csis.org/analysis/the-development-of-the-ict-landscape-in-mexico-cybersecurity-and-opportunities-for-investment)

## IN-SEC-M MISSION INSIGHTS

The international mission to Mexico conducted in March 2024 revealed that:

- › The Mexican cybersecurity ecosystem is still in its early stages of development, with low maturity in terms of cybersecurity structures. While there is a clear need for cybersecurity services, Mexican organizations have not made it a priority to invest in this area.
- › The presence of well-established U.S. cybersecurity companies in Mexico poses a challenge for Canadian providers. These U.S. companies have already acquired a significant market share in Mexico, making it difficult for Canadian companies to penetrate the market.
- › There is a difference in corporate culture between Canada and Mexico, with the latter requiring a considerable investment of time for companies wishing to enter the market. This is in contrast to Canada, the United States, and some major Western markets where entry processes may be smoother and faster.
- › Mexican structures show relatively low interest in Canadian cybersecurity expertise. However, this difficulty can be overcome through the long-term efforts of Canadian representatives on the ground, building relationships and showcasing the value of Canadian expertise.
- › Mexican SMEs are in the early stages of their digital transformation journey and will face significant challenges in upgrading their cybersecurity capabilities in the coming years. This presents a potential market opportunity for Canadian companies that can offer products and services tailored to the needs and price points of this market.
- › Technological partnerships have been an efficient way to enter foreign markets, but in Mexico, the cybersecurity innovation ecosystem is already dominated by American structures. This suggests that Canadian companies may need to explore alternative strategies to establish a foothold in the Mexican market.

## Brazil

### MARKET SUMMARY

Brazil, as the world's eighth largest economy and the most populous state in South America, has made significant advancements in domestic digitization. The country has the fifth largest internet user base globally and is a leading country in South America in terms of ICT usage. Brazil's National Cybersecurity Strategy (E-Ciber) outlines strategic actions to enhance cyber resilience and international cooperation. The country remains committed to multilateral solutions and actively participates in joint cyber resilience events and exercises.<sup>31</sup>

### MARKET ENTRY AND COMPETITION

Establishing a local office or partnering with a trusted local representative is crucial for success in the Brazilian market. Face-to-face communication and local support are highly valued by Brazilian companies. The telecommunications market in Brazil is competitive and prefers working with local suppliers. Canadian companies should consider long-term commitments and partnerships to navigate Brazil's complex legal and regulatory system.<sup>32</sup>

### OPPORTUNITIES

Opportunities exist in the fintech sector, with Brazilian banks investing in new technologies to support fintech services. There is demand for cybersecurity, mobile and online banking, artificial intelligence, data analytics, IoT, blockchain, and cloud services. The potential revenue generated by financial technology companies in Brazil is estimated to reach £24 billion (equivalent to approximately \$41 billion in Canadian dollar in 2024 value), in the next decade.<sup>33</sup>

31. [Brazil: EU Cyber Direct](#)

32. [Information and Communications Technologies \(ICT\) market in Brazil \(tradecommissioner.gc.ca\)](#)

33. [Exporting guide to Brazil - great.gov.uk - great.gov.uk](#)

## RISKS AND CHALLENGES

For clients that are federal and state law enforcement agencies in Brazil, their importation requirements for cybersecurity products and services involve obtaining prior importation licenses and the International Importation Certificate (CII) from the Brazilian Army. The current administration in Brazil has not prioritized cyber strategy, which may impact the development of the cybersecurity industry.<sup>34 35</sup>

## STAKEHOLDER INTERVIEW INSIGHTS

No additional interview insights available.

## IN-SEC-M MISSION INSIGHTS

The international mission to Brazil conducted in February 2024 revealed that:

- › The consulting market in Brazil is already well serviced by both Brazilian companies and major international accounts. This indicates that consulting companies may face strong competition in the market.
- › The implementation of the LGPD (Brazil's data protection law) in 2020 has created a demand for compliance support services. Lawyers specializing in this sector may be interested in partnering with foreign cybersecurity experts who can provide advanced cybersecurity solutions that meet the specific requirements of the LGPD.
- › Brazil has a large market for the protection of personal information, driven in part by the measures taken to meet physical security needs. For example, biometrics and ID cards are collected in condominiums and office buildings.
- › The healthcare sector in Brazil lags behind in terms of cybersecurity, despite a significant number of Brazilians having private insurance. The retail sector also represents a substantial market opportunity due to Brazil's large population and growing economy.
- › Brazil's banking sector has embraced digital transformation and is at the forefront of technology. There is interest from major banking institutions in working with Canadian companies and acquiring Canadian solutions, particularly in cybersecurity solutions based on AI or quantum expertise. The telecommunications sector also presents potential opportunities.
- › The mining and oil sectors in the Rio region may be of interest to IoT solution providers. In the defense sector, having a local partner is recommended for responding to government tenders, and the two cyber companies acquired by Embraer could be essential for entering this market.
- › There is a demand for cybersecurity training and awareness services across all sectors, driven by advanced social engineering techniques in Brazil. The banking sector, in particular, is concerned about the amount of bank fraud in the country.
- › Technological partnerships, such as through the Canada-Brazil Calls for Proposals (EMBRAPII), can be a strategy for market penetration, especially in sectors where current service providers have cutting-edge expertise.
- › Selling solutions directly from Canada is possible if comparable solutions are not available in Brazil. However, it is generally preferable to find a distributor, sales representative, or legal representative in Brazil due to factors such as legal responsibilities, facilitating payments, and the need to communicate in Portuguese for business transactions.

34. [Brazil - Safety and Security \(trade.gov\)](#)

35. [Brazil's Cyber Strategy Under Lula: Not a Priority, but Progress Is Possible - Carnegie Endowment for International Peace](#)

# United Kingdom

## MARKET SUMMARY

The cybersecurity market in the United Kingdom (UK) has experienced significant growth, with total annual revenue reaching £10.1 billion in 2021 (equivalent to approximately \$17 billion in Canadian dollar in 2024 value), a 14% increase from the previous year. There are currently 1,838 active firms providing cybersecurity products and services in the UK. The UK Government has actively supported the growth of the cybersecurity sector through various initiatives, including direct investment, skills and profession support, and investment in regions and clusters.<sup>36</sup>

In the last In-Sec-M survey to cybersecurity businesses, out of 148 respondents, 49 (33%) of them export cybersecurity products and services to the United Kingdom.

## MARKET ENTRY AND COMPETITION

Companies looking to enter the UK cybersecurity market need to be knowledgeable about data sourcing and storage regulations, which will be a focus in trade agreement negotiations. The UK market is highly competitive, with a large number of firms operating in the cybersecurity sector.<sup>37,38</sup>

## OPPORTUNITIES

**Large Enterprises:** The majority of the cybersecurity market in the UK revolves around large commercial enterprises, particularly in the financial services, utilities, and transportation sectors.

**Public Sector:** The central and local governments in the UK are investing heavily in securing sensitive data in health-care and education, as well as in online services such as universal credit.

**Defense and Security (D&S):** The D&S market in the UK focuses on securing national secrets and involves security and intelligence agencies, as well as the Ministry of Defence (MoD).

**SMEs:** Many SMEs in the UK lack sufficient cybersecurity measures, making them vulnerable to cyber threats. The government is encouraging SMEs to adopt basic cyber hygiene standards, and some public procurement contracts require minimum cybersecurity requirements for supply chains.<sup>39</sup>

## RISKS AND CHALLENGES

While the UK IT security market is open to North American companies, there are specific UK regulations that companies should be aware of, including the Data Protection Act, Privacy and Electronic Communication regulations, Freedom of Information Act, and Environmental Information regulations. Compliance with these regulations is essential for operating in the UK market.<sup>40</sup>

## STAKEHOLDER INTERVIEW INSIGHTS

Stakeholder interview mentioned that the UK has traditionally been a favourable market for Canadian enterprises, presenting opportunities for collaboration and expansion.

## IN-SEC-M MISSION INSIGHTS

The international mission to the United Kingdom conducted in February 2024 revealed that:

- › The UK is known for heavily investing in innovation, including the cybersecurity industry. Incubators and accelerators in the UK support the development of cutting-edge solutions. The government has also supported the growth of incubators through public-private initiatives.
- › The UK attracts high-talent workers from around the world and is home to many venture capitalists (VCs) and sources of private investment. The renowned post-secondary education system and competitive market make the UK an attractive destination for cybersecurity companies.

36. [Market insights for exporting cyber security to United Kingdom | Market search tool \(business.gov.au\)](#)

37. [Market insights for exporting cyber security to United Kingdom | Market search tool \(business.gov.au\)](#)

38. [Cyber security sectoral analysis 2022 - GOV.UK \(www.gov.uk\)](#)

39. [export.gov](#)

40. [export.gov](#)

- › Recognized cybersecurity hubs in the UK are concentrated in London, Belfast, Manchester, and Cheltenham. The Belfast cluster, which was originally built around the Queen's University Belfast, has positioned itself as a pioneer in cybersecurity. It houses world-class research, attracts multinational companies, and offers accelerated workforce training programs. The Belfast ecosystem aims to position itself as a gateway to the European and British markets, similar to Luxembourg for Europe and Singapore for Asia. The low corporate tax rates and presence of major multinational cyber divisions have attracted companies to set up headquarters in Belfast. However, there is a lack of SMEs in the local economic fabric.
- › Canadian companies have opportunities in the UK cybersecurity sector due to the fact that Canada is part of the Five Eyes intelligence alliance. The defence sector, including organizations like DSTL, is interested in targeted Canadian solutions. Other sub-sectors of interest include insurance and critical infrastructure protection, such as finance and nuclear power plants.
- › In the UK, bidding on central government contracts often requires obtaining the Cyber Essentials or Cyber Essentials Plus certification. This certification contributes to the cyber resilience of the UK economy and supports the financial health of the local cybersecurity industry. The National Cyber Security Centre plays a crucial role in this initiative.

## Germany

### MARKET SUMMARY

The German cybersecurity market is one of the fastest growing in Europe, second only to France. In 2021, IT security spending in Germany reached €6.2 billion (equivalent to approximately \$9.1 billion in Canadian dollar in 2024 value), a significant increase of 9.7% compared to the previous year. This growth is driven by the country's focus on cybersecurity as a governmental top priority, with the publication of multiple national cybersecurity strategies since 2011. Germany's latest strategy, published in September 2021, builds upon previous ones and emphasizes the importance of cybersecurity in the digital landscape.<sup>41</sup>

Germany is a federal republic, with considerable autonomy given to its 16 federal states (Länders). This has resulted in uneven distribution of cybersecurity demand, know-how, and market opportunities across the country. Some states, such as Bavaria, have been more proactive in the field of cybersecurity than others. Therefore, companies looking to enter the German market need to consider these regional variations.

### MARKET ENTRY AND COMPETITION

German firms tend to be conservative and are often hesitant to trust unknown foreign companies. In some cases, having a local presence is legally required and generally desirable to submit bids or join local cybersecurity communities. Furthermore, Germany has ambitions for technological independence, and the cybersecurity community, particularly in research and development, recognizes the need for domestic ICT solutions. This focus on home-grown startups may reduce opportunities for foreign firms and technologies.

To overcome barriers of trust and conservatism, it is recommended to partner with a German stakeholder, such as a prime contractor, system integrator, or value-added reseller. These partners can provide customer support in German and comply with availability requirements. Additionally, there is an increasing number of specialized German start-ups in the cybersecurity field, intensifying local competition.<sup>42</sup>

### OPPORTUNITIES

There are two key opportunities in the German cybersecurity market:

**Cybersecurity for the Mittelstand (SMEs):** Germany's economic fabric relies heavily on SMEs, also known as the Mittelstand. These SMEs, often global leaders in their respective fields, may have been reluctant to invest in new tools and policies to enhance the security of their ICT systems. Protecting their systems is a top priority for business continuity and to remain competitive and innovative. Network security, compliance, identity and access management (IAM), and security as a service (SecaaS) are identified as top priorities for SMEs to ward off cyber threats.

41. Exporting to the EU - A guide for Canadian cybersecurity companies, Canada Trade Commissioner Service

42. Ibid.

Digitalization of services and the public sector: The digitalization of services and the public sector is a key agenda item in German politics. Although progress has been slow, the COVID-19 pandemic highlighted the country's digital deficits, leading to new initiatives. This presents significant market opportunities for cybersecurity-related hardware and software.<sup>43</sup>

## RISKS AND CHALLENGES

While Germany offers opportunities for niche, high-quality technology providers in the industrial sector, it is important to note that the regulatory environment is rapidly evolving. Changes can occur suddenly, and compliance with regulations is crucial. The IT-Security Act 1.0 and 2.0 serve as Germany's legal framework for implementing the EU's NIS Directive. The Act 2.0, introduced in May 2018, increased momentum in the German cybersecurity sector, particularly for critical infrastructure. It mandates companies involved in critical infrastructure to take appropriate security measures and imposes significant fines for non-compliance. The Act also grants more authority to the Federal Office for Information Security (BSI).<sup>44</sup>

## STAKEHOLDER INTERVIEW INSIGHTS

No additional insights are provided in the stakeholder interview for Germany.

## IN-SEC-M MISSION INSIGHTS

The international mission to Germany conducted in October 2023 revealed that:

- › The German cybersecurity ecosystem is complex and fragmented, lacking a clear and centralized direction. Private companies have a lot of autonomy and influence in the market.
- › The German cybersecurity ecosystem is described as highly sophisticated and technically advanced. Canadian companies entering this market should be prepared to face fierce competition from highly competent local players.
- › The general business mindset in Germany is often compared to that of Americans – direct and with little procrastination. This can influence business interactions and decision-making processes.
- › Language can be a significant barrier for Canadian exporting companies, especially when targeting SMEs. It is crucial for non-German-speaking companies to have employees who can speak and write German to effectively navigate the market.
- › IT-SA is a significant cybersecurity event in Europe, providing insights into the size of the German cybersecurity market, which is the largest in Europe by a significant margin.

## France

### MARKET SUMMARY

The French cybersecurity market is dynamic and mature, generating €13.4 billion in revenue in 2021 (equivalent to approximately \$19.8 billion in Canadian dollar in 2024 value). The market experienced a growth rate of 6.4% between 2019 and 2020 and employed 69,200 people. Foreign players, primarily from Israel and the United States, accounted for 30% to 40% of the cybersecurity market, including services. The French government has established a strong support framework to stimulate the development of the cybersecurity sector and position French actors as global leaders. France adopted a key strategy in 2011 to become a world leader in cyber defense, safeguard national sovereignty, strengthen critical infrastructure cybersecurity, and ensure security in cyberspace. The market is expected to continue growing at a rate of approximately 6% between 2021 and 2026, with increased spending on cybersecurity driven by compliance with GDPR standards.<sup>45</sup>

In the last In-Sec-M survey to cybersecurity businesses, out of 148 respondents, 72 (49%) of them export cybersecurity products and services to France.

43. Exporting to the EU - A guide for Canadian cybersecurity companies, Canada Trade Commissioner Service

44. Ibid.

45. Ibid.

## MARKET ENTRY AND COMPETITION

To enter the French market, it is crucial to network and build personal relationships. Active professional communities and trade associations can help raise awareness of your products/services among French customers. Participating in events, competitions, innovation clusters, start-up incubators, and flagship events like the InCyber Forum (previously known as International Cybersecurity Forum, or FIC) and Les Assises de la Cybersécurité can serve as entry points into the French cybersecurity ecosystem. Selecting a local distributor or value-added reseller (VAR) with relevant networks, such as Orange Cyberdéfense, Sopra Steria, Atos, or Capegimi, is recommended. The market remains fragmented, with strategic partnerships and collaborations being formed to increase market presence and develop new products and services.<sup>46</sup>

## OPPORTUNITIES

The French cybersecurity market offers opportunities in various sectors:

- › Banking, Finance, and Insurance: This sector accounts for 17% of the market.
- › Defense and Security: Approximately 12% of the market is focused on defense and security.
- › Industry: The industrial sector represents 11% of the market.
- › Public Sector: Around 10% of the market is dedicated to the public sector.
- › IT-Digital: This sector accounts for 9% of the market.
- › Aerospace: Approximately 7% of the market is focused on the aerospace industry.
- › Transport: The transport sector represents 6% of the market.
- › Energy and Environment: Around 6% of the market is dedicated to energy and environmental sectors.

The large number of existing and potential cybersecurity customers, particularly SMEs, presents an opportunity for entry-level cybersecurity solutions. This trend has been accelerated by the COVID-19 pandemic.<sup>47</sup>

## RISKS AND CHALLENGES

The French cybersecurity market, although offering opportunities, is highly regulated. Compliance with regulations is crucial, and staying updated with the evolving regulatory environment is essential.

## STAKEHOLDER INTERVIEW INSIGHTS

Insights from interviews suggest that France is considered a viable market due to its historical reputation as a trustworthy market and the presence of the French diaspora living in Canada. These factors can facilitate market entry and establish business relationships.

## IN-SEC-M MISSION INSIGHTS

The international missions to France conducted in 2023 and 2024 revealed that:

- › In-Sec-M has extensive knowledge and experience in the French cybersecurity market, with established networks and high-level contacts within the ecosystem. These networks include industrialists, associations, academics, and government and security authorities.
- › Accessing the French market for Canadian companies selling cybersecurity products and services could be challenging as some public sector organizations and large industrial groups tend to prioritize domestic solutions, exhibiting a certain level of national preference. The French state will only consider foreign solutions if equivalent French options are not available.
- › Exporters may face tough competition from French cybersecurity companies in terms of technological competence. French companies are known for their expertise and innovation in the field, making it a competitive market for international players.
- › France operates on a network-based business culture. Conducting business in France can be complex, frustrating, and unsuccessful for those who do not have established connections within French networks. Building and leveraging these networks is crucial for success.

46. Exporting to the EU - A guide for Canadian cybersecurity companies, Canada Trade Commissioner Service

47. Ibid.



- › In-Sec-M has signed a partnership agreement with the Cyber Pole of Excellence during their visit to Brittany. This partnership provides Canadian companies privileged access to key players in the French ecosystem.



## Benelux

(Belgium, Netherlands, and Luxembourg)

### MARKET SUMMARY

The Benelux region, consisting of Belgium, Netherlands, and Luxembourg, offers potential in the cybersecurity market. Luxembourg ranks 11th globally in the Global Cybersecurity Index (GCI), highlighting its commitment to cybersecurity and best practices in technical and capacity-building fields. The Netherlands is marketed as the digital gateway to Europe and has a strong internet economy<sup>48</sup>. Belgium recognizes cyber threats as one of the most important risk clusters and has implemented a Cyber Security Strategy.<sup>49</sup>

In the last In-Sec-M survey to cybersecurity businesses, out of 148 respondents, 38 (26%) of them export cybersecurity products and services to Benelux.

### MARKET ENTRY AND COMPETITION

In the Netherlands, foreign companies, particularly those from the U.S., often establish themselves in the United Kingdom before entering the Dutch market. The Dutch market benefits from being early adopters of new technologies.<sup>50</sup> The research did not identify any distinct market entry requirements or specific recommendations for entering Belgium and Luxembourg. The market entry practices for these two countries are comparable to other European markets.

### OPPORTUNITIES

In Belgium, there is an openness to external actors in the cybersecurity and data protection sector. Belgian companies tend to outsource their cybersecurity needs to other EU counterparts, creating opportunities for external providers. There is also a need for prepared SMEs and a lack of qualified staff.<sup>51</sup> Brussels is also home to many international organizations, which create opportunities for a pan-European approach to market entry.

Luxembourg's cybersecurity supply is characterized by the involvement of traditional IT companies and companies from the banking, financial services, and insurance (BFSI) sector. Small companies play a significant role, and market opportunities for emerging EU solutions remain open.<sup>52</sup>

The Netherlands presents similar opportunities to other advanced and highly digitalized countries. The Dutch market is receptive to new technologies, making it an attractive target for foreign companies.<sup>53</sup>

### RISKS AND CHALLENGES

The Benelux countries have distinct economic identities and business cultures. However, they have strong rule of law, intellectual property rights protection, and transparent contract enforcement, providing a favourable business environment.

### STAKEHOLDER INTERVIEW INSIGHTS

Insights from interviews suggest that the Netherlands has traditionally been a favourable market for Canadian enterprises. This historical reputation can facilitate market entry and establish business relationships.

48. [Netherlands - Cyber Security \(trade.gov\)](#)

49. The European Cybersecurity Market, Enterprise Ireland

50. [Netherlands - Cyber Security \(trade.gov\)](#)

51. [Belgium - Market Challenges \(trade.gov\)](#)

52. Luxembourg Cybersecurity Ecosystem, Cybersecurity Luxembourg

53. [Netherlands - Cyber Security \(trade.gov\)](#)

## IN-SEC-M MISSION INSIGHTS

The international missions to Benelux conducted in October 2023 revealed that:

- › In future years in Netherlands, it might be worthwhile to work on inviting Canadian industry representatives to speak at the One Conference (on invitation only), which is a good forum for demonstrating Canadian industry's excellence to a select group of representatives.
- › In Luxembourg, the government has chosen to focus on a strong digital economy and the few strategic, cutting-edge sectors that go hand in hand with it, in an environment where all players act in a concerted, agile manner. The territory is small, it is relatively easy to connect with all the relevant players in one's sector of activity, and Luxembourg society has the means to match its ambitions. Luxembourg "manage" cybersecurity in an agile way; the Ministry of the Economy is in direct contact with the House of Cybersecurity, which is the first point of contact with industry, and the Cybersecurity Board coordinates the players from the various ministries.
- › In addition to the financial sector, which is of great interest to Canadian solution and service providers targeting this vertical in particular - especially with the DORA regulation - Luxembourg is an attractive gateway to the European market, and openly positions itself as such. The support offered to foreign companies is particularly important and of high quality.
- › Luxembourg cybersecurity companies have developed their offer for large customers, such as banks, while the need for Luxembourg and European SMEs is increasing, and Canadian cybersecurity companies have developed expertise in solutions and services adapted to this clientele.
- › The Interdisciplinary Centre for Security, Reliability and Trust at the University of Luxembourg has launched its CyberHub, which will benefit from 3.5 M euros per year, in November 2023. They have an acceleration program; offer soft-landing to companies wishing to access the European market; and technical support to companies establishing their headquarters in Luxembourg.
- › Regarding Belgium, specific organizations offer excellent opportunities to meet major buyers and develop potential technological partnerships with a view to penetrating the European market.
- › Apart from bilateral relations with Belgium, and the Belgian market more specifically, forging strategic partnerships with pan-European organizations headquartered in Brussels to help ensure that the voice of Canadian SMEs is heard on standardization committees, for example, could benefit Canadian industry in terms of interoperability, influence on future demand, and privileged information to adapt the supply accordingly.
- › Privileged access to potential European buyers, investors and partners, through alliances with targeted pan-European organizations, can also be a strategy for growing Canadian exports and maintaining the excellence of its innovation ecosystem.
- › There is a need to build stronger relationships between Canada's joint delegation to NATO and Canadian industry to contribute more effectively to allies' cyber defenses.

## Spain

### MARKET SUMMARY

The Spanish market offers significant opportunities for cybersecurity products and services due to the country's dynamic business landscape and ongoing digital transformation. The Next Generation EU program has injected substantial investment into the Spanish economy, with a focus on digitalization through the National Recovery and Resilience Plan. The plan allocates a significant portion of its budget to digital transformation, including cybersecurity initiatives. Spain's ICT sector is highly advanced, with extensive investments in infrastructure and connectivity.<sup>54</sup>

In the last In-Sec-M survey to cybersecurity businesses, out of 148 respondents, 37 (25%) of them export cybersecurity products and services to Spain.

54. [Information and Communications Technologies \(ICT\) market in Spain \(tradecommissioner.gc.ca\)](https://tradecommissioner.gc.ca)

## MARKET ENTRY AND COMPETITION

The Spanish government has implemented measures to attract foreign firms and investments, easing regulations and providing incentives. Face-to-face meetings and personal relationships are highly valued in the Spanish business culture, making it important to establish direct contact with local representatives. Proficiency in the Spanish language is recommended, as English fluency among local managers is relatively low. Major international companies, including IBM, Microsoft, HP, Google Cloud, and Amazon, have chosen Spain for research and development centers and data centers.<sup>55 56 57</sup>

## OPPORTUNITIES

No specific sectors are identified in the research.

## RISKS AND CHALLENGES

Spain has a comprehensive legal framework for cybersecurity, including data protection laws and legislation to protect critical infrastructure and electronic communications. Compliance with these regulations is essential for businesses operating in the Spanish market.

## STAKEHOLDER INTERVIEW INSIGHTS

No additional insights from interviews are provided.

## IN-SEC-M MISSION INSIGHTS

The travel to Spain in February 2024 for the purpose of attending a conference (MWC Barcelona) revealed that:

- › The MWC Barcelona is a significant event that brings together leading players in the telecommunications sector from around the world. It provides an opportunity for organizations like In-Sec-M to identify key players and establish connections. Numerous countries have pavilions at the event.

## Italy

### MARKET SUMMARY

The cybersecurity market in Italy has experienced significant growth, with a market value of \$2.1 billion USD in 2022 (equivalent to approximately \$2.9 billion in Canadian dollar in 2024 value), representing an 18% increase from the previous year. The Italian government has recognized the importance of cybersecurity and has implemented strategies to facilitate investment in R&D and increase digital literacy levels. Large companies are driving the cybersecurity market, with the financial/banking and utility sectors being the main end-users. However, many SMEs are still unprepared to face increasing threats.<sup>58</sup>

In the last In-Sec-M survey to cybersecurity businesses, out of 148 respondents, 35 (24%) of them export cybersecurity products and services to Italy.

### MARKET ENTRY AND COMPETITION

Companies entering the Italian market should ensure that their distribution, franchising, and agency arrangements comply with EU and Italian laws. Many foreign firms have established their own sales organizations in Italy, while others work with specialized importers or sales agents. It is common for well-established Italian firms to prefer exclusive arrangements.<sup>59</sup>

55. [Information and Communications Technologies \(ICT\) market in Spain \(wedc.org\)](https://wedc.org)

56. [Spain: Cybersecurity | Insights | DataGuidance](https://dataguidance.com)

57. [Spain - Market Entry Strategy \(trade.gov\)](https://trade.gov)

58. The Italian Cyber Security Market 2019, Ibs Italia

59. [Italy - Cybersecurity \(trade.gov\)](https://trade.gov)

## OPPORTUNITIES

Italy is an interesting market for Canada in the cybersecurity field, with potential for collaboration and synergy between the two countries. Disruptive innovations and digital infrastructures, such as cloud computing, security and privacy incident management, IoTs, and big data, present opportunities for collaboration. Key sectors for cybersecurity solutions include government, defense, energy, media and technology, transportation, finance, and automotive.<sup>60</sup>

## RISKS AND CHALLENGES

No risks or challenges identified.

## STAKEHOLDER INTERVIEW INSIGHTS

No additional insights from interviews are provided.

## IN-SEC-M MISSION INSIGHTS

The international mission to Italy conducted in November 2023 revealed that:

- › In-Sec-M's presence at Cybertech Europe facilitated direct exchanges with cybersecurity managers of major Italian industrial groups, fostering connections between European customers and Canadian solution providers. This event attracted international delegations and companies who are interested in expanding their markets in Italy and Europe.
- › Italy is actively seeking cutting-edge technological solutions in cybersecurity, but budgetary considerations remain a priority. Canadian exporters entering this market should take this into account when positioning their offerings.
- › There is a strong interest in Italy for Canadian expertise in Quantum Key Distribution (QKD). This presents an opportunity for Canadian exporters to cater to this demand.

# Switzerland

## MARKET SUMMARY

Switzerland is known for its innovation, competitive companies, and excellent universities, making it a top performer in terms of innovation. The country has a well-established infrastructure, legal certainty, and a balanced political system. A national strategy for Switzerland's protection against cyber risks was developed in 2012, providing a framework for addressing cyber threats more efficiently. Swiss companies are increasingly turning to managed security services due to the shortage of skilled workers in the security sector and the fast-paced innovation cycles in cyber defense.<sup>61</sup>

## MARKET ENTRY AND COMPETITION

Switzerland and Canada share common interests and values in the fight against cyber threats. Both countries have federal structures, multilingual societies, and open, market-oriented economies that encourage trade and investments. The strong bilateral trade between Switzerland and Canada is regulated by a Free Trade Agreement. Switzerland is among the top foreign investors in Canada, and economic cooperation between the two countries is significant. Switzerland's strengths, including its neutrality, legal certainty, and political stability, are also evident in the cybersecurity sector. Many international organizations choose Switzerland as the ideal location for their regional data centers.<sup>62</sup>

60. The Italian Cyber Security Market 2019, Ibs Italia

61. Cyber Security Market Study - Switzerland & Liechtenstein, Canada Trade Commissioner Services

62. Ibid.

## OPPORTUNITIES

Network security is a prominent field in Switzerland's cybersecurity market. The country is recognized as a center of expertise in Internet Governance, and a significant percentage of global internet activities are domiciled in Switzerland. The financial industry in Switzerland and Liechtenstein considers data and intellectual property as important corporate assets, creating opportunities in data security and processing. Other potential opportunities in the ICT sector include Swiss outsourcing of IT services, social computing, process optimization, and data security.<sup>63</sup>

## RISKS AND CHALLENGES

The Swiss legal system is conservative in implementing legislation specific to cybercrime. New legislation is introduced when conventional laws and mechanisms are unable to address cybercrime effectively.

## STAKEHOLDER INTERVIEW INSIGHTS

No additional insights from interviews are provided.

## IN-SEC-M MISSION INSIGHTS

The international mission to Switzerland conducted in October 2023 revealed that:

- › Switzerland has a huge market with high demand for state-of-the-art solutions for the cyber protection of networks, communications, and financial infrastructures. This presents opportunities for Canadian companies in the cybersecurity sector.
- › Regional economic development organizations show a strong interest in developing operational ties with Canada, particularly with Quebec due to the common language, French. Switzerland has programs in place to welcome and support foreign companies looking to establish a presence in the country.
- › Switzerland has a high demand for digital trust and digital identity technologies, providing opportunities for Canadian companies with cutting-edge expertise in these areas.
- › Switzerland prioritizes hosting innovative technology companies, and there are numerous support programs available for such companies. This demonstrates the country's commitment to fostering innovation and attracting foreign companies in the technology sector.
- › Many Swiss business mediator believe that Switzerland is an almost perfect entry point for Canadian companies looking to penetrate the European market as a whole. Switzerland's central geographical position, ability to conduct business in multiple languages (English, French, German, and Italian), economic stability, advantageous tax regime, and access to cutting-edge expertise make it an attractive destination for Canadian companies.

## Singapore

### MARKET SUMMARY

The cybersecurity market in Singapore is experiencing a significant increase in cyber threats, with a 145% YoY rise in cyberattacks in 2021. Ransomware and data theft are the most common types of attacks. The average cost of a cybersecurity breach in Singapore is the highest in the Asia-Pacific region. In 2022, the country has seen a rise in phishing, ransomware incidents, infected infrastructure, and website defacements. Singapore provides a favourable environment for the cybersecurity industry, with support from the government and a strong regulatory framework.<sup>64</sup>

63. Ibid.

64. Singapore Cybersecurity Market (trade.gov)

## MARKET ENTRY AND COMPETITION

The Cyber Security Agency (CSA) encourages the growth of the cybersecurity industry in Singapore by supporting advanced research and engineering capabilities. The CSA collaborates with the Economic Development Board (EDB) to leverage Singapore's pro-business climate and skilled workforce. Singapore is home to many top cybersecurity organizations, and the CSA, along with the Infocomm Media Development Authority, supports the establishment of a cybersecurity startup incubation hub.<sup>65</sup>

## OPPORTUNITIES

Singapore offers a large and competitive cybersecurity market, serving both local and multinational businesses. Key opportunities in the market include identity and access management, advanced endpoint, network, and cloud security, threat and vulnerability management, ICS and SCADA security, critical infrastructure information, artificial intelligence, data analytics and protection, IoTs, blockchain, distributed ledger technology, and quantum cryptography/computing.<sup>66</sup>

## RISKS AND CHALLENGES

The Singapore government provides a favourable environment for the cybersecurity industry, with support and relevant regulatory and legal frameworks. However, the market is highly competitive and can be challenging to penetrate. The market is receptive to innovative solutions, but redundant products may face difficulties.

## STAKEHOLDER INTERVIEW INSIGHTS

Interview insights highlight Singapore's strength as one of the largest cybersecurity markets in Asia. However, the market is highly competitive and can be difficult to enter. The market favours innovative solutions over redundant products.

## IN-SEC-M MISSION INSIGHTS

The international mission to Singapore conducted in November 2023 revealed that:

- › The exploratory mission provided a better understanding of the complex and mature cybersecurity ecosystem in Singapore. It helped identify key local players necessary for success in the market.
- › The level of technical expertise among existing players in Singapore is very high. This indicates that the market is reserved for solution providers with cutting-edge expertise and a proven ability to compete in a highly competitive environment, where the world's best cybersecurity providers operate.
- › Singapore demonstrates a strong interest in foreign innovation and has a welcoming approach to integrating start-ups and innovative companies into existing programs. This presents a promising avenue for Canadian companies seeking to enter the Singaporean market. Singapore is considered a gateway to Asia-Pacific markets.

65. Ibid.

66. Ibid.

## Development Priorities

The shortlisted markets, as outlined above, have been categorized into specific groups based on their priorities for future export development. The prioritization process primarily considered In-Sec-M's past experience of visiting these target markets, along with additional research insights discussed in the previous section. It also considered Canada's capabilities and the opportunities present in the target markets, as well as any insights gathered from interviews.

### High Priority Market

The countries/regions listed below have been classified as high priority markets that should be the primary focus in the short-term (1 year) for exploring new export opportunities and/or strengthening existing export partnerships. These countries and regions demonstrate significant potential for Canada's export of cybersecurity products.

High Priority Markets	Sectors of Opportunities
<b>UK</b>	<ul style="list-style-type: none"> <li>› Finance</li> <li>› Health</li> <li>› Defense and Security</li> <li>› Retail &amp; SMEs</li> <li>› Energy &amp; Utilities</li> <li>› Education</li> </ul>
<b>France</b>	<ul style="list-style-type: none"> <li>› Health</li> <li>› Defense and Security</li> <li>› Retail &amp; SMEs</li> <li>› Industry</li> <li>› Public Sector</li> <li>› Aerospace and Transportation</li> <li>› Energy and Environment</li> </ul>
<b>Switzerland</b>	<ul style="list-style-type: none"> <li>› Network and Telecommunication</li> <li>› Health</li> <li>› Industry</li> <li>› Energy &amp; Public Sector</li> <li>› Transportation &amp; Logistic</li> <li>› Banking, Finance and Insurance</li> </ul>

### Medium Priority Market

The following countries/regions are prioritized as medium priority markets that should receive attention in the mid-term (1 to 3 years) as Canada continues to diversify its export of cybersecurity products and services. These countries and markets exhibit opportunities but also may impose uncertainty or risks/challenges. For some markets, entry could take time and relationship buildings.

Medium Priority Markets	Sectors of Opportunities
<b>Mexico</b>	<ul style="list-style-type: none"> <li>› Banking, Finance and Insurance</li> <li>› SMEs</li> <li>› Transportation &amp; Logistic</li> <li>› Energy</li> <li>› Public Sector</li> </ul>
<b>Brazil</b>	<ul style="list-style-type: none"> <li>› Banking, Finance &amp; Insurance</li> <li>› Healthcare</li> <li>› Mining &amp; Energy</li> <li>› Agriculture</li> <li>› Retail &amp; SMEs</li> <li>› Transportation &amp; Logistic</li> <li>› Industry</li> </ul>
<b>Germany</b>	<ul style="list-style-type: none"> <li>› Banking, Finance &amp; Insurance</li> <li>› Health</li> <li>› Government, Defense &amp; Security</li> <li>› Energy</li> <li>› Manufacturing &amp; Industry</li> <li>› Transportation &amp; Logistic</li> <li>› Public Sector</li> <li>› SMEs</li> </ul>
<b>Benelux</b>	<ul style="list-style-type: none"> <li>› Banking, Finance and Insurance</li> <li>› Transportation &amp; Logistic</li> <li>› Defense &amp; Security</li> <li>› Public Sector</li> <li>› Retail &amp; SMEs</li> <li>› Automotive Industry</li> </ul>
<b>Italy</b>	<ul style="list-style-type: none"> <li>› Banking, Finance &amp; Insurance</li> <li>› Automotive</li> <li>› Transportation &amp; Logistic</li> <li>› Defense &amp; Security</li> <li>› Telecommunications</li> <li>› Energy and Utilities</li> <li>› Health</li> </ul>
<b>Singapore</b>	<ul style="list-style-type: none"> <li>› Finance, Fintech &amp; Banking</li> <li>› Health</li> <li>› Government and Public Sector</li> <li>› Transportation &amp; Logistic</li> <li>› Energy</li> <li>› Telecommunications</li> <li>› Industry &amp; Manufacturing</li> <li>› Defense &amp; Security</li> </ul>



## Future Consideration

Spain is currently not listed as a high or medium priority market due to the lack of information throughout the research exercise. However, it is recommended that continued information gathering and monitoring is needed, and whenever opportunities allowed, to further examine opportunities in Spain. While the following countries - India, Malaysia, Japan, and South Africa - were mentioned in one of the multiple sources of information used during the research and stakeholder interview process, they were not included in the shortlisted analysis above. However, it is recommended that these countries be closely monitored for potential future consideration.

---

## Recommendations

The market analysis and the priorities presented above can be used by In-Sec-M and Canadian companies in the cybersecurity industry to consider their future export diversification. As different companies may present different strengths and capabilities, the market priority at an individual company level should be carefully assessed. Nevertheless, the analysis presented above provides comprehensive information for consideration.

As this report is being prepared, international engagement activities are actively pursued and conducted by In-Sec-M. Therefore, as new information and intelligence are received, the recommendations above should be reviewed on an ongoing basis and refreshed regularly.

It is also worth noting that the purpose of this study is to diversify Canada's export of cybersecurity products and services, and the shortlisted markets presented above were chosen based on an aggregate of multiple information sources. Certain markets that have already established strong trading relationships with the Canadian cybersecurity industry are not included in this analysis, but it does not mean that future exports should not focus on these markets. Canadian companies should continue to leverage their existing partnerships in these markets. In addition, exploring new markets remains an important activity for market development. In-Sec-M and Canadian companies in the industry should actively pursue new market development opportunities.

# International Business Strategy Development

In this section, the findings from the sector analysis and target market analysis have been aggregated to provide a comprehensive SWOT analysis. This analysis serves as a foundation for establishing strategic objectives and developing a detailed action plan for In-Sec-M and Canadian companies in their efforts to diversify their exports in the cybersecurity industry. By identifying strengths, weaknesses, opportunities, and threats, this SWOT analysis will guide the formulation of effective strategies and actions to capitalize on market potential and overcome challenges. Through a focused approach, In-Sec-M and Canadian companies can leverage their strengths, address weaknesses, seize opportunities, and mitigate threats to successfully expand their presence in international markets.



# 3.1 SWOT Analysis

The following SWOT analysis summarized the Strengths, Weaknesses, Opportunities, and Threats identified in the sector analysis and the selection of target markets.

## Strengths



- › In-Sec-M has exhibited leadership in the Canadian cybersecurity sector through its ambitious organizational objectives, international trade ventures, and extensive services offered to the industry.
- › The Canadian cybersecurity sector has shown robust growth in terms of revenue, job creation, and GDP over recent years, indicating positive trends.
- › The Canadian cybersecurity industry possesses strong capabilities in delivering cybersecurity infrastructure services and solutions, which could be advantageous in foreign markets and clients with deficient infrastructure.
- › Canadian firms exhibit a strong commitment to serving SMEs and the public sector. The health, e-commerce, and manufacturing industries are also significant clients of Canadian cybersecurity companies.

## Weaknesses

- › Some sub-sectors of Canadian cybersecurity have not experienced growth. Between 2020 and 2022, sectors such as Encryption and ICS, SCADA, and OT saw a decline in sales.
- › Over 70% of Canada's cybersecurity product and service exports are destined for the U.S., which indicates a strong trading partnership but also reveals a lack of export diversification.



## Opportunities

- › The research identified several major international cybersecurity conferences that could provide Canadian companies with opportunities to increase brand awareness and explore potential export opportunities.
- › Global socio-economic trends are driving increased demand for cybersecurity products and services. These trends include the increasing digitalization across all sectors, new challenges arising from the pandemic, and the growing adoption of AI.
- › Trends within the cybersecurity sector present opportunities for Canadian companies to innovate and enhance their capabilities. These trends include the rapid evolution of technology and the increasing complexity of cyber threats.
- › Potential export diversification opportunities exist in the following markets: North, Central, and South America (Mexico and Brazil), Europe (United Kingdom, Germany, France, Benelux (Belgium, Netherlands, Luxembourg), Spain, Italy, and Switzerland), and Asia (Singapore).



## Threats

- › Internationally, several countries are imposing stricter data sovereignty regulations, which could affect international solution providers, increase market entry costs, and potentially lead to geopolitical risks.
- › Export controls in certain countries could also pose a threat to the Canadian export of cybersecurity products and services.
- › In some target markets, although the demand for cybersecurity is rising, it may not be a top priority for companies and/or the government.
- › Some target markets exhibit strong competition, and entry might be challenging as it requires time to build relationships and partnerships and necessitates high-quality and cost-competitive solutions to succeed.
- › Due to cultural and business environment differences, Canadian companies seeking market diversification need to develop understanding of their target markets and can benefit from information and guidance from experts and industry organizations.



# Strategic Objectives

Whilst there are risks and challenges to international expansion, such as regulatory issues and currency fluctuations, expanding into international markets can offer companies significant growth opportunities and strategic advantages. These generally include:

1

### Revenue Growth:

International markets offer new customer bases, potentially leading to increased sales and revenue.

2

### Diversification:

Operating in multiple countries can help companies reduce risk by diversifying their revenue streams and minimizing the impact of economic downturns in any single market.

3

### Access to Resources:

Companies may expand internationally to access resources such as raw materials, skilled labour, or technological expertise that may be scarce or expensive in their home country.

4

### Competitive Advantage:

Expanding globally can provide companies with a competitive advantage by allowing them to offer unique products or services, take advantage of lower production costs, or access new distribution channels.

5

### Market Saturation:

Companies may expand internationally when their domestic market becomes saturated, providing opportunities for growth.

6

### Economies of Scale:

Operating in multiple markets can lead to economies of scale, allowing companies to reduce production costs and increase efficiency.

7

### Brand Building:

International expansion can help companies build their brand presence and reputation on a global scale.

8

### Strategic Partnerships:

Companies may expand internationally to form strategic partnerships with foreign companies, allowing them to access new markets or technologies.

For Canadian companies within the cybersecurity sector, export diversification starts with the identification of the overall strategic objectives. The following three strategic objectives emerged from the research and stakeholder engagement.

---

## Strategic Objectives

# #1

### *Improving Canadian Cybersecurity sector's global awareness and reputation*

Improving the global awareness and reputation of the Canadian cybersecurity sector is critical for its international success. This can be achieved through a combination of marketing initiatives, thought leadership, and demonstrating expertise in handling cybersecurity threats. Participating in international cybersecurity forums, publishing research papers, and showcasing successful case studies can position Canada as a leader in the field. Additionally, ensuring that Canadian cybersecurity products and services meet the highest global standards can enhance the sector's reputation for quality and reliability. The goal is to make the Canadian cybersecurity sector top-of-mind for organizations worldwide when they seek robust cybersecurity solutions.

# #2

### *Establishing global strategic alliances and partnerships for Canadian Cybersecurity sector*

Establishing strategic alliances and partnerships can help Canadian cybersecurity companies to expand their global reach and access new markets more effectively. These partnerships can be with local technology firms, government entities, or even universities in target markets. Such alliances can offer valuable local market insights, ease regulatory compliance, and provide a more established customer base. Additionally, partnerships can lead to collaborative innovation, helping Canadian companies stay at the forefront of cybersecurity technology. The aim is to build a network of alliances that can provide a solid platform for the Canadian cybersecurity sector's international growth.



# #3

## *Strengthening Canadian Cybersecurity companies' presence in the target markets*

Strengthening the presence of Canadian cybersecurity companies in target markets involves more than just selling products and services. It requires building strong relationships with local customers, understanding their unique needs, and providing tailored solutions. This can be achieved through multiple channels, such as local offices or representatives, customer engagement activities, and localized marketing campaigns. It is important to note that different countries may require different methods due to cultural and business disparities, as well as the level of market penetration. Moreover, providing excellent customer service and support in the local language and according to local cultural norms can enhance customer satisfaction and loyalty. The goal is to make Canadian cybersecurity companies the preferred choice for customers in the target markets.

# #4

## *Maximizing market penetration and exploring new market opportunities*

In addition to the above strategic objectives, it is important to continue expanding the presence and market penetration of Canadian cybersecurity companies in already well-served markets or markets that have established strong trading partnerships with the Canadian cybersecurity industry, while simultaneously exploring new market opportunities. This objective aims to leverage existing relationships and partnerships to further strengthen market share and revenue generation, while also diversifying into untapped markets to capture new customers and increase overall market reach.

# Tactical Action Plan

The following tactical action table presents potential actions for In-Sec-M to consider implementing this International Business Development Strategy, move towards the strategic objectives and diversity Canadian export of cybersecurity products and services.

## Strategic Objectives

# #1

*Improving Canadian Cybersecurity sector's global awareness and reputation*

Action	Description	Timeline
1.1	Highlight and exhibit Canadian cybersecurity products and services to potential buyers at international industry events and conferences in potential target markets.	On-going
1.2	Amplify the visibility of Canadian exporters to major buyers in potential target markets through collaboration with local entities and Canadian diplomatic representatives and Trade Commissioners.	On-going
1.3	Refresh existing and develop additional comprehensive marketing tactics and branding that highlight the strengths and capabilities of the Canadian cybersecurity sector.	Short-term
1.4	Leverage digital platforms (such as online advertisement and promotional video) to increase global visibility and reach of Canadian cybersecurity products and services.	Mid-term



## # 2

*Establishing global strategic alliances and partnerships for Canadian Cybersecurity sector*

Action	Description	Timeline
2.1	Arrange a networking event between Canada and potential target markets during international industry conferences.	On demand
2.2	Schedule meetings with cybersecurity associations and private partners in potential target markets to integrate Canadian technological solutions into existing cybersecurity portfolios.	On demand
2.3	Continue to seek In-Sec-M's member feedback through existing communication channels, such as the business survey, on potential opportunities for oversea partnerships.	Recurring Annually

## # 3

*Strengthening Canadian Cybersecurity companies' presence in the target markets*

Action	Description	Timeline
3.1	Based on information provided in this Strategy and in collaboration with relevant government agencies, develop a comprehensive market entry guide and training for each potential target market, that considers local regulations, business practices, and cultural nuances.	Short-term
3.2	Provide ongoing support and resources to Canadian cybersecurity companies to help them navigate and succeed in potential target markets. Explore collaborations with other partners and organizations, including the Trade Commissioners.	On-going

## # 4

*Maximizing market penetration and exploring new market opportunities*

Action	Description	Timeline
4.1	In markets that are already well-served or have strong trading partnerships, strengthen relationships with existing partners by actively collaborating on joint initiatives, sharing resources, and exploring new business opportunities together. This can involve regular communication, joint marketing campaigns, and co-hosting events or webinars.	On-going
4.2	For new markets, conduct market visits and attend industry events to potential new markets to assess market potential, meet with local stakeholders, and understand the regulatory environment.	On-going
4.3	Actively and regularly refresh the International Business Strategy to reflect new accomplishments and identify emerging opportunities, to ensure that In-Sec-M and the Canadian cybersecurity industry remain well-positioned for continued success.	Annually



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

#### About Deloitte

Deloitte provides audit and 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<sup>®</sup> 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. 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.

Our global Purpose is making an impact that matters. At Deloitte Canada, that translates into building a better future by accelerating and expanding access to knowledge. We believe we can achieve this Purpose by living our shared values to lead the way, serve with integrity, take care of each other, foster inclusion, and collaborate for measurable impact.

To learn more about Deloitte's approximately 330,000 professionals, over 11,000 of whom are part of the Canadian firm, please connect with us on LinkedIn, Twitter, Instagram, or Facebook.

© Deloitte LLP and affiliated entities.





**IN·SEC·M**  
THE CANADIAN CYBERSECURITY CLUSTER