prompt

Overview of the Cybersecurity Industry in Quebec

October 8, 2024

Updated: February 2025

In collaboration with

IN·SEC·M
LA GRAPPE CANADIENNE DE LA CYBERSÉCURITÉ

cyber eco
Écosystème en cybersécurité

Contents

Message from the Executive Director

Studies indicate that the cybersecurity industry is grappling with a global talent shortage of 4 million professionals, and that the cost of cybercrime is projected to reach US$10.5 trillion by 2025[1].

In response to this unprecedented threat, Quebec's cybersecurity ecosystem has experienced rapid growth in recent years. Major corporations and the consulting firms that support them have recruited a significant number of experts. Education programs have been established in Quebec universities. As demand accelerates amid multiplying threats and growing public and corporate awareness of the need for cyber-resilience, local companies are making their mark in this market.

It is estimated that US$101.5 billion will be spent on cybersecurity service providers by 2025[2]. This is a rapidly evolving technological field, and PROMPT, given its role as a sectoral industrial research cluster in digital technologies, felt compelled to engage. Since 2019, we have been doing so through our innovation funding programs and cybersecurity certifications.

However, there is still very little data on Quebec's cybersecurity industry, its challenges, and its needs. This is why PROMPT, in collaboration with key ecosystem players, has developed this industry profile. This profile aims to better understand the companies in the industry, their needs and challenges, as well as the ecosystem in which they operate. It provides a common foundation of understanding that will facilitate reflection and the search for solutions to support even more effectively this ecosystem of undeniable strategic importance for Quebec.

I wish you an enjoyable read,

Liette Lamonde

Executive Director, PROMPT

[1] Cybersecurity Ventures 2023

[2] "Cybersecurity trends: Looking over the horizon", McKinsey & Company, march 2022.

COLLABORATORS

This overview is the result of numerous collaborations and contributions.

PROMPT extends its gratitude to the following for their contributions to the writing:

- Daniel J. Caron, Professor at the École Nationale d'Administration Publique
- Benoît Dupont, Full Professor at the School of Criminology at Université de Montréal and holder of the Canada Research Chair in Cyber-Resilience and the Research Chair in Cybercrime Prevention
- Nicolas Duguay, Co-Executive Director of In-Sec-M
- Pascal Fortin, President and CEO of Cybereco

For their feedback on the initial version and their valuable insights and funding of the study:

- The Ministry of Economy, Innovation and Energy
- The Ministry of Cybersecurity and Digital

Finally, we especially thank all members of Quebec's cybersecurity ecosystem (CISOs, experts, consultants, etc.) who graciously gave their time by responding to the survey and participating in numerous formal and informal meetings and discussions.

INTRODUCTION

Presentation of the Initiative and Its Objectives

In July 2023, PROMPT initiated a survey to produce an overview of cybersecurity companies in Quebec. The goal was to better understand the Quebec offering of cybersecurity products and services, as well as the ecosystem supporting this industry.

This overview is divided into five sections, presented in this report. The first section is a review of Quebec, Canadian, and international literature on the cybersecurity market and its dynamics. The second section highlights key data on the main actors of the industry, relying on a mapping of companies offering cybersecurity products and services, as well as a survey of about fifty of these companies. The third section deepens this panorama by examining the major public, private, and community players that make up Quebec's cybersecurity ecosystem, enabling the market to acquire new talent, develop innovative products, and benefit from supportive public policies and regulatory frameworks. The fourth section analyzes the challenges and opportunities of cybersecurity in Quebec. Finally, the fifth section explores considerations likely to strengthen the Quebec industry.

Context

Every day, the media highlight the perils associated with the omnipresence of digital technologies in every aspect of our daily lives. Data breaches affecting millions of consumers, ransomware attacks that paralyze companies of all sizes for extended periods, and foreign interference campaigns that disrupt electoral processes are just a few examples of a vast array of digital damages preventing citizens, businesses, and public organizations from fully benefiting from the Digital Revolution and the high connectivity rates available in Canada and Quebec[3]. In the post-pandemic context where companies have radically accelerated the digitization of their activities and many employees continue to work in hybrid mode, the proliferation of digital risks can harm our economy's prosperity and the well-being of the population.

In the largest representative survey of businesses conducted to date, Statistics Canada found that in 2019, 21% of Canadian businesses were affected by at least one cybersecurity incident that prevented employees from carrying out their daily activities and generated financial losses and reputational damage. This exposure to risk has not improved in recent years, despite cybersecurity spending estimated at $9.7 billion per year in Canada in 2021 (Statistics Canada, 2022). Small and medium-sized enterprises (SMEs), which constitute the bulk of Quebec's economic fabric, are particularly exposed to cyber risks, lagging in

[3] In this regard, see Canadian statistics showing that 94% of the population used the internet in 2022, compared to a global average of 67.4%, 90.5% in Europe, and 97.1% in the United States. See the International Telecommunication Union's page, retrieved from https://datahub.itu.int/data/?e=CAN&c=701&i=11624.

deploying the most basic protection measures due to organizational and technological challenges (Berry and Berry, 2018).

Cybersecurity is a term that appeared in the late 2000s (Bouchard and Henri, 2023). It "can be broadly defined as the practice of protecting oneself and one's organization against digital attacks" (Quan and Herron, 2022). Since its emergence, cybersecurity has continued to gain importance given the essential nature of digital technologies in the functioning of today's society.

Cybersecurity professionals have seen the terminology used to frame their service and product offerings evolve, from computer security in the 1960s to information security in the 2000s, with the prefix "cyber" becoming widespread in the 2010s (Landwehr, 2010). This evolution not only reflects new trends launched by entrepreneurs eager to differentiate their solutions from those of competitors. It also denotes the broadening scope of cybersecurity, which has gone beyond its initial narrow interest in machine security to gradually integrate considerations about the information stored and processed by these machines, and finally the humans and institutions that interact with them (Dupont and Whelan, 2022).

In such a context, the cybersecurity industry plays a central role today in protecting critical infrastructures and digital technologies that drive our prosperity and allow our economy to remain globally competitive. It therefore appears necessary, in order to better understand the factors influencing its development and to implement effective support mechanisms, to assess the current state of affairs. This report brings together various primary and secondary data sources to provide the most comprehensive overview possible of the cybersecurity industry in Quebec, for which information was until now partial and fragmented. Due to the nature of the available data, this document has certain limitations in terms of the representativeness of the results, which we will highlight where relevant. Nevertheless, it offers valuable insights into the current state and evolution of this industry, thanks to the full collaboration of its main actors.

The Cybersecurity Industry

An industry is typically defined as a group of companies or businesses that produce or provide goods, services, or sources of revenue related to their core business activities. In this sense, the various companies offering cybersecurity products and services can be considered an industry.

This industry encompasses a wide range of activities, products, and services designed to protect networks, computing devices, programs, and data from attacks, damage, or unauthorized access. The main criteria that define an industry are examined below in the particular context of cybersecurity to determine its level of maturity:

Specific Products and Services	This industry offers distinct products and services such as antivirus software, firewalls (and other network protection equipment), security monitoring, threat analysis,	

	cybersecurity education, and security consulting services, which are specifically designed to meet the IT security needs of organizations and individuals.	
Common Market	Companies within the industry serve the same market or customer base, although they may target different segments of this market. They compete for the same group of clients. The demand for cybersecurity is constantly increasing worldwide due to the growing digitization of businesses and society in general. This growth is fueled by the rise in cyber threats and the awareness of the need to protect critical information and infrastructures.	
Supply Chain and Ecosystem	The cyber industry includes a complex supply chain and ecosystem, involving software developers, hardware suppliers, service companies, security consulting firms, as well as research and standardization organizations. Companies within an industry may source technology or labour from the same suppliers and sell their solutions through similar channels.	
Regulations and Standards	The industry is regulated irregularly and unevenly, notably with specific laws aimed at protecting data in the context of personal information protection. Businesses and public organizations are generally subject to the same laws, regulations, and directives. The industry helps them comply with these. However, best practices, quality, and the scope of services and solutions are not governed by laws and instead rely on unreliable self-regulation mechanisms. These regulatory frameworks can define the boundaries of an industry and affect how companies operate within it.	
Economic and Market Forces	Industry players are influenced by similar economic and market forces, such as demand and supply dynamics, technological advancements, and global economic trends. Companies within this industry respond similarly to these external factors. Macro-trends (e.g., XDR, Zero Trust, the move towards all-inclusive platforms, etc.) are extremely influential on consumer behaviour and consequently on companies.	
Economic and Social Impact	Cybersecurity has a significant impact on the economy and society, as cyberattacks can lead to considerable financial losses, damage corporate reputations, and compromise national security.	
Innovation and Research	The cybersecurity industry is characterized by rapid and continuous innovation, with ongoing research to develop new technologies and approaches to counter emerging cyber threats.	

Classification Systems	Various classification systems, such as the North American Industry Classification System (NAICS) in Canada, Standard Industrial Classification (SIC) codes, and the International Standard Industrial Classification of All Economic Activities (ISIC), are used to categorize and define industries based on a hierarchical structure of economic activities. Most companies in this industry use codes related to software development or scientific consulting services. There is no category for cybersecurity.	

Given these observations, cybersecurity constitutes a full-fledged industry, even though it is closely tied to the IT industry in general. As we have already emphasized, this industry plays a crucial role in protecting critical infrastructures (which are increasingly dependent on digital technologies) and in securing the global digital economy. This exposes it to issues and constraints that transcend the boundaries of industry actors alone and represent a complex set of challenges requiring an integrated approach encompassing technology, management, education, and cross-sector collaboration to effectively protect digital assets in an ever-evolving threat landscape.

These issues and constraints are as follows:

1. **Ubiquity of Threats**: Cyberattacks know no sectoral boundaries. They can affect any organization, regardless of its field of activity. Critical infrastructures such as financial institutions, telecommunications operators, transportation companies, energy distributors, or healthcare services are often prime targets due to their importance to society and the economy.

2. **Management and Governance**: Protecting against cyber threats requires a strategic management approach that integrates cybersecurity into the company's planning and daily operations. This necessitates strong governance, adequate resource allocation, and decision-making at the highest level of the organization. These processes are relatively complex to implement for organizations with significant resources and a high level of cybersecurity maturity, but they can discourage small or medium-sized enterprises that rarely have the means and knowledge to adopt them (Westin et al., 2022).

3. **Technological Capabilities**: The challenges of cybersecurity and cyber resilience require advanced technological solutions and continuous adaptation to new threats. This implies not only investing in technology but also developing the capacity to integrate and effectively manage these technologies within existing business processes. This constant responsiveness to attackers' innovations explains why this industry has difficulty stabilizing and does not conform to traditional development models like those of the automotive or aerospace industries (Carmel and Roche, 2023).

4. **Knowledge and Skills**: Combating cyber threats demands specialized knowledge and advanced technical skills. Organizations must invest in education and developing their personnel's competencies, but also in raising cybersecurity awareness at all levels of the organization.

5. **Cross-Sector Collaboration:** Given that supply chains and infrastructures are interconnected across different sectors, resilience against cyber threats depends on collaboration between various industry actors. Sharing information on threats, best practices, and mitigation strategies is crucial to collectively strengthen cyber resilience.

6. **Standards and Regulations**: While some cybersecurity standards are specific to certain industries (PCI-DSS, NERC/FERC, etc.), many standards, guidelines, and best practices are applicable across different sectors (ISO 27000, US NIST, SOC II, CyberSecure Canada, etc.). Compliance with these standards requires a comprehensive approach to cybersecurity that goes beyond the limits of a single industry.

1. OVERVIEW OF CYBERSECURITY IN THE WORLD AND IN QUEBEC (LITERATURE REVIEW)

1.1 Data Sources and Methodology

This report is based on data collected using three complementary methodologies (document analysis, survey, and semi-structured interviews) that allow us to provide a relatively detailed picture of the cybersecurity industry in Quebec and the ecosystem within which it operates.

First, a document analysis was conducted to paint an overview of cybersecurity in the Canadian and Quebec contexts and to compare this information with data from the global context when relevant. In this regard, about thirty reports, government websites, and scientific articles identified using the Google Scholar search engine were consulted and analyzed based on the following themes: the current state of cybersecurity in Quebec, Canada, and the world; trends and developments in the cybersecurity market; and government interventions to support and strengthen the cybersecurity industry.

Secondly, a statistical overview of cybersecurity companies in Quebec was produced based on public information collected about 157 companies operating in this field. Furthermore, PROMPT conducted a survey of a sample of 47 companies from this industry. This survey included 43 questions specific to the module administered to cybersecurity suppliers and providers, aiming to obtain quantitative and qualitative data on the companies in the following areas: geographical location, company history, workforce composition and main challenges in talent acquisition and retention, types of products and services offered, technological intensity of the products and services offered (existence of a company-specific software solution), R&D investment, target clientele and clients' fields of activity, main challenges in client interactions, factors influencing sales to private and public clients, profitability, state of competition, export activities, and anticipated future of the company.

Thirdly, the report uses qualitative data collected from open-ended questions in the survey, allowing respondents to specify certain issues and challenges faced by their company, as well as testimonies gathered during four semi-structured interviews with key individuals working within cybersecurity companies in Quebec.

As indicated in the introduction, this report has a number of limitations: it does not claim to be representative of the diversity of situations and trends in a very dynamic and ever-evolving industry. The survey reached only a limited sample of respondents, and its length discouraged some who did not answer all the questions. However, the quantity of responses obtained and the access they provide to the experiences of executives from cybersecurity companies of all sizes seem to contribute to a significant improvement in knowledge about this industry. Furthermore, the available statistical data on the size and activities of this industry remain very fragmentary, whether in Quebec or Canada, which does not allow for reliable tracking of its evolution over time. Finally, the four qualitative interviews were conducted openly with small-sized companies (from three to forty employees) whose experiences might be very

limited in certain areas and whose responses could vary according to the immediate interests or knowledge of the respondents.

These limitations therefore reinforce the very purpose of this report and the need to continue the effort to map the cybersecurity industry in Quebec, whose strategic role in protecting vital digital assets is undeniable.

1.2 The Global Cybersecurity Market and the Three Mega-Clusters

To better contextualize the activities of Quebec's cybersecurity industry and its supporting ecosystem, it is important to understand the place cybersecurity occupies as an economic activity on a global scale and where the main clusters of expertise and capabilities are concentrated in this rapidly growing field.

In September 2023, the specialized consulting firm Gartner estimated that the global cybersecurity market represented a turnover of US$166 billion in 2022, and predicted it would reach US$188 billion in 2023 and US$214 billion in 2024, an impressive average growth of 13% per year in an otherwise rather gloomy general economic context (Gartner, 2023). Among the sub-sectors with the highest growth were cloud infrastructure security (+24.7% in 2024), privacy protection (+24.6% in 2024), and critical infrastructure protection (+17.5% in 2024). Services would account for 42% of this global market, thus constituting the largest expenditure item in this field (Gartner, 2023). At the continental level, the North American market was estimated at just over US$67 billion in 2022, which then represented 44% of the global market and made it an undisputed leader (Fortune Business Insights, 2024).

The supply of products and services is concentrated around approximately 3,000 companies worldwide (The Economist, 2018), with more than half of the most powerful ones headquartered in three geographic areas that can be called mega-clusters: Silicon Valley south of San Francisco, the Washington, D.C. region, and Israel (around the four urban centers of Haifa, Tel Aviv, Jerusalem, and Beersheba). Indeed, in 2018—the most recent year for which comparative data are available—these three regions hosted over 930 companies that accumulated US$37 billion in venture capital investments and collectively generated US$33 billion in revenues (Carmel and Roche, 2023). Other centers are trying to form a critical mass and emerge in London, New York, Boston, San Antonio, Singapore, or even Paris, but they find it difficult to bring together the main factors that allow the emergence and development of such a high-performing cybersecurity cluster.

In a landmark study, Cohen et al. (2017) identified seven determining factors. First, they note four well-known factors common to other types of industrial clusters: the existence of social and business networks that facilitate information exchange, relationship building, collaboration, and workforce mobility; the presence of research centers and universities that serve as research platforms, sources of funding for startups, and generators of skilled personnel; nearby complementary industries that understand the market (for example, in cloud computing, artificial intelligence, or quantum computing); and favorable government policies regarding public procurement, R&D funding, and commercial promotion abroad. Three factors specific to cybersecurity were identified, which stimulate the growth of these clusters: the proximity to government activities in cybersecurity; the availability of skilled personnel, often resulting from the retirement of government employees from security and intelligence agencies and from

education provided by colleges and universities; and a more intangible factor—the existence of strong industrial leadership that helps catalyze the efforts of what resembles a diversified and functional ecosystem.

1.3 Demand for Cybersecurity in Canada and Quebec

Several technological factors have contributed to making cybersecurity an increasingly important concern. Among these are the adoption of cloud computing, the integration of digital systems, the use of artificial intelligence, 5G connectivity, and the rising popularity of remote work (Heron et al., 2020; TECHNOCompétences, 2021). Today, all companies utilize technology in their operations. The transition of organizations toward digital practices brings cybersecurity to play a leading role in their functioning (Deloitte, 2023).

In Quebec, a survey conducted among 336 boards of directors found that cybersecurity is perceived by administrators as the second most significant risk for the coming year, just behind employee retention and recruitment (Bouchard and Henri, 2023). However, this same study notes differences in the importance given to cybersecurity depending on the size of the companies (Bouchard and Henri, 2023). Cybersecurity ranks second among concerns for medium and large organizations (Bouchard and Henri, 2023). For small organizations, cybersecurity ranks fifth (Bouchard and Henri, 2023).

A study conducted by the Fédération des chambres de commerce du Québec (2021) also highlights the importance given to cybersecurity by senior company executives. In this regard, 87% of CEOs in Canada say they are concerned about cyber threats (Fédération des chambres de commerce du Québec, 2021). Canadian organizations are concerned about cybersecurity for many reasons, but the 2017 Canadian Survey of Cyber Security and Cybercrime reveals that their main motivation is the protection of personal information (Quan and Herron, 2022).

As mentioned earlier, a significant factor increasing the importance of cybersecurity is compliance with new legislative and regulatory obligations implemented by the Canadian and Quebec governments. Major and highly publicized attacks have also drawn attention to cybersecurity in recent years. Indeed, "attacks targeting Desjardins, Revenu Québec, Bell Canada, Equifax, Capital One, Cégep de St-Félicien, and the Société de transport de Montréal have captured the public's imagination due to the number of personal data stolen, the size of the ransoms demanded, or the duration of operational shutdowns of infected organizations" (Bouchard and Henri, 2023, p.5). Consequently, companies are under increasing pressure to protect their IT assets and data, creating opportunities for the cybersecurity industry (Aiyer et al., 2022).

In a market economy, every industry must provide satisfactory and tailored responses to the demands of buyers who have the necessary resources to acquire its goods and services. The data collected by Statistics Canada as part of its biennial survey on cybersecurity and cybercrime is likely among the most representative of a national market. Indeed, more than 12,000 companies participated in the 2021 survey, achieving a response rate of 74% (Statistics Canada, 2022). Faced with an ever-evolving threat landscape, 62% of Canadian businesses purchased cybersecurity products or services in 2021, with total expenditures estimated at CAD 10 billion. Large enterprises accounted for 45% of these expenses, medium-sized

businesses for 25%, and small businesses for 30%. Additionally, expenditures related to restoring operations after a cyber-attack amounted to approximately CAD 600 million, marking a significant increase of 50% over two years compared to 2019.

The exposure of Canadian businesses to cyber-attack risks is fairly evenly distributed, with about 20% of companies affected by incidents each year. Large enterprises are the most exposed, with 37% having been victims, while medium and small businesses are not immune, with 25% and 16% respectively experiencing incidents. Although the survey does not allow for the calculation of the total damages and indirect costs resulting from cyber-attacks targeting Canadian businesses, it does reveal that affected companies report spending approximately 80% more on their cybersecurity compared to unaffected businesses (+120% for small businesses and +75% for large businesses). These combined figures suggest that the cybersecurity industry in Canada is poised for robust growth in the coming years, as the number and frequency of cyber-attacks are expected to continue increasing.

While Statistics Canada does not provide provincial-level data, a 2021 survey conducted by Cybereco among 157 of the largest companies indicates a similar trend. Specifically, 60% of cybersecurity expenditures are allocated to remediation efforts, and 90% of companies have experienced budget increases over the past two years. Furthermore, with 50% of companies dedicating less than 6% of their IT budgets to cybersecurity and customer data theft remaining a major concern, there is considerable room for improvement (Cybereco, 2022). However, an uncertain economic situation could potentially hinder the necessary investments.

1.4 Retombées économiques de l'industrie de la cybersécurité au Canada et au Québec

In recent years, the cybersecurity industry has grown significantly both in Canada and Quebec under the pressure of the aforementioned factors. Between 2018 and 2020, the Canadian cybersecurity industry outpaced the broader ICT sector in terms of revenue (30% growth versus 12%), employment (31% growth versus 3%), research and development (35% growth versus 19%), and exports (10% growth versus 2%) (Innovation, Science and Economic Development Canada, 2022). In 2020, the Canadian cybersecurity industry generated CAD 3.2 billion in GDP through direct revenues (CAD 1.6 billion), revenues generated by industry suppliers (CAD 0.8 billion), and employee consumption expenditures (CAD 0.8 billion). Additionally, 29,400 jobs were created, including direct jobs within the industry (14,100), jobs with suppliers (7,800), and jobs induced by associated employee consumption expenditures (7,500) (Innovation, Science and Economic Development Canada, 2022).

This industry is overwhelmingly composed of small and medium-sized enterprises (SMEs), with 90% employing fewer than 250 people and only 6% employing more than 500 people. However, the revenues generated and jobs created by large companies accounted for 36% and 37% of the total, respectively, compared to 47% in both areas for their small and medium-sized counterparts. Nevertheless, SMEs make a significant contribution to exports, responsible for 55% of cybersecurity product and service sales abroad, compared to 26% for large companies. In total, over CAD 1.1 billion in exports were generated,

with more than 72% originating from the United States (Innovation, Science and Economic Development Canada, 2022). The dynamism of the industry is also reflected in Canada's ranking as the 6th largest global market for venture capital investments in cybersecurity in 2019 (Investissement Québec, 2021).

Quebec ranks third among Canadian cybersecurity hubs, accounting for 15% of the total reported cybersecurity jobs, behind Ontario (58% of cybersecurity jobs) and Western Canada around the Vancouver hub (20%) (Innovation, Science and Economic Development Canada, 2022). It is noteworthy that this represented a 4% decrease compared to the situation in 2017, while Ontario increased its workforce by 6% during the same period. The COVID-19 pandemic and the explosion of artificial intelligence, where Montreal holds a privileged position, have certainly caused significant changes, but unfortunately, no statistics are available for the past five years. The most widespread cybersecurity activities in Quebec include security infrastructure solutions, compliance audits and program development, bundled solutions, penetration and monitoring testing, and education (Innovation, Science and Economic Development Canada, 2022).

1.5 The Cybersecurity Workforce

One of the essential conditions for the harmonious growth of the cybersecurity market is the existence of a qualified workforce capable of filling available positions. "Cybersecurity professionals are responsible for protecting organizations and individuals against cyberattacks" (Quan and Herron, 2022). These individuals possess the skills to create, operate, and maintain secure systems while responding to threats (Herron et al., 2020). However, the high demand for cybersecurity observed in recent years poses significant challenges for the recruitment and retention of personnel.

The substantial talent shortage in cybersecurity is a global phenomenon (Quan and Herron, 2022). Between 2016 and 2021, the demand for cybersecurity talent increased by over 40% (Fédération des chambres du commerce du Québec, 2021). In Canada, by 2021, although the number of people working in cybersecurity had surged in recent years, a talent shortage remained (Quan and Herron, 2022). In a field where unemployment is virtually nonexistent, approximately one in six positions remains unfilled (Quan and Herron, 2022, p. 4). In Quebec, in 2022, more than half of the organizations employing cybersecurity professionals had vacant positions (31% were looking to fill 1 to 5 full-time equivalents (FTEs), 12% for 6 to 15 FTEs, and 11% for more than 15 FTEs) (Cybereco, 2022). Furthermore, another major workforce challenge in cybersecurity is the alignment between the actual skills of employees and the skills required to meet current and foreseeable security needs. Once again, Quebec organizations seem to suffer from a concerning deficit, as 62% of them estimated that their specialized cybersecurity staff lacked skills or even had significant gaps in the field (Cybereco, 2022).

Another consequence of the talent shortage is that it increases competition among employers, thereby driving up salaries for employees in this industry, which does not help organizations in their search for personnel. The work of Quan and Herron (2022) shows that salaries are inflated by demand. Additionally, the lack of diversity is also mentioned as a factor that has negative consequences on the workforce. For example, the underrepresentation of women in the field exacerbates the workforce shortage (ISC², 2021).

In Canada, in 2020, women held only 23% of technical and scientific positions in cybersecurity, while their presence was more balanced in administrative, marketing, and management roles, where they held 40% of positions (Innovation, Science and Economic Development Canada, 2022). Recruitment challenges also affect the public sector. On the contrary, it faces its own unique challenges, such as "lower salary levels compared to the private sector, insufficient funding, bureaucratic obstacles, cumbersome hiring processes, background checks, and burnout" (Quan and Herron, 2022, p. 8).

While this workforce shortage is also present in the United States, the Canadian shortage has its peculiarities. Firstly, Canada does not have a national competency framework (similar to the NICE in the United States), which hinders communication between employers and potential cybersecurity employees regarding the necessary skills to succeed (Quan and Herron, 2022). Secondly, the work of Quan and Herron (2022) indicates a lack of communication between the cybersecurity industry and the academic sector. Finally, the U.S. job market competes with the Canadian market by offering often more attractive compensation (Quan and Herron, 2022). The United States faces a workforce shortage 15 times greater than that experienced in Canada (Quan and Herron, 2022). The loss of Canadian talent moving to the United States highlights the fragility of the Canadian industry. This competition and its negative manifestations have drastically increased since the COVID-19 pandemic, where the widespread adoption of remote work allows Canadian employees to be geographically relocated while accessing the highly attractive compensation offered by their American employers.

Moreover, a significant number of workers in the cybersecurity field are IT generalists who have been assigned cybersecurity responsibilities (Herron et al., 2020). Not all companies wish to hire specialized personnel (Herron et al., 2020). In this regard, a pan-Canadian survey highlights two main reasons why companies have not hired cybersecurity professionals: 1) they relied on external consultants rather than their own staff, or 2) they believed that their company's cybersecurity was not sufficiently threatened (Herron et al., 2020, p. 22). This second point underscores the need to recognize the risks, as well as cybersecurity expertise, and to raise awareness among companies about its importance.

Several strategies are being implemented by companies to address recruitment and retention issues in cybersecurity personnel. A survey conducted by Deloitte (2023) highlights the following strategies as the most used by respondents: offering education and access to certifications, a flexible or hybrid work environment, specialized career paths, differentiated compensation models, opportunities for internal and international mobility, and support for completing an MBA (Deloitte, 2023).

Cybersecurity is a specialized field for which there are numerous education programs and certifications, with more than 70 different certifications cataloged by Knowles et al. (2017). Certifications are an integral part of the cybersecurity ecosystem. A 2019 survey of over 3,000 respondents worldwide revealed that 59% of cybersecurity professionals planned to obtain a certification during the year or were already pursuing one ((ISC)², 2019). However, certifications can be costly, which poses a barrier to entry for the field (Quan and Herron, 2022). Moreover, the ability of these certifications to reliably assess the skills of their holders is questioned by many professionals, who believe that the near-systematic use of multiple-choice questions as a method of evaluating qualifications is too static and ineffective (Knowles et al., 2017).

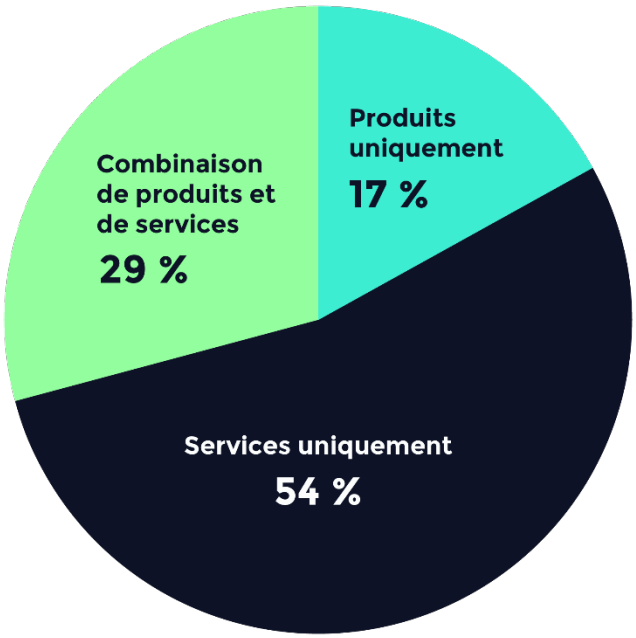
In addition to certifications, several university and college education programs are offered in cybersecurity in Quebec and Canada. Canada is actually ranked first for its number of undergraduate and graduate programs in cybersecurity (Montréal International, 2021). In Montreal alone, there are 14 college and continuing education programs in cybersecurity, in addition to over ten research chairs in cybersecurity (Montréal International, 2021). According to a count carried out in 2018 by the Integrated Cybersecurity Network, Quebec hosted nearly 30% of the available college and university cybersecurity programs in Canada, or 37 programs out of 125. This multiplicity and diversity of education programs provide a substantial pool of potential employees, but the fragmentation of the programs and the lack of coordination in developing their curricula hinder their visibility and do not help students adequately evaluate which are best suited to the needs and requirements of the job market. The Canadian Centre for Cyber Security did publish in 2024 a commented list of the main cybersecurity certifications available in Canada (Canadian Centre for Cyber Security, 2024), but no similar resource is yet available for university and college education programs.

2. OVERVIEW OF CYBERSECURITY COMPANIES FROM QUEBEC

To provide an overview of the cybersecurity industry in Quebec, we conducted a review of the characteristics of companies listed in this sector.

2.1 Company Offerings and Their Areas of Activity

Of the 157 companies catalogued through the document analysis, 26 (16.6%) offer only products[4], 46 (29.3%) offer a combination of products and services[5], and 85 (54.1%) offer only services[6].



The survey conducted among the 47 respondents reveals a similar reality, with 26 companies (55.3%) in the sample reporting that they offer cybersecurity consulting services, and 21 companies (44.7%) offering cybersecurity products, likely accompanied by complementary service offerings.

Whether characterized by services or products, the vast majority of companies rely on proprietary software solutions: 44 companies (93.6%) reported using one or more software solutions, while only 3 companies (6.4%) offered exclusively services to their clients. In more than half of the cases (56.8% of the sample), the software solutions were entirely developed in-house by the companies, and partially in 29.5% of cases, with only 13.6% of companies depending on solutions developed by third parties[4]. Thus, 86.3% of the surveyed companies had generated intellectual property and innovation internally, which can constitute a significant differentiation and competitiveness factor for these companies in global markets.

A survey question addressed the geographical origin of these software developments: 65.9% of companies that had developed software solutions relied on Quebec-based resources, 13.6% on American resources, 9.1% on resources from other Canadian provinces, and 9.1% on European resources. This indicates that cybersecurity companies from Quebec have a good command of their digital supply chain, which remains two-thirds based in Quebec, and in over 20% of cases concentrated in the rest of North America.

The main areas of expertise of the companies were also compiled. To do this, 13 categories were selected with the study's partners to specify the predominant areas of expertise in Quebec. The table below

presents the distribution of survey respondents across these 13 areas of activity, listed in descending order[16].

Area of Expertise	N	%
Managed cybersecurity services	33	77%
Cybersecurity governance	21	49%
Penetration testing	21	49%
Assistance with cybersecurity certifications and audits	20	47%
Workforce education/awareness/education/upskilling	19	44%
Incident response/forensics	19	44%
Personal information protection	19	44%
Access management/authentication (IAM)	18	42%
Threat detection	18	42%
Cyberprotection of operational technologies (O.T.) and IoT	14	33%
Software development security	13	30%
Asset protection	12	28%
Other	9	21%

The survey indicates that managed services, cybersecurity governance, and penetration testing are the three main areas of expertise for Quebec companies, closely followed by about half a dozen other types of activities. Conversely, cyberprotection of operational technologies (O.T.) and the Internet of Things (IoT), software development security, and asset protection are the areas with the least activity among the surveyed companies (though nearly a third of companies declare competence in these areas). These results suggest that the majority of cybersecurity companies from Quebec are generalists operating across multiple areas of expertise, with only a minority (seven companies, or 15% of the sample) being "pure players" specializing in a single area of activity.

A significant dimension of the cybersecurity industry in Quebec is the role it plays in protecting essential infrastructures. Indeed, 34 companies (72.3%) in the sample reported offering services related to the protection of essential infrastructures. The most frequently cited clients include the transportation and logistics sector (82.3%), critical electricity and water distribution infrastructures (79.4%), government and parastatal sectors related to the protection of citizen data (70.6%), followed by the telecommunications sector (67.6%), the financial sector (banking and insurance) (67.6%), and the healthcare sector (64.7%). The legal sector, for its part, appeared to be much less covered, with only 32.3% of responding companies reporting offering products or services in this area.

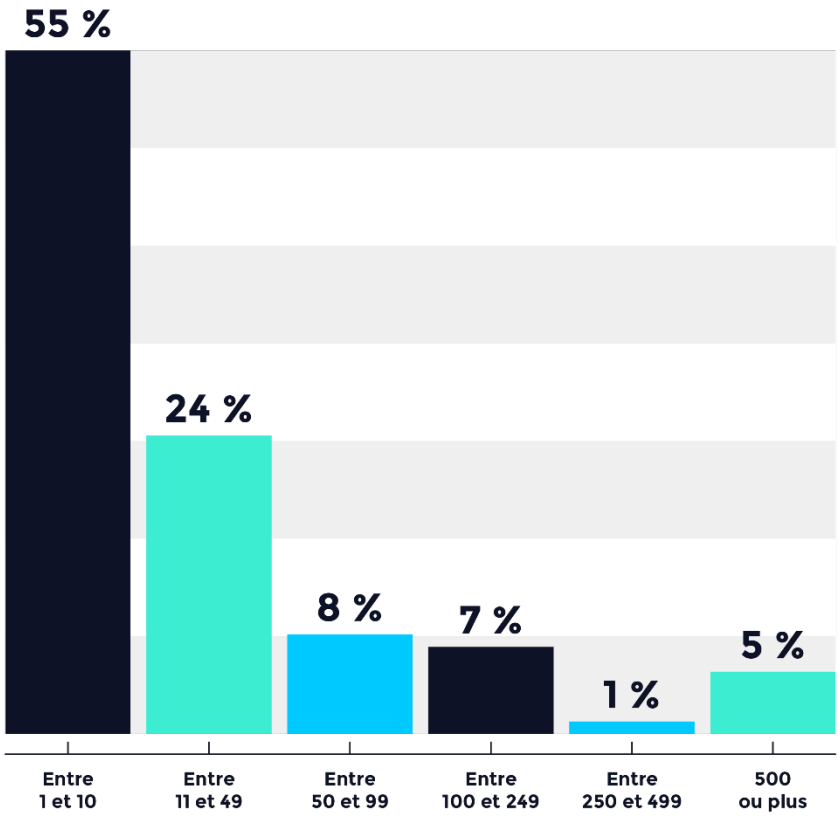
These results allow for the definition of a typology of active companies in the cybersecurity field and for measuring their economic impacts and added value.

[16] For this survey question, 43 responses were obtained. The total exceeds 100% since each company can apply its expertise in multiple fields simultaneously.

Type of Organization	Value Creation	Economic Impact
Producers of Specialized Software and Hardware Technologies	These companies directly contribute to technological innovation and economic development by creating high-tech products. They generate skilled jobs and stimulate R&D in the region.	Their success in exporting can improve the region's trade balance and strengthen its position as a technological leader.
Consulting Service Firms	These firms provide crucial expertise in assessing cybersecurity risks, designing tailored security strategies, and training personnel. They play a vital role in raising awareness and preparing businesses to face cyber threats.	Their work helps minimize economic losses due to cyberattacks and strengthen confidence in the digital ecosystem, which is essential for attracting investments across all sectors and ensuring stability in the operational capacity of organizations and government entities.
Resellers and Solution Integrators	By facilitating access to cutting-edge technologies and customizing cybersecurity solutions to meet clients' specific needs, these companies help democratize digital security.	They support the competitiveness of small and medium-sized enterprises (SMEs) by enabling them to access advanced security solutions, thereby contributing to overall economic resilience. They also allow Quebec's cybersecurity software and hardware technology producers to reach customers, addressing a critical need for market access.
Resource Leasing - Based on Short and Long-Term Requests (1 Month to Several Years)	These companies facilitate the matchmaking between employers and a workforce that may appear inaccessible, difficult to recruit, and retain.	They help fulfill unstructured demand.

2.2 Number of Employees and Workforce Characteristics

Of the 157 companies catalogued through the document analysis, the majority fit the profile of SMEs. Specifically, 54.7% have fewer than 10 employees, and 24.2% have fewer than 50 employees, with the remaining companies having more than 50 employees.



The sample of 47 companies surveyed showed a similar distribution, with 49% of companies having fewer than 10 employees, 34.1% having between 11 and 49 employees, and 12.8% having between 50 and 200 employees, suggesting that the more detailed responses regarding the workforce also fairly accurately reflect the state of the industry.

A primary observation from the survey concerning the workforce is that cybersecurity companies have experienced significant employee growth over the past two years, as illustrated in the table below. In an unsettled post-pandemic context, more than a third of cybersecurity companies (38.2%) recorded a personnel growth of over 31%, in a sector where we have seen that the workforce shortage represents a significant tension factor. Several adaptation strategies are being implemented by companies to respond to this positive pressure on their development.

Employee Growth Rates of Cybersecurity Companies from Quebec: 2021-2023

Growth Rate	Percentage (%) of Companies	Number of Companies
Over 100%	10.6%	5
51 to 100%	8.5%	4
31 to 50%	19.2%	9
21 to 30%	25.6%	12
11 to 20%	10.6%	5
1 to 10%	14.9%	7
No Growth or Negative	10.6%	5

The first strategy is the use of contractual employees to complement permanent staff. A majority of the companies surveyed employed contractual workers: 70.2% (33 companies) employed between 1 and 10 contract workers, 12.8% (6 companies) employed between 11 and 49 contract workers, 2.2% (1 company) employed more than 200 contract workers, and only 14.9% (7 companies) employed no contract workers. The use of contractual employees, through the flexibility it provides, allows cybersecurity companies to absorb the growth that accompanies the dynamism of this market.

A second adaptation strategy is the use of interns or students: 80.9% of the surveyed companies (38 companies) reported using this temporary workforce, which can also be the subject of recruitment offers when their skills match the organization's needs. For 68.5% of the companies (26 companies), these interns and students represented 1 to 10% of the workforce, while nearly a quarter of the sample (23.7% or 9 companies) accounted for between 10 and 20% of the workforce, a substantial share.

A third strategy deployed by cybersecurity companies is recruiting individuals from immigration, whether by facilitating the acquisition of open or closed work permits or tapping into the pool of permanent residents. Thus, more than a quarter of the surveyed companies (27.7% or 13 companies) employed more than 25% of their workforce from immigration, and another quarter (27.7% or 13 companies) employed between 10 and 24% of their workforce from immigration. Companies that had no employees from immigration accounted for only 19.1% of the sample. Cybersecurity companies from Quebec are thus embedded in international labor circulation networks that contribute to the diversity of their expertise.

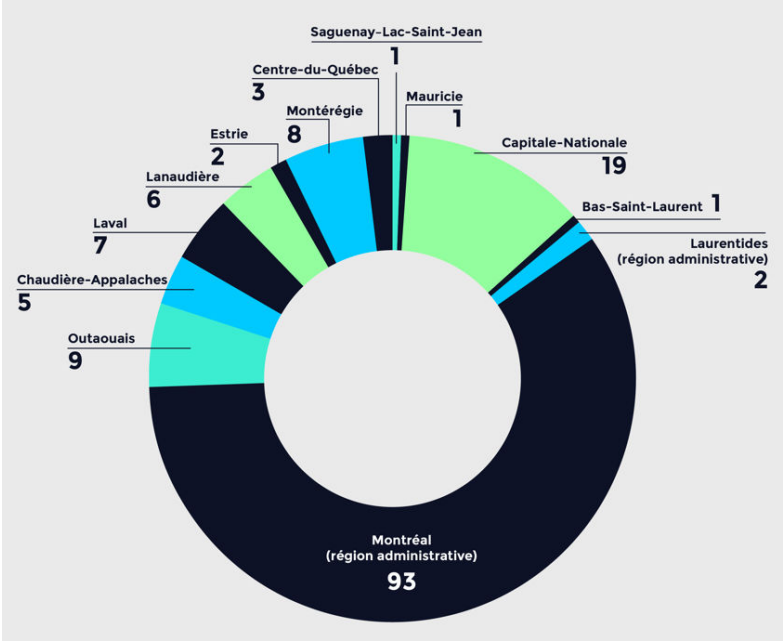
Despite all these efforts, nearly three-quarters of the companies (78.7% or 37 companies) still had positions to fill or were in the process of hiring, reinforcing both the observation of a growing market and a workforce shortage.

An additional factor that could help alleviate this workforce tension—but which remains largely underexploited—is increased participation of women within companies. The table below describes the proportion of technical roles occupied by women in the surveyed companies[4]. Nearly half of the companies (46.6%) had female participation rates of less than 5%, and a quarter of the companies did not have any women occupying technical cybersecurity roles.

Female Participation Rates in Technical Cybersecurity Roles

Participation Rate	Percentage (%) of Companies	Number of Companies
Over 25%	20.1%	9
21 to 25%	8.9%	4
16 to 20%	6.7%	3
11 to 15%	4.4%	2
6 to 10%	13.3%	6
1 to 5%	22.2%	10
0%	24.4%	11

2.3 Geographical Distribution of Companies



Within the document analysis sample, it is evident that the vast majority of cybersecurity companies are based in Montreal, a trend also observed in the survey sample, where companies headquartered in the Montreal metropolitan area (Montreal, Laval, and Longueuil) accounted for 55.2% of the respondents (32 companies).

2.4 Company History and Profitability of Their Activities

Although cybersecurity is a sector with relatively recent economic dynamism, more than half of the surveyed companies (53.2% or 25 companies) have been in operation for over 6 years (25.5% for over 15 years), while nearly a third (29.8% or 14 companies) have been in existence for 3 to 5 years. Startups operating for 2 years or less represent only 17% of the sample. This distribution reflects the historical evolution of cybersecurity, which was previously marketed under the term "computer security," then "information security," and whose rebranding allowed already well-established companies to improve their visibility in a context where cybersecurity issues are at the forefront.

In terms of profitability, more than three-quarters of the companies had generated a positive net result (55.3% or 26 companies) or had reached a break-even point between their revenues and expenses (19.2% or 9 companies). A quarter of the companies (25.5% or 12 companies) were, however, in a situation of negative net results. These figures must be considered in a context of strong growth activities, which can cause a temporary cash flow imbalance for companies investing in recruiting new employees and acquiring new clients.

As previously noted, the cybersecurity sector is experiencing strong growth, with figures well above the averages of other Quebec industries. Thus, between 2021 and 2023, nearly half of the companies (48.8%

or 23 companies) reported a net result growth rate of over 40%, while nearly one-fifth (19.1% or 9 companies) exceeded 100% net growth. The table below presents the distribution of companies in the sample according to the reported growth rates.

Net Result Growth Rates for 2021-2023

Net Growth Rate	Percentage (%) of Companies	Number of Companies
Over 100%	19.1%	9
51 to 100%	19.1%	9
41 to 50%	10.7%	5
31 to 40%	8.5%	4
21 to 30%	10.7%	5
11 to 20%	25.5%	12
1 to 10%	0.0%	0
No Growth or Negative	6.4%	3

These figures are to be compared with the evolution of real GDP by industry in Quebec, which grew by 6.0% in 2021, 2.8% in 2022, and 0.1% in 2023 for all goods and services industries combined[4]. They indicate how cybersecurity constitutes a reservoir of economic prosperity for Quebec, even within its reference sector of professional, scientific, and technical services, where its performances are evident.

Although more modest, export growth still represents a valuable contribution to Quebec's economy, especially for predominantly small and medium-sized enterprises. The table below describes the export growth of the surveyed companies during the 2021-2023 period. It is noted that more than a quarter (27.7% or 13 companies) of respondents experienced export increases of over 25%, and another quarter (27.7% or 13 companies) saw more modest increases of 1 to 10%, while nearly one-fifth (19.1% or 9 companies) even experienced stagnation or a decline in exports. These figures should be analyzed in light of Quebec's external trade statistics over these three years, during which exports of goods and services increased cumulatively by 18.6% (Government of Quebec, 2024: p. 13).

Export Growth Rates (Outside Quebec) for 2021-2023

Growth Rate	Percentage (%) of Companies	Number of Companies
Over 25%	27.7%	13
20 to 25%	6.4%	3
15 to 19%	10.6%	5
10 to 14%	8.5%	4
5 to 9%	14.9%	7
1 to 4%	12.8%	6
No Growth or Negative	19.1%	9

A more concerning result pertains to the stability of the shareholding of these companies, as a quarter of respondents (25.5% or 12 companies) planned to sell their companies within the next five years. It is difficult to verify whether these intentions have been realized or if steps have been taken in this direction, but one can deduce from the geographical distribution of the main competitors who the potential acquirers of these companies might be. Respondents indicated that their main competitors were located in Quebec (91.5% or 43 companies), the rest of Canada (74.5% or 35 companies), the United States (44.7%

or 21 companies), and to a lesser extent in Europe (36.2% or 17 companies). Therefore, there is a significant likelihood that companies from these three major markets may take control of companies that have developed expertise and skills in Quebec.

2.5 Intensity of Research and Development (R&D) Activities

A final aspect of the survey explored the practices of Quebec cybersecurity companies regarding research and development, a strategic area in a sector where the needs for innovation are constantly renewed under the combined pressure of factors such as the boundless creativity of malicious actors and the accelerated development of new technologies to secure (the Internet of Things, operational technologies, quantum computing, or artificial intelligence, to name a few). In this context, it is rather reassuring to note that 80.9% of respondents (38 companies) reported conducting research and innovation activities.

The intensity of these activities, measured as a proportion of annual operating costs, is also significant, as indicated in the table below[4], since more than half of the companies (52.6% or 20 companies) allocate more than one-fifth of their operating costs to research and innovation activities. These figures may seem excessive, but they reflect the intensity of innovation investments required in the digital technologies industry to remain competitive. A study conducted in the United States in 2019 found that software publishing companies invested on average between 17% and 26% of their annual revenues in research and innovation expenditures, depending on their growth velocity, with some companies aiming to conquer new markets not hesitating to invest up to 40% or 50% of their annual revenues in R&D (Ahlawat et al., 2019).

Research and Innovation Intensity of Cybersecurity Companies from Quebec: 2021-2023

Share of Research and Innovation in Operating Costs	Percentage (%) of Companies	Number of Companies
Over 25%	42.1%	16
20 to 25%	10.5%	4
15 to 19%	13.2%	5
10 to 14%	18.4%	7
5 to 9%	13.2%	5
1 to 4%	2.6%	1

Government assistance plays an important role in executing these activities, with just over half of the respondents (53.2% or 25 companies) reporting having benefited from it over the past three years. Among these beneficiaries, there is a clear preference for provincial programs, favored by 92% (23 companies), in contrast to federal programs, which were utilized in only 40% of cases (10 companies). These government aids are primarily allocated to general innovation-related expenditures such as the development of new products, processes, and procedures (80% of cases), R&D expenditures (68%), as well as marketing activities (60%).

In their research and innovation activities, Quebec companies appear to be much less frequently associated with universities, public research centers, or collegiate technology transfer centers (CTTCs). Less than a third of them (31.9% or 15 companies) reported having engaged with one of these

organizations, despite the significant number of research chairs and active cybersecurity resources in Quebec. Among the academic institutions most active in collaborations with this sample of 15 companies were Polytechnique Montréal (40% of cases or 6 companies), Concordia University (26.7% of cases or 4 companies), followed by Laval University, Université de Sherbrooke, and École de technologie supérieure (ETS) each with 20% of cases (3 companies).

3. INSTITUTIONAL ECOSYSTEM OF CYBERSECURITY IN QUEBEC

Regardless of their size, business model, workforce profile, degree of profitability, or the nature of their R&D activities, cybersecurity companies from Quebec operate within a complex organizational network composed of a diversity of public, private, and community actors whose interactions either facilitate or constrain their activities and innovation capabilities. In this sense, cybersecurity constitutes a true business ecosystem, a concept whose structure and functioning have been analyzed by scientific literature since the early 1990s (Moore, 1993).

Instead of studying the functioning of companies in isolation, this approach prefers to consider them as a community whose members cooperate or compete to develop and market innovative products and services. Other organizational actors, through their actions and capabilities, also strongly influence the performance of the entire ecosystem by enabling, for example, the establishment of a research infrastructure conducive to innovation, education a highly qualified workforce that can operationalize and commercialize this innovation on a large scale, mobilizing sufficient venture capital to foster the emergence and growth of digital startups, or developing regulatory frameworks that will accelerate the adoption of certain products or services. Thus, we are dealing with a "large-scale cooperation architecture" (Moore, 1996), whose mapping is necessary to better understand the levers that can be used to strengthen the effectiveness of the entire ecosystem and its constituent parts.

The systematic study of the Quebec ecosystem, whose contours are outlined in this report, is based on nine major categories of interdependent entities. This typology is inspired by research conducted on innovation and governance ecosystems in cybersecurity (Deloitte, 2016; Dupont, 2024) and allows for an understanding of the complementary capabilities mobilized by each of the major categories to build robust collective cybersecurity.

- Cybersecurity Companies
- Private Buyers
- Insurers
- Public Buyers
- Cybersecurity Support Organizations
- Education and Research Organizations (Academic World)
- Investors & Incubation and Acceleration Infrastructures
- Regulatory Authorities
- Professional Associations and Community Groups

For each category, a brief description of its role in the ecosystem is provided, along with some Quebec-specific highlights.

3.1 Cybersecurity Companies

The previous section provided a recent overview of Quebec cybersecurity companies, so there is no need to revisit it in detail. We conducted a mapping (see Appendix 2) of the companies, attempting to categorize them according to their primary area of activity. These companies can be classified according to a taxonomy developed by Cybereco[4], an overview of which is provided below. This taxonomy is particularly suited to describe the expertise of the Quebec ecosystem in order to develop *a common language for proper categorization and to have a shared appreciation of the sector in efforts to develop solutions targeting the cybersecurity industry, notably measures supporting commercialization, export, or innovation* (Pascal Fortin, Cybereco).

3.2 Private Buyers

The category of private buyers includes small and large businesses that consume the products and services marketed by cybersecurity companies. These companies are therefore the originators of demand in this dynamic market, and through their purchasing power, needs, and requirements, they dictate the types of solutions and technologies that vendors must develop. Within this category, two subgroups must be distinguished: large enterprises and SMEs.

Large enterprises generally have comfortable budgets and sizable teams to acquire and deploy cybersecurity solutions, especially when they belong to sectors operating critical infrastructures such as financial services, energy, telecommunications, or transportation. For example, the average consolidated costs related to purchasing cybersecurity products and services were CAD 601,000 in 2021 for large Canadian enterprises, compared to CAD 7,950 for small businesses, according to Statistics Canada[4]. Thus, large enterprises play a central role in the cybersecurity ecosystem and influence the practices of this ecosystem.

The status of small and medium-sized enterprises – which represent nearly 98% of Quebec companies – in this ecosystem is much more marginal, despite the importance of cybersecurity for maintaining their daily operations. These companies are indeed slow to adopt cybersecurity solutions that could protect them against emerging risks, and are therefore vulnerable to the most common attacks such as ransomware, phishing, or CEO fraud. The main cause of this disinterest is the lack of financial resources, which hinders the acquisition of solutions and the recruitment of competent cybersecurity employees. The lack of expertise also complicates the outsourcing of cybersecurity functions to external providers who rarely offer technical solutions adapted to the reality of SMEs. Indeed, cybersecurity is a sector where promises made by marketing services rarely rely on evidence-based data and where exaggerations hinder informed decision-making. SMEs are particularly ill-equipped to analyze and interpret these hyperbolic claims. Not knowing where to start their long journey toward a more robust cybersecurity state, many SMEs simply choose to ignore the problem until a crisis disrupts their operations (Westin et al., 2022). Thus, in 2021, only 14.2% of Canadian small businesses had a written policy to manage cybersecurity risks, compared to 62.7% of large enterprises that had undertaken this process[4].

3.3 Insurers

Insurance companies represent a distinct category in the cybersecurity market, as they offer both a service to private buyers (coverage allowing the transfer of the negative impacts of incurred risks to a third party that contributes to their financial mitigation) while also serving as a powerful intermediary between these same buyers and cybersecurity companies.

Insurers play a key role in the functioning of the cybersecurity ecosystem through five main mechanisms:

- First, when subscribing to an insurance policy, insurers meticulously assess the risks to which their clients are exposed and their security posture, in order to identify weaknesses and vulnerabilities to be corrected before finalizing the contract;
- Second, they can offer financial incentives in the form of premium reductions in exchange for clients' investments in improving their cybersecurity, although this approach remains difficult to implement;
- Third, insurers impose minimum security requirements on their policyholders, such as activating multi-factor authentication or implementing an incident response plan;
- Fourth, they provide their clients with specialized service providers in the event of a major incident, offering legal services, crisis management, forensic expertise, and communication services;
- Finally, the fifth lever of influence for insurers lies in their accumulation of data and knowledge about effective cybersecurity practices and technologies. They use this information to pre-select

[4] Retrieved from https://www150.statcan.gc.ca/t1/tbl1/fr/tv.action?pid=2210013001&pickMembers%5B0%5D=3.1&pickMembers%5B1%5D=4.4&cubeTimeFrame.startYear=2019&cubeTimeFrame.endYear=2021&referencePeriods=20190101%2C20210101

high-performing solutions and offer more advantageous contractual conditions, or to establish awareness and education programs for their clients (Dupont, 2024).

Overall, insurers exert a significant influence on the cybersecurity ecosystem through governance mechanisms ranging from risk assessment to knowledge dissemination, including financial incentives, imposing requirements, and crisis support. Their role as *ad hoc* regulators and data aggregators helps shape practices and innovations in this field.

Although the insurance industry is generally well-developed in Quebec, particularly in the Quebec City region, which hosts about ten insurance company headquarters, it does not appear that cyber insurance represents a particularly dynamic growth pole. However, the potential seems full of promise, as only 46.5% of large Canadian enterprises, 24.4% of medium-sized businesses, and 13.7% of small businesses had subscribed to cyber risk insurance in 2021[5].

3.4 Public Buyers

Public organizations play a central role in the cybersecurity ecosystem due to the size and extended duration of the contracts they can offer to cybersecurity companies to protect government informational assets. The sensitivity of the data that must be secured also ensures that the needs of public buyers meet higher standards than their private counterparts (particularly in the security and defense sectors), ultimately resulting in the development of more advanced expertise among their suppliers.

Through their tendering strategies, public buyers can also promote the development of certain categories of companies by, for example, reserving a proportion of their contracts for startups – which allows these companies to establish a reference clientele that can reassure their investors and open doors to new markets – or for local businesses, thereby strengthening their offerings and fostering innovation in the face of multinational companies whose size sometimes acts as a distortion factor in competition, hindering the emergence of a national industry.

The creation of the Ministry of Cybersecurity and Digital (MCN) in Quebec in 2022 and the publication in July 2024 of the Governmental Cybersecurity and Digital Strategy 2024-2028 thus constitute powerful levers to outline and frame the procurement practices of public organizations with the dual objectives of efficiency and effectiveness.

[5] Retrieved from https://www150.statcan.gc.ca/t1/tbl1/fr/tv.action?pid=2210013001&pickMembers%5B0%5D=3.1&pickMembers%5B1%5D=4.3&cubeTimeFrame.startYear=2019&cubeTimeFrame.endYear=2021&referencePeriods=20190101%2C20210101

3.5 Investors & Incubation and Acceleration Infrastructures

Supporting entrepreneurs who wish to offer innovative cybersecurity products and services largely depends on the availability of venture capital necessary to ensure the growth of startups. Beyond capital, investors strategically guide entrepreneurs toward the most promising segments of a highly competitive market, connect them to business opportunities or partners with complementary expertise, and foster the emergence of a corporate culture that combines agility and profitability.

In Canada, the total amount of venture capital investments made in 2023 (across all sectors) amounted to nearly CAD 7 billion, with 48% concentrated in Ontario and 20% in Quebec (CVCA, 2024). The year 2024 appears to follow an identical trajectory, with over CAD 3.8 billion in investments recorded during the first six months (CPE Media & Data Company, 2024). It is not possible to quantify the proportion of these investments that pertain to cybersecurity, but some recent announcements in Quebec include Inscora (CAD 2 million in funding announced in August 2024), Mondata (CAD 17 million in funding announced in July 2024)[7], Qohash (CAD 17.4 million announced in April 2024)[8], Flare (CAD 12.5 million raised in 2022)[9], and Terranova (CAD 9 million in funding in 2021)[10].

Analysis of the origin of the investments made further indicates that 55% of venture capital comes from American companies. Regarding Canadian private funds, they heavily rely on investments made by the federal government and its provincial counterparts, making the Canadian venture capital industry a "quasi-governmental entity" according to some observers (CPE Media & Data Company, 2024).

Incubators and accelerators are structures that offer support in terms of mentorship, resources, and networks, in addition to the initial funding sometimes available for startup companies. They help young businesses refine their business models, test their products, and prepare for larger fundraising rounds. According to the Quebec Innovation Accelerators Movement, there are over sixty incubators and accelerators in the province, but only three, to our knowledge, have developed specialized tracks in cybersecurity. The organization Cilex, based in the Gatineau region, launched a cybersecurity networking program in January 2023 that leverages local resources specialized in security and digital identity[7]. This one-year program welcomed a first cohort of six startups. In Montreal, the Propolys program at Polytechnique Montréal offers a ten-month specialized entrepreneurial track in cybersecurity, enabling ten projects to launch their companies[8]. Finally, the organization Cybereco launched its Carrefour Cyber in November 2023, which aims to become an innovation and commercialization complex focused on the cybersecurity of essential infrastructures. Carrefour Cyber hosts about ten cybersecurity startups and scale-ups, providing them with opportunities to cultivate their business networks[9].

3.6 Cybersecurity Support Organizations

Two major categories of organizations also contribute to the funding of research and innovation, support for entrepreneurship, and the formation and consolidation of technological clusters that contribute to the growth of a robust cybersecurity ecosystem. Some of these organizations belong to the public sector, while others are non-profit organizations (NPOs).

3.6.1 Public Organizations

Provincial and federal ministries of economy and innovation have generic and specific support programs to bolster the cybersecurity ecosystem. For instance, the Ministry of Economy, Innovation, and Energy announced financial assistance of CAD 3.5 million to the In-Sec-M cluster in April 2023 as part of its strategic Offensive in Digital Transformation (OTN) initiative, enabling the cluster to offer cybersecurity awareness and education activities to Quebec companies across all industries[6]. The federal government, on its part, released CAD 80 million in February 2022 to fund the Cybersecurity Innovation Network, whose mandate is to intensify research and development, increase commercialization, and train specialized cybersecurity personnel[7].

Public support funds and programs can also be included in this category of actors, whether through recurring programs designed to support companies and universities developing innovative solutions, such as the federal government's[8] IDEeS (Innovation for Defense, Excellence, and Security) program, or through one-time initiatives like the decision by Quebec's Chief Scientist to allocate CAD 2.5 million to the University of Quebec in Outaouais in October 2023 to create a research and innovation center in cybersecurity and society[9].

The cybersecurity ecosystem can also benefit from the support of government organizations through programs aimed at accelerating the development of emerging technologies such as artificial intelligence or quantum computing, for which various levels of government have allocated substantial resources in recent budget cycles. These investments will propel the next generations of cybersecurity solutions.

3.6.2 Non-Profit Organizations

Furthermore, public organization support in Quebec is relayed and amplified by two industry clusters co-funded by the private sector and various levels of government: Cybereco and In-Sec-M. The primary mandate of these two organizations is to structure and promote the expertise of local companies. Equipped with boards of directors that represent the ecosystem in all its diversity, they can rely on dozens of active members who engage in activities aimed at accelerating the development of a vigorous and innovative Canadian cybersecurity ecosystem. These two clusters offer, for example, according to their respective missions, communities of practice to their members, large conferences bringing together all ecosystem actors, overseas business development missions, tools and support programs for SMEs, as well as innovation tracks for startup entrepreneurs and initiatives aimed at developing the cybersecurity talent pool[6].

Another NPO contributing to ecosystem support is PROMPT, an industrial research sectoral grouping (RSRI) specializing in the digital technologies sector, which since 2019 has allocated over CAD 44.5 million to finance more than 150 business projects under the PICQ1 and PICQ2 programs (Quebec Cybersecurity Innovation Program) (PROMPT, 2023). The funding provided comes from the Ministry of Economy, Innovation, and Energy. PROMPT collaborates closely with other ecosystem actors to offer tailored and evolving funding based on industry needs.

[6] For more information, see https://cybereco.ca/ and https://insecm.ca/.

3.7 Education and Research Organizations (Academic World)

Quebec universities and colleges have established world-class research centers and units that contribute to the development of technologies, processes, and best practices capable of strengthening cybersecurity, even though it appeared in the previous chapter that the links between the academic world and cybersecurity companies could benefit from deeper collaborations.

Three universities notably stand out with a critical mass of cybersecurity researchers from diverse disciplines united within federating entities: Concordia University and its cybersecurity research hub bring together 18 professors, including three heads of industrial research chairs from the National Research Council of Canada (NRC)[7]. Université de Sherbrooke founded the Interdisciplinary Cybersecurity Research Group (GRIC), which mobilizes 20 professors from five different faculties and schools (sciences, engineering, law, management, and political science)[8]. Finally, Polytechnique Montréal, Université de Montréal, and HEC Montréal have created the Multidisciplinary Institute in Cybersecurity and Cyberresilience (IMC2), which brings together 45 professors from the three institutions[9].

More concentrated expertise hubs also exist at Université Laval, which hosts a research chair on cybersecurity governance and management, jointly funded by Microsoft and the Ministry of Cybersecurity and Digital (MCN)[7], as well as the cybersecurity and societal impacts expertise hub at OBVIA[8]; at UQAM, with the Canada Research Chair in Privacy-Respecting Big Data Analysis and Ethics and the Cybersecurity Research Group[9]; at McGill University, with the Canada Research Chair in Data Mining for Cybersecurity[10]; at UQO, which hosts a Computer Security Research Laboratory led by three professors; and at UQAC with the Institutional Research Chair in Cyberdefense and Personal Data Protection[11].

The Cégep de l'Outaouais also founded in June 2018 a collegiate technology transfer center (CCTT) specializing in cybersecurity named CyberQuébec, whose main areas of intervention include cybersecurity and digital transition support services for SMEs, awareness, and to a lesser extent, applied research[7].

Moreover, colleges and universities contribute to workforce education by creating undergraduate, master's, and doctoral programs designed to meet employers' needs and the evolving required skills. A mapping effort initiated by the Integrated Cybersecurity Network (SERENE-RISC) in 2018 and updated by IMC2 in 2024 reveals the existence in Quebec of 34 education programs accessible at the collegiate and university levels, offering more than 300 courses covering the technical, organizational, legal, and social aspects of cybersecurity[8].

[7] Retrieved from https://cyberquebec.org/wp-content/uploads/2024/02/Planification-quinquennale-2024-2029-de-CyberQuebec.pdf.
[8] Retrieved from https://www.serene-risc.ca/fr/repertoire-des-programmes-en-cybersecurite.

3.8 Regulatory Authorities

In the face of increasing insecurity, governments have a role to play in limiting and mitigating the risks associated with cyberspace and new technologies (Montreal Institute of International Studies, 2020, p. 1). In recent years, states have implemented new legislative and regulatory measures to govern cyberspace and strengthen the protection of citizens. These new frameworks have significant implications for the cybersecurity industry. Indeed, they encourage organizations to adopt additional security measures and adopt more proactive approaches to protect the personal data they hold.

3.8.1 Quebec Context

At the provincial level, in 2019, the Government of Quebec established the *Government Cyberdefense Center* as part of the Treasury Board Secretariat and, since 2022, the Ministry of Cybersecurity and Digital. "The Government Cyberdefense Center acts as a trusted entity within the government cyberdefense network. Its responsibilities include coordinating the cybersecurity efforts of public organizations and cyberdefense operational centers, managing security incidents at the governmental level, and playing a collaborative role within the Quebec, national, and international cybersecurity ecosystems" (Fortin et al., 2021). The following year, in 2020, the Government of Quebec published its Government Cybersecurity Policy, which emphasized the openness and sharing of knowledge, expertise, and best practices in cybersecurity (Fortin et al., 2021). On January 1, 2022, the Government of Quebec created the Ministry of Cybersecurity and Digital, tasked with leading and coordinating state actions in the fields of cybersecurity and digital technologies.

Later, in September 2022, the adoption of Law 25 compelled all private organizations to demonstrate greater transparency in the collection and use of personal information, increased legal obligations and corporate responsibility in this area, required them to disclose cyberattacks and incidents threatening personal data, and introduced harsher penalties for non-compliance (Groupe Novipro and Léger, 2023). This strengthened regulatory framework pushes organizations to consolidate their cybersecurity measures, improve incident management processes, intensify employee awareness and education, and engage cybersecurity experts. The various provisions of Law 25 have been gradually phased in over a three-year period, making it still difficult to analyze their direct and indirect impacts on the cybersecurity market. The Information Access Commission (CAI) is the authority holding the evaluation and sanctioning powers provided by the law, which also publishes information regarding reported privacy incidents.

Sector-specific regulatory authorities, such as the Financial Markets Authority (AMF), also incorporate cybersecurity into their monitoring and control activities, thereby defining the measures to be taken to reduce exposure to cyberattack risks[9].

3.8.2 Federal Context

At the federal level, in 2018, the Canadian government established a National Cybersecurity Strategy (Public Safety Canada, 2018). As a result of this strategy, the same year saw the creation of the Canadian

[9] Retrieved from https://lautorite.qc.ca/professionnels/obligations-et-formalites-administratives/protection-des-donnees-et-des-renseignements-personnels.

Centre for Cybersecurity (CCC) (Canadian Centre for Cybersecurity, 2022). "As Canada's technical authority on cybersecurity, the CCC team leverages its expertise to protect the information and systems Canadians rely on every day" (Canadian Centre for Cybersecurity, 2022). In addition to providing guidance to businesses of all sizes and the general public, the CCC collaborates with operators of essential infrastructures to help secure their systems. Strategic partnerships are formed with cybersecurity companies to evaluate emerging technologies entering the market. Notably, the CCC collaborates with the Build in Canada Innovation Program, acting as a technical authority to support cybersecurity companies seeking to commercialize innovative products[10].

More stringently, certain sector-specific federal regulatory authorities are establishing increasingly precise cybersecurity requirements that regulated entities must comply with. For example, the Office of the Superintendent of Financial Institutions (OSFI) published its guidelines on technology risk and cyber risk management in July 2022, detailing the organizational and technical measures that banks and insurance companies must implement to be deemed compliant[11]. In the telecommunications sector, the Canadian Radio-television and Telecommunications Commission (CRTC) is responsible for overseeing telecommunications service providers[12]. Its regulatory activities related to cybersecurity have focused in recent years on combating the widespread dissemination of online spam and the spread of malware by blocking botnets (computer systems infected without the knowledge of their legitimate owners) on the one hand, and on enhancing the resilience of communication systems on the other (CRTC, 2023). Through their increasingly detailed cybersecurity requirements, these regulatory authorities push regulated entities to revise their internal policies, enhance their technical capabilities, and acquire more effective solutions in the market for products and services.

Finally, the federal Parliament is currently reviewing Bill C-26, which is in second reading in the Senate and would strengthen the cybersecurity regulatory framework to which four sectors deemed essential to the economy would be subject: telecommunications, finance, transportation, and energy. Operators from these four sectors would be required to comply with new obligations in four areas: developing and implementing cybersecurity programs; mitigating risks related to the digital supply chain; reporting security incidents; and complying with any ministerial directives related to cybersecurity[11].

3.9 Professional Associations and Volunteer Initiatives

The final category of ecosystem actors includes professional associations, non-profit organizations (NPOs), and community groups that organize activities contributing to the sharing and mobilization of knowledge.

Professional associations such as ISACA[12], ISC2[13], ASIMM[14], and ASIQ[15] offer their members networking activities, events such as seminars and conferences that foster knowledge exchange, as well as certification programs that allow cybersecurity professionals to demonstrate their expertise according to internationally recognized standards. Their existence thus promotes the informal circulation of

[10] Retrieved from https://www.cyber.gc.ca/fr/propos-centre-cybersecurite/collaboration-avec-secteur-prive.
[11] Retrieved from https://www.parl.ca/legisinfo/fr/projet-de-loi/44-1/c-26.

information between cybersecurity companies and their clients, as well as among buyers who wish to share their experiences with specific suppliers.

Organizations like CyberCap[12], École Cybersécurité[13], and Co-savoir[14] disseminate education and awareness content related to major cybersecurity issues to segments of the population that are not directly in contact with sector companies. However, these groups need to improve their knowledge to maintain adequate protection against digital risks or to take advantage of professional opportunities in the sector. For example, CyberCap has developed, in collaboration with Cybereco, a education program for high school students that encourages the adoption of safe online behaviors while sparking their interest in cybersecurity and digital professions. This education was attended by over 6,200 students aged 12 to 17[15]. Meanwhile, École Cybersécurité offers more technical education accessible online, created a directory of female cybersecurity experts to enhance the visibility of women in the field, and annually awards the Cybertalent trophy to inspire careers and recognize inspiring pathways among individuals under 30[16]. In a different vein, Co-savoir (formerly the Documentation Centre on Adult Education and the Feminine Condition) developed a toolkit tailored to the needs and capabilities of community organizations wishing to strengthen their digital security and the confidentiality of the data they process[17]. These three examples are not exhaustive, and many other initiatives exist in Quebec. However, they are not centrally cataloged, which limits their visibility.

A significant contribution is also made by ethical hacking competitions and conferences on the latest vulnerabilities, attacker evolution, or best security practices. These events, which can be described as community-driven due to the educational and inclusivity values they promote, are organized by volunteer teams who dedicate many hours to designing challenging events and diverse programs that bring together several hundred participants. Although these events do not have commercial aims, they contribute to consolidating cross-cutting links between various ecosystem entities and strengthening workforce skills. Among the more reputable events are NorthSec[12], MontreHack[13], and BSides[14] in Montreal, and HackFest[15] and SéQCure[16] in Quebec City. These initiatives complement professional conferences organized by industry clusters or private companies, such as the ITSec Summit, InCyber Forum, GoSec, or the Cyber Conference.

3.10 Some Comparison Elements with World-Class Ecosystems

As part of its international development missions, the technological cluster In-Sec-M has had the opportunity to deepen its understanding of the functioning of other cybersecurity ecosystems in the United States, Israel, France, and Germany (see the summary analyses in Appendix 1). The following paragraphs identify the strengths leveraged by ecosystems deemed the most globally effective, based on this field knowledge. These characteristics are selectively examined in light of the properties of the Quebec ecosystem to draw useful lessons for it.

Five main factors seem to explain the vigor of cybersecurity ecosystems deemed the most performant. The first is a strong governmental commitment to coordination through national strategies that enable all actors to understand their roles and access interlocutors with the resources to facilitate cooperation and synergistic initiatives. Canada indeed has a national cybersecurity strategy, but it dates back to 2018, and

the new version of this strategy has not yet been made public at the time of writing. Quebec also adopted a Government Cybersecurity and Digital Strategy for the period 2024-2028 in the summer of 2024, but its objectives and means remain focused on public services.

A second success factor concerns the establishment of structures that promote entrepreneurship in cybersecurity. For example, Israel defines itself as the "Startup Nation" and values this culture of entrepreneurship both among its innovators and foreign investors. The United States has established renowned incubators and accelerators that attract entrepreneurs from around the world to Silicon Valley or the suburbs of Washington. France, on the other hand, has designed the "France Cybersecurity" label to promote French cybersecurity solutions internationally and to differentiate the offerings of its entrepreneurs in this highly competitive market. All these examples involve considerable steering efforts from public authorities or private investors.

A third factor relates to massive investments in research and development (R&D) by governments using various channels: defense sector agencies in the United States (DARPA) and Israel (Unit 8200), research institutes dedicated to fundamental and applied research in France (INRIA and CEA) or Germany (Fraunhofer Institute). In all cases, strategies aimed at creating critical masses of research excellence are being implemented, whereas Canada and Quebec tend to prefer a more fragmented distribution of resources.

A fourth factor is the existence of world-class education systems and universities that offer reputable cybersecurity programs, whether it involves conducting applied research projects or eduction highly qualified experts. Parallel education mechanisms, such as professional certification programs or ongoing education provided within certain military or intelligence units, also play an important role. In Quebec, education hubs are emerging at the collegiate and university levels, but it is still difficult to assess the quality of the programs offered and their real alignment with the ecosystem's needs.

A fifth and final common factor among high-performance cybersecurity ecosystems is the encouragement of formal collaborations between public and private actors. France, for instance, created a Cyber Campus in early 2022 in Paris, which also played a catalytic role by bringing together companies, public services, and educational and research institutions in a building where nearly 280,000 square feet are dedicated to cybersecurity. Israel, for its part, inaugurated its CyberSpark campus in the Negev Desert in the mid-2010s, where entrepreneurs, researchers, and military personnel coexist. The United States developed a set of intelligence-sharing programs around the Cybersecurity & Infrastructure Security Agency (CISA), which consolidated exchanges that had already existed since the late 1990s among operators of 27 industries deemed essential through the Information Sharing and Analysis Centers (ISACs)[12] system. These initiatives promote the agility of partnerships that can quickly respond to changing ecosystem conditions and seize new opportunities as they arise.

These five factors illustrate the central role that public and quasi-public actors play in creating and maintaining a robust cybersecurity ecosystem capable of meeting national needs and standing out in international markets. This role involves seeking a delicate balance between coordination efforts based on a shared vision and the injection of significant resources, on one hand, and the valorization of the skills

and capabilities of other ecosystem actors, who must be able to maintain substantial initiative margins to develop innovative approaches.

4. CHALLENGES AND OPPORTUNITIES FOR THE CYBERSECURITY INDUSTRY IN QUEBEC

For certain survey questions, cybersecurity companies had the option to supplement their response choices with qualitative details about the main challenges they face. Additionally, four in-depth interviews were conducted with company leaders who participated in the survey. This section of the report presents the main insights drawn from these responses[12].

4.1 Talent and Skilled Workforce[13]

The survey results reflect what was observed in the documentary review. According to the survey and interviews, the workforce presents five main challenges to respondents, presented in descending order of frequency in the responses.

Firstly, the most frequently mentioned challenge is employee retention, appearing in 38.9% of responses (14 companies)[14]. Respondents find it difficult to retain trained employees, particularly in a context where they are competing with large companies that can offer higher salaries, attractive working conditions, and appealing promotion opportunities. This intense competition for a limited pool of human resources makes it challenging to retain certain expertise, resulting in high turnover rates for several positions.

Similarly, in response to this market reality, 36.1% of respondents (13 companies) express that compensation is also a challenge. The high cost of specialized labor and the aggressive salary demands of potential employees represent particularly thorny challenges for startups. They find it difficult to compete with the salary offers of large industry companies, especially since the latter are willing to recruit employees for remote work in areas where they do not have physical offices.

Recruiting qualified talent in a context of shortage is a third issue to overcome for 27.8% of respondents (10 companies). The job market does not seem to have a sufficient quantity of qualified resources, and Quebec cybersecurity companies struggle to find candidates who meet their needs. Certain areas of expertise appear to be particularly affected by this shortage. Small and medium-sized enterprises, whose

[12] In order to facilitate the analysis of unstructured data and to limit selection and interpretation biases, the qualitative data were coded and categorized according to thematic analysis principles using two generative artificial intelligence applications: ChatGPT 4.0 and Claude 3.5. The data were first anonymized, then ingested by both models, accompanied by directives asking them to identify the main themes present in the responses and to classify them based on their frequency of occurrence within the identified themes. Using two models instead of one allows for comparing results and retaining only those that reach consensus, that is, the most robust. The results were then cross-verified to ensure their integrity and to detect any possible errors introduced by the models.

[13] Challenges and Opportunities Related to the Workforce within Cybersecurity Companies in Quebec (Number of survey respondents: 36).

visibility in the market is less than that of their international rivals, also struggle to attract the attention of competent recruits.

Training and skills development represent a fourth challenge for 16.7% of respondents (6 companies). Since some respondents find it difficult to find fully qualified employees, they must offer internal training. However, the associated costs and the time required to train employees impact other business activities and can temporarily hinder innovation and commercial development when resources are limited.

Finally, immigration and international mobility pose an issue for 5.6% of respondents (2 companies). Companies that resort to this approach seek to address the local labor shortage, but one respondent who turned to this solution mentioned the cumbersome process. Another company also indicated plans to establish offices abroad to offer an international mobility and remote work program for certain tasks. However, resource limitations are anticipated for small and medium-sized enterprises.

Despite these challenges, some respondents find solutions and opportunities for their companies in recruitment and retention. For example, one respondent now recruits across Canada since their company is virtual, even though this can generate related challenges such as a reduced sense of belonging. Another focuses on company culture to attract and retain employees. Although this practice is resource-intensive, some respondents hire students and interns with the aim of retaining them within their company. This practice was also noted by two interview participants. Another respondent even proposed the following solution: "obtain grants to fund training, which would create loyalty. This would allow us to free up between 200 and 300 hours, or about 10% of an employee's time, for example, which would be very useful, especially for junior workforce".

4.2 Research and Innovation in Cybersecurity in Quebec[14]

Regarding partnered research, the main constraints reported by survey respondents are related to the long bureaucratic delays resulting from interactions with universities or support organizations, the alignment of priorities and objectives between various partners, issues related to intellectual property management, and the lack of resources. Delays deemed excessive for establishing partnerships and finalizing projects do not align with the speed at which the sector evolves and constitute an irritant for 27% of respondents (10 companies), whether these delays are experienced during the partnership setup phase, their daily management, or when it comes time to generate quick results. This mismatch between the need for responsiveness from companies and the much slower academic timelines is clearly a deterrent for businesses.

The lack of alignment between the needs of the academic world and those of companies also causes frictions that discourage 22% of respondents (8 companies). By this, companies mean the gap between

[14] Main Constraints to Establishing Research and Innovation Activities with an Academic or Private Partner (Number of survey respondents: 37) and Issues Related to Research and Innovation Investments within Companies (Number of survey respondents: 36).

their needs for applied research and the fundamental research interests of their academic partners, the identification of reliable academic partners, or the radical cultural differences between the two communities.

Intellectual property management also poses challenges for companies collaborating with the academic world, with 19% of respondents (7 companies) viewing it as an issue. In particular, the stringent constraints imposed by universities on the use of intellectual property developed in partnership are perceived as a barrier to its sharing. This seems to create a cascading effect, stretching delivery timelines for cybersecurity companies and creating commercial uncertainty for them.

Facing these three major categories of complications and the bureaucratic delays that result, respondents find themselves confronted with costs they find difficult to justify and bear. Insufficient financial resources are mentioned by 16% of respondents (6 companies), and this seems to include funding obtained from government sources to support such projects, which are deemed insufficient in the face of the actual costs incurred by their implementation.

4.3 Innovation Funding

When it comes to innovation, the main issue raised by survey respondents is funding. Transforming innovation into capital can take time. The return on investment is not guaranteed. 34% of respondents (16 companies) report challenges related to financing and access to capital, which hinder their innovative drives.

Government support is also a concern for respondents, who note that aid programs are complex and poorly adapted to the reality of startups. The unpredictable renewal and changing criteria of the programs can also create instability for companies. Government incentives require significant time investments due to their administrative burden during the preparation of applications, which proves prohibitive according to several respondents. Additionally, some respondents find it difficult to navigate a diverse range of programs. These comments seem to indicate that the central issue concerns the adequate targeting of these programs and their overall coherence, rather than the volume of support available.

Government policies can influence company behavior in two opposite ways:

Advantages	Disadvantages
▪ Stimulate Innovation: Investments, tax measures, and grants can encourage research and development in the field of cybersecurity, fostering innovation	• Dependence on Grants: Over-reliance on government aid can make cybersecurity companies vulnerable to policy changes and less inclined to

and maintaining a highly skilled workforce. ▪ Increased Security: By making cybersecurity solutions more accessible and affordable for public and private organizations, the government contributes to the protection of critical infrastructures and data security. ▪ Economic Development: These measures can attract cybersecurity companies and talent to a region, thereby stimulating the local economy and positioning it as a center of excellence in cybersecurity.	innovate and compete in the free market. • Resource Allocation: There is a risk that grants are not always allocated to the most deserving or effective projects, which could result in the misallocation of public funds. • Market Distortion: Government interventions can sometimes distort the market, favoring certain companies or technologies over others and inhibiting healthy competition.

To maximize benefits and minimize disadvantages, it is crucial that government measures are well-designed, targeted, and implemented in a transparent and equitable manner. Close collaboration with industry, academic institutions, and other stakeholders is essential to ensure that policies effectively support the existing ecosystem and take into account the constantly evolving threats and technologies required to address them.

4.4 Commercialization: Challenges and Issues[15]

When asked about the biggest challenges related to offering cybersecurity services or products, respondents highlighted three major challenges particularly associated with commercial interactions with government buyers and large contractors. Firstly, the complexity and prolonged timelines of tender processes are reported by 44% of respondents, who lament the administrative burden associated with these processes and the very long decision-making delays, which prohibitively extend sales cycles for SMEs.

A second challenge concerns the selection criteria applied by large contractors to choose their cybersecurity suppliers, which do not seem aligned with the reality of SMEs: 35% of respondents believe that the rigidity of the criteria used does not match a very dynamic and constantly evolving risk landscape, that the focus on price rather than quality of services hinders the deployment of effective solutions, and that the qualification requirements to participate in tenders are excessive and discouraging for SMEs. According to respondents, this results in a reluctance of large contractors to trust startups and a preference for solutions offered by established large companies.

[15] Barriers to Offering Cybersecurity Services or Products in Quebec (Number of survey respondents: 44); Specific Challenges in the Sales Process to Government Buyers or Major Clients (Number of survey respondents: 34); and Barriers to Profitability for Cybersecurity Companies in Quebec (Number of survey respondents: 12).

These tender characteristics induce 18% of respondents to feel that local SMEs are disadvantaged in favor of large American companies and that the most profitable segments of the cybersecurity market are not accessible to them. In interviews, a responding company also addressed this issue: "The probable cause is the image of Quebec products; buyers assume that we are not up to the task. It's a very serious perception problem." Similarly, an interview participant described how this market dynamic impacts their company: "Regarding market dynamics, Canada can be a difficult place to launch a cybersecurity company. The trend is to buy products from the United States from large companies, which means we need to already sell in the U.S. before expanding in Canada. Commercialization issues are related to capital, which limits the development of our company."

If access to the large contractors' market is challenging, that of SMEs also raises a number of challenges that constitute obstacles to growth and profitability for cybersecurity companies. The first of these challenges is client awareness and education, according to 19% of respondents. Cybersecurity risks remain perceived as distant for the majority of SMEs, and it is difficult for cybersecurity companies to convince potential clients of the importance of investing in technologies that do not provide immediate revenues, unless regulatory requirements impose them. It is therefore necessary for cybersecurity companies to educate the SME market about available solutions, which generates additional costs with outcomes that are difficult to predict.

Compliance with industry standards is crucial in the field of cybersecurity. However, the need to obtain multiple certifications poses challenges for offering cybersecurity services or products according to 10.6% of respondents. Respondents and interview participants report that the certifications required are not always the same. The fees required to obtain these certifications are not insignificant. Additionally, the time and resources needed to establish and maintain the procedures and controls required by these certifications are added.

Adapting to the needs of SMEs, whose budgets are limited and whose low technological maturity require simplified solutions, represents another challenge for 8.5% of cybersecurity companies. This challenge is exacerbated by a market structure where it is difficult to stand out due to market saturation and the dominant visibility of large companies, even if their solutions are not adapted to the needs and capabilities of SMEs. As one interview participant mentioned: "It is essential for small suppliers to deploy marketing efforts to explain the advantages of an innovative solution beyond current trends." However, several survey respondents encounter difficulties in getting known. They do not benefit from the expected visibility. It seems difficult to stand out in the market, especially for emerging companies with limited advertising budgets.

However, although the market is saturated, this does not mean it is static and cannot hold opportunities. The nature and methods of cyber threats are constantly evolving, thus creating a continuous need for innovation and adapted cybersecurity solutions. Moreover, with the increase in digital connectivity and the growing reliance on information technologies in all business sectors, the demand for robust and adaptive security solutions continues to grow. There are also regional, even national, growth drivers when

human expertise must accompany the solution or when normative or legal frameworks (e.g., Law 25) emerge.

4.5 SWOT Analysis Summary

A SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis for the cybersecurity products and services industry and cyber resilience in the province of Quebec is provided here to serve as a summary of the current situation.

Strengths	Weaknesses
▪ Technological Expertise and Innovation: Quebec has a solid base in research and innovation, notably thanks to renowned research institutions and specialized university programs in cybersecurity. ▪ Government Support: Provincial initiatives, such as investments in technological hubs and tax incentives for R&D in cybersecurity (RSDE, PROMPT, CDAE, PARI, etc.), strengthen the industry. ▪ Dynamic Ecosystem: Presence of a dynamic ecosystem including startups, SMEs, and large companies specialized in cybersecurity. Companies like QoHash, SecureExchanges, Cyberwall.ai, BoostSecurity.io, and OkiOk are notable examples based in Quebec and owned by Canadian interests.	▪ Small-Sized Companies, Low Capitalization, and Reputational Deficit: Few technological champions with patent creation. ▪ Few Large Local Contractors ▪ Weak Academic/Business Open Innovation ▪ International Competition: Facing global giants, Quebec companies may struggle to carve out a place in the international market. ▪ Lack of Skilled Workforce: Although the educational ecosystem is robust, the growing demand for cybersecurity specialists often exceeds supply, creating recruitment challenges. ▪ Dependence on Public Funding: Some startups and SMEs may be heavily reliant on government grants and incentives, which can affect their long-term viability in case of policy changes. ▪ Increasing Outsourcing to Third Countries for Cybersecurity Labor
Opportunities	**Threats**
▪ Global Demand Growth: The constant increase in cyber threats boosts global demand for innovative cybersecurity solutions, offering international opportunities for Quebec companies. ▪ Strategic Collaborations: Opportunities for partnerships with academic institutions, research consortia, and international companies can foster innovation and expansion.	▪ Evolving Cyber Threats: The rapid evolution and increasing sophistication of cyberattacks represent a constant challenge for the industry, requiring continuous R&D investments. ▪ Competition from Emerging Markets: Countries with lower development costs can offer competitive solutions at lower prices, putting pressure on the prices and margins of Quebec companies.

▪ Specific Vertical Sectors: Developing targeted solutions for specific industries (e.g., aerospace, where Quebec excels) represents an opportunity for differentiation and growth.	▪ International Regulations: Changes in international regulatory frameworks can affect access to foreign markets for solutions developed in Quebec.

5. SIX STRATEGIC REFLECTION PATHWAYS

The analysis of documentation and survey and interview data allows for drawing certain conclusions and identifying some reflection pathways to better support the development of the cybersecurity industry in Quebec, as well as the ecosystem whose vitality is essential to this development.

5.1 Fragmentation of the Ecosystem

Firstly, the data recalled that the ecosystem surrounding the cybersecurity industry is complex. The documentation analysis and survey results point to the same observation: the industry is nascent, diverse, and holds enormous commercial potential. However, the ecosystem in which this industry operates remains fragmented and composed of numerous actors with very varied capacities and objectives. Some of these actors are major industry players, possessing undeniable comparative advantages such as their size, links with software or platform producers dominating the market for technological infrastructures used globally. This gives them significant advantages, such as their ability to attract top talent. In contrast, smaller actors and startups have fewer relays in the ecosystem and thus face significant obstacles if they wish to carve out a sustainable place in this market. It could thus be useful to initiate a collective reflection among the various ecosystem actors and on strategies that can be developed to reduce this fragmentation and consolidate the links between the various categories of actors that compose it.

5.2 Incomplete Data on the Industry and Ecosystem

Secondly, to support this sector and ecosystem, higher quality and regularly updated data will be necessary. This is a rapidly evolving sector where issues are multiple, particularly for small players. We note a lack of solid and recent data to have a thorough understanding of the cybersecurity industry in Quebec and its reference ecosystem. If measures are adopted to improve the management and capabilities of this industry, it is necessary to regularly collect relevant statistics to better understand the current state of the industry, ecosystem trends, and buyer needs. This issue arises on both the supply and demand sides, as even if it can be easily assumed that demand exists for all companies, it is essential to better understand how they procure cybersecurity and on what bases they make their decisions. For example, where do they buy their services and why? Additionally, there appears to be a need to establish more regular communication channels between cybersecurity industry actors and governments to better share aspirations, needs, and challenges they respectively face.

5.3 Access of Industry SMEs to Public Markets

The analysis of quantitative and qualitative survey responses highlighted the difficulties experienced by SMEs in accessing markets through public buyer tenders and large institutional contractors, as well as, to a lesser extent, public support programs through grants and other forms of contributions.

SMEs often have very limited administrative capacity and therefore cannot properly equip themselves to meet the contractual requirements of tenders. Helping SMEs to navigate these processes more smoothly could allow them to gain maturity through access to contracts that enable them to develop, become known, and gain reputation. Some jurisdictions like Canada, the United States, or the United Kingdom have developed innovative approaches in this area. These programs use different levers to support national SMEs: firstly, they reserve a percentage of public markets for eligible SMEs, allowing them to compete with companies with comparable capacities. This is the case, for example, in the United States where the goal is for SMEs to be awarded 23% of federal public markets through various programs overseen by the Small Business Administration[16]. In other cases, tender processes are simplified for public contracts not exceeding certain amounts to encourage SMEs to apply. This is the case, for example, for Public Services and Procurement Canada, which launched an initiative in this direction in the fields of AI services procurement and software-as-a-service[17]. Finally, some governments develop tools and practices that facilitate SME participation: the United Kingdom has developed a research and innovation initiative for SMEs that offers contracts within a competitive but pre-commercial process to develop innovation prototypes that meet public service needs[18]. Specific training is also provided, mentoring opportunities are offered, and payments are also made in an accelerated manner, to limit the negative impacts on SMEs' cash flow. In this latter case, the British government commits to paying 90% of invoices from SMEs within 5 business days[19].

Similar practices could be experimented with in Quebec in the cybersecurity field to assess their impact on industry SMEs.

5.4 International Support and Valuation of Local Companies

A fourth finding from the analyzed data is an issue of reputation. Respondents sometimes perceive a lack of trust from public organizations and large contractors in working with smaller, less established suppliers compared to large industry players. This issue is certainly common for new entrants in an emerging market. However, in the cybersecurity universe, this issue can have greater implications given the repercussions that security breaches will have for potential buyers. The offered product must be reliable and robust. Small organizations entering this sector are therefore often not sufficiently recognized to sustainably penetrate the market.

This reputational deficit also impacts the valuation of local companies, which tend to be acquired before reaching full maturity and, consequently, full valuation. Mainly, the recent trend is for these exits to benefit foreign interests, most often American and European. The impact of acquisitions is complex,

influencing not only the entrepreneurs themselves but also the cybersecurity ecosystem as a whole, the investment landscape, and technological innovation.

However, some Quebec cybersecurity companies have already gained international recognition, and the region is well-positioned to continue producing innovations in this field. To address this perceived lack of national and international visibility, developing a unifying quality label could facilitate the promotion activities of local cybersecurity companies. This label, supported by advertising campaigns and assistance for participation in major international cybersecurity fairs, could help improve the recognition of Quebec companies among local buyers and make them more visible internationally compared to their American, French, English, or Israeli competitors, in a political context where Quebec solutions can be perceived as more "neutral" and respectful of buyers' digital sovereignty. This is, for example, the choice made by France with its "France Cybersecurity" label[16].

5.5 Targeted Government Support

Fifth, it would be beneficial to explore support for creating niche markets. The cybersecurity market is vast with numerous players in both Canada and the United States. Additionally, survey and interview results indicate that breaking into the Canadian market is very challenging unless a company is already known and recognized in the United States, where major tech giants are located. This may explain why Quebec-based companies primarily operate in the cybersecurity services market and, to a lesser extent, in product development.

It might be worthwhile to consider the possibility of more targeted government assistance in areas where it would be most impactful and help differentiate from the competition. Funding opportunities could therefore focus on specific niches or a limited number of sectors where Quebec has proven competitive advantages. Personal data protection appears to be a promising area for the future, given legislative obligations and the fact that it is cited as one of the top concerns for Canadian organizations. Artificial intelligence as a cybersecurity tool or a technology to protect, as well as quantum computing, are also natural candidates for this targeted approach. This is due to the possible synergies with highly dynamic innovation ecosystems that are developing in Quebec with government support.

5.6 Collaborations Between Industry and Academia

Sixth, it would be desirable to strengthen the connections between cybersecurity companies and universities for two main reasons. First, developing an innovative and robust cybersecurity industry requires a strategic approach centered on entrepreneurs supported by research centers. In this regard, there seems to be a communication gap between the cybersecurity industry, particularly the SMEs that make it up, and the academic sector. Enhanced dialogue and partnerships between educational

[16] https://www.francecybersecurity.fr/.

institutions and cybersecurity industry players, whether they are entrepreneurs or buyers, would be beneficial to accelerate the transfer of knowledge from fundamental research projects to concrete industrial applications that meet industry needs.

Furthermore, there is a talent shortage, and closer ties with higher education institutions would be crucial to address this issue. Strategic networking activities between researchers and companies could be considered, with a particular focus on SMEs. The same targeted support approach proposed in the previous section could also be extended to research centers to encourage them to prioritize certain themes deemed critical for the ecosystem in the short, medium, and long term.

Finally, government assistance in recruitment through partnerships with colleges and universities (e.g., matching programs) could help mitigate the talent shortage in the sector while ensuring better visibility of cybersecurity careers among college and university students.

CONCLUSION

Beyond its strategic importance, the cybersecurity industry represents a promising economic sector for Quebec, driving prosperity and growth in an uncertain world where digital risks continue to become more complex. This industry is innovative and offers products and services in high demand both nationally and for export. Quebec appears well-positioned due to its highly qualified workforce and the presence of world-class educational and research institutions within its territory.

However, the Quebec ecosystem remains fragmented and fragile. It is primarily composed of small and medium-sized enterprises that compete directly with large multinationals and often lack the resources to respond to major contracts or form productive partnerships with academic research teams. A model that leverages the strengths of this ecosystem while reducing barriers to its development is yet to be defined. This model should emerge from a common vision developed by all components of the ecosystem in a spirit of collaboration.

Another significant challenge for the cybersecurity ecosystem is its interconnection with other emerging innovation ecosystems in Quebec, whether in artificial intelligence and quantum computing within the digital sector or in energy, transportation, and agri-food sectors for other industries.

The profound technological transformation initiated by the digital revolution now exposes all businesses and infrastructures to cyber risks that could threaten their survival by disrupting the logistical, energy, financial, and informational flows they depend on. The global race for innovation also drives some countries to engage in aggressive practices of intellectual property theft developed in Quebec using advanced technological means. It may therefore be pertinent to make cybersecurity a pivotal aspect of innovation policies and strategies by creating incentives for the entire innovation ecosystem to benefit from the expertise of specialized cybersecurity partners, thereby enhancing the resilience of Quebec's economy. This concept of cyber-resilience will become central in the ever-evolving landscape of cyber risks. Businesses, governments, and individuals all need to protect their data and systems against cyberattacks. This situation creates a fertile ground for the growth of the cybersecurity industry.

The cybersecurity industry offers enormous growth potential and exciting opportunities. By working together, we can create a safer and more resilient digital future.

REFERENCES

Ahlawat, P., Krause, T., Pagano, E., Banerjee, S., Jarvis, F., Justin, J., et Emerson, G. (2019). *How software companies can get more bang for their R&D buck*. Boston Consulting Group. Repéré à https://www.bcg.com/publications/2019/software-companies-using-research-and-development-more.

Aiyer, B., Caso, J., Russell, P. et Sorel, M. (2022). *New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers*. McKinsey & Company.

Berry, C. et R. Berry (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management* 8 (1): 1-10.

Bouchard, L. et Henri, J.-F. (2023). *Gouvernance de la cybersécurité - Portrait et tendance au Québec*. Repéré à https://www.cas.ulaval.ca/wp-content/uploads/2023/04/Article_Gouvernance_Cybersecurite_vue2pages.pdf.

Carmel, E. et Roche, E. (2023). The dominant cybersecurity industry clusters: evolution and sustainment.
Industry and Innovation 30 (3): 361-391.

Centre canadien pour la cybersécurité (2022). *À propos du Centre pour la cybersécurité*. Repéré à À propos du Centre pour la cybersécurité - Centre canadien pour la cybersécurité

Centre canadien pour la cybersécurité (2024). *Certifications dans le domaine de la cybersécurité*. Repéré à https://www.cyber.gc.ca/sites/default/files/certifications-domaine-cybersecurite-2024-f.pdf

Cohen, N., Hulvey, R., Mongkolnchaiarunya, J., Novak, A., Morgus, R. et Segal, A. (2017). *Cybersecurity as an engine for growth*. Repéré à http://www.jstor.com/stable/resrep10491.1

CPE Media & Data Company (2024). *Strong Q2 2024 VC drives Canadian VC reaching $3.87B*. Repéré à https://www.newswire.ca/news-releases/strong-q2-2024-vc-drives-canadian-vc-reaching-3-87b- 817250967.html.

CRTC (2023). *Plan ministériel 2023-2024*. Repéré à https://crtc.gc.ca/fra/publications/reports/dp2023/dp2023.htm.

CVCA (2024). *Year-end 2023 VC & PE Canadian market overview.*
Repéré à https://www.cvca.ca/insights/market-reports/year-end-2023/.

Cybereco (2022). *Sondage sur la cybersécurité*. Résultats présentés à la Cyber Conférence 2022.

Deloitte (2016). *Harnessing the cybersecurity opportunity for growth: Cybersecurity innovation & the financial services industry in Ontario*. Repéré à https://www.oc-innovation.ca/wp-content/uploads/2021/03/Harnessing-the-cybersecurity-opportunity-for-growth.pdf

Deloitte (2023). *2023 Global Future of Cyber Survey - Building long-term value by putting*

cyber at the heart of the business. Repéré à https://www.deloitte.com/global/en/services/risk-advisory/content/future-of-cyber.html

Dupont, B. (2024). *La cybercriminalité : Approche écosystémique de l'espace numérique*. Paris : Armand Colin.

Dupont, B. et C. Whelan (2022). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology* 54 (1): 76-92.

Fédération des chambres du commerce du Québec (2021). *Étude sur la cybersécurité et les opportunités offertes par l'accès aux données au Québec*. Repéré à https://www1.fccq.ca/wp-content/uploads/2021/11/RapportAviseo_cybervalorisation_FCCQ_final.pdf

Fortin, A., Watler, P., Ladouceur, R., Montès, F. C. et Roberge, L. (2021). *Chapitre 7 Cybersécurité*. Rapport

du Vérificateur général du Québec à l'Assemblée nationale pour l'année 2021-2022.

Fortune Business Insight (2024). *Cyber security market*. Repéré à https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

Gartner (2023). *Gartner forecasts global security and risk management spending to grow 14% in 2024*. Repéré à https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global- security-and-risk-management-spending-to-grow-14-percent-in-2024

Gouvernement du Québec (2024). *Le commerce extérieur du Québec*. Repéré à https://www.economie.gouv.qc.ca/fileadmin/contenu/publications/etudes_statistiques/echanges_exte rieurs/calepin_exterieur.pdf.

Groupe Novipro et Léger (2023). *Portrait des TI dans les petites, moyennes et grandes entreprises canadiennes*. Étude Portrait TI.

Herron, C., Rice, F. et Snider, N. (2020). *À la recherche des talents cachés : L'expérience et l'expertise de la communauté de cybersécurité du Nouveau-Brunswick*, Ottawa: Conseil des technologies de l'information et des communications.

Innovation, Sciences et Développement économique Canada (2022). *L'état de l'industrie canadienne de la cybersécurité – Automne 2022*. Repéré à https://ised-isde.canada.ca/site/aerospatiale- defense/fr/rapport-letat-lindustrie-canadienne-cybersecurite

Institut d'études internationales de Montréal (2020). *La stratégie internationale du Canada en matière de cybersécurité : enjeux et recommandations*. Recommandations politiques. Repéré à https://www.ieim.uqam.ca/IMG/pdf/ieim-recommandations_politiques-cyberse_curite_-fe_v2020.pdf

Investissement Québec (2021). *Le Québec, pôle florissant de la cybersécurité*. Présentation PowerPoint.

(ISC)² (2021). *A Resilient Cybersecurity Profession Charts the Path Forward - Cybersecurity Workforce Study.* Repéré à https://www.mvrop.org/cms/lib/CA01922720/Centricity/Domain/59/ISC2%20Cybersecurity%20Workfor ce%20Study%202021.pdf

(ISC)² (2019). *Strategies for Building and Growing Strong Cybersecurity Teams*. Repéré à https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2 Cybersecurity-

Knowles, W., Such, J., Gouglidis, A., Misra, G. et Rashid, A. (2017). All that glitters is not gold: On the effectiveness of cybersecurity qualifications. *Computer* 50: 60-71.

Landwehr, C. (2010). History of US government investments in cybersecurity research. *2010 IEEE Symposium on Security and Privacy*. Repéré à https://ieeexplore.ieee.org/abstract/document/5504783.

Ministère de l'Économie, de l'Innovation et de l'Énergie (2021). *Aperçu de l'industrie des technologies de l'information*. Repéré à https://www.economie.gouv.qc.ca/bibliotheques/le-secteur/technologies-de- linformation-et-des-communications/apercu-de-lindustrie-des-technologies-de linformation#:~:text=Au%20Qu%C3%A9bec%2C%20l'industrie%20des,pr%C3%A9pond%C3%A9rante%2 0dans%20l'%C3%A9conomie%20qu%C3%A9b%C3%A9coise.

Montréal International (2021). *Grand Montréal : un hub de cybersécurité en pleine effervescence*. Repéré à https://www.montrealinternational.com/app/uploads/2019/04/cybersecurite_profil_sectoriel_2021- 1.pdf

Moore, J. (1993). Predator and prey: A new ecology of competition. *Harvard Business Review* 71 (3): 75- 86.

Moore, J. (1996). *The death of competition: Leadership and strategy in the age of business ecosystems*. New York: Harper Business.

Prompt (2023). *S'unir pour renforcer la cybersécurité au Québec.* Montréal : Prompt. Repéré à https://Promptinnov.com/wp-content/uploads/2023/12/Memoire-cyberVF.pdf.

Quan, T. et Herron, C. (2022). *Développement des talents en cybersécurité : protéger l'économie*

numérique du Canada, Ottawa : Conseil des technologies de l'information et des communications.

Sécurité publique Canada (2018). *Stratégie nationale de cybersécurité*. Repéré à ntnl-cbr-scrt-strtg-fr.pdf (securitepublique.gc.ca)

Statistique Canada (2022). *L'incidence du cybercrime sur les entreprises canadiennes, 2021*. Repéré à https://www150.statcan.gc.ca/n1/daily-quotidien/221018/dq221018b-fra.htm.

TECHNOCompétences (2021). *Diagnostic sectoriel 2021-2024*. Portrait de la main-d'œuvre dans le secteur

des technologies de l'information et des communications (TIC) au Québec.

The Economist (2018). *Defence companies target the cyber-security market*. 26 juillet. Repéré à

https://www.economist.com/business/2018/07/26/defence-companies-target-the-cyber-security- market.

Westin, F., Ream, F. et Dupont, B. (2022). *Adapting cybersecurity to the needs and capacities of SMEs: A Canadian perspective*. Montréal: SERENE-RISC. Repéré à https://www.serene-

risc.ca/public/media/files/prod/page_files/31/Serene_Cybersecurity_Ecosystem_Canada.pdf.

Cyberéco (2024). Ontologie des sociétés fournisseurs en cybersécurité v.1.0. Disponible sur demande.

APPENDIX 1: International Cybersecurity Ecosystems

Summary Analysis of Major International Cybersecurity Ecosystems Prepared by In-Sec-M

Israeli Ecosystem

Strengths

Military Service and Intelligence

- Unit 8200:
  - This elite intelligence unit of the Israeli Defense Forces is often compared to the American NSA. It focuses on cyber defense, intelligence gathering, and cyberattacks. Many former members go on to found cybersecurity startups or join technology companies, bringing advanced skills in cyber technologies.

- Culture of Military Innovation:
  - The Israeli military encourages risk-taking and innovation, education young individuals to think creatively and solve complex problems—crucial skills in cybersecurity.

Startup Ecosystem

- "Startup Nation" :
  - Israel is renowned for its dynamic startup ecosystem, boasting the highest number of startups per capita in the world, with a significant focus on technology and cybersecurity.

- Venture Capital Investments:
  - The country attracts substantial venture capital investments, both local and international. Investors are particularly drawn to cybersecurity innovations emerging from Israel.

Government Support

- Support Programs and Grants:
  - The Israeli government offers grants and tax incentives to technology startups, including those specializing in cybersecurity. Since at least 2011, Tel Aviv has been coordinating and centralizing cybersecurity efforts nationwide.

- Public-Private Partnerships:
  - Israel actively promotes collaborations between the government, businesses, and academic institutions to develop robust cybersecurity solutions.

Education and Research

- Academic Institutions:
  - Israeli universities, such as Tel Aviv University, Ben-Gurion University (Negev), Hebrew University of Jerusalem, and the Technion, are recognized for their advanced cybersecurity research programs.

- Education Programs:
  - There are numerous cybersecurity education programs at various levels aimed at educating the next generation of cybersecurity professionals.

Technological Innovation

- Strong R&D Culture:
  - Israel dedicates a significant portion of its GDP to research and development (R&D), focusing on technological innovation, including in cybersecurity.

- Advanced Technologies:
  - The country is at the forefront of emerging technologies like artificial intelligence, blockchain, and machine learning applied to cybersecurity.

Global Market

- Technology Exportation:
  - Israel exports a large portion of its cybersecurity technologies globally. Israeli companies secure contracts with governments and international businesses to protect their critical infrastructures.

- Attraction of Multinationals:
  - Many global technology giants, such as Microsoft, Google, and IBM, have established R&D centers in Israel, attracted by the local expertise in cybersecurity.

Entrepreneurial Mindset

- Culture of Resilience and Innovation:
  - Israeli culture values resilience, innovation, and the ability to tackle complex challenges—essential traits for success in the cybersecurity field.

- Success of Expatriates:
  - Numerous Israeli entrepreneurs achieve international success, enhancing the visibility and credibility of Israel's technological ecosystem.

Weaknesses

Dependence on Foreign Markets:

- A significant portion of Israeli cybersecurity companies depend on clients and markets abroad, particularly in the United States and Europe. This dependence can make companies vulnerable to economic fluctuations and policy changes in these regions.

Talent Shortage:

- Although Israel has a strong talent pool in cybersecurity, demand often surpasses supply. This shortage can limit company growth and make it challenging to retain top talent, who may be attracted to opportunities overseas.

Intense Competition:

- The large number of startups in the cybersecurity sector leads to intense competition for funding, clients, and talent. This environment can result in market fragmentation and difficulties for emerging companies to differentiate and stabilize.

Security Risks:

- As a nation in conflict, Israel is frequently targeted by cyberattacks. While this situation provides valuable practical experience in defending against cyber threats, it also poses risks to local businesses. The ongoing conflict with Hamas adds another layer of complexity to the development of the local cybersecurity ecosystem.

High Cost of Innovation:

- Research and development in cybersecurity are costly. Companies must continuously invest in innovation to remain competitive, which can be financially challenging, especially for startups.

Bureaucracy and Regulation:

- Despite strong government support for the cybersecurity sector, some companies face difficulties with regulations and bureaucracy, particularly concerning data protection and compliance.

Conclusion

Israel has become a pivotal player in the global cybersecurity landscape through a unique combination of advanced military education, a dynamic startup ecosystem, robust government support, cutting-edge research and development, and a culture of innovation. These factors have enabled Israel to develop world-class cybersecurity solutions and attract significant investments and international collaborations, thereby solidifying its position as a leader in this strategic field.

French Ecosystem

Strengths

Government Policies and Support

- ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information):
  - Established in 2009, ANSSI is France's primary cybersecurity authority. It plays a crucial role in protecting critical infrastructures, regulating the sector, and raising awareness about cybersecurity issues.

- National Cybersecurity Strategy:

- The French government has implemented several national strategies to strengthen cybersecurity, including investments in research, development, and education. These strategies aim to enhance the nation's resilience against cyber threats and foster innovation within the sector.

Research and Development

- Research Institutes:
  - Institutions such as INRIA (National Institute for Research in Computer Science and Automation) and CEA (French Alternative Energies and Atomic Energy Commission) are key players in cybersecurity research. They contribute significantly to advancements in cybersecurity technologies and methodologies.

- Public-Private Collaborations:
  - France promotes partnerships between academic institutions, private companies, and government bodies to encourage innovation in cybersecurity. These collaborations facilitate the development of robust cybersecurity solutions and drive technological progress.

Startup Ecosystem

- "France Cybersecurity" Label:
  - Launched in 2015, this label aims to promote French-developed cybersecurity solutions and enhance their international visibility. It helps startups gain recognition and access new markets.

- Incubators and Accelerators:
  - Initiatives like the Cyber Campus in Paris and programs such as "La French Tech" support innovative cybersecurity startups by providing resources, mentorship, and networking opportunities essential for their growth and development.

Education and Training

- Academic Programs:
  - French universities and grandes écoles offer specialized programs in cybersecurity. Institutions like Télécom Paris and the University of Rennes 1 are renowned for their cutting-edge curricula that prepare students for careers in cybersecurity.

- Cyber Range:
  - The establishment of cyber ranges—simulation and training platforms—enables cybersecurity professionals to train in realistic environments. These facilities enhance practical skills and preparedness for real-world cyber threats.

Standards and Regulations

- GDPR (General Data Protection Regulation):

- The LPM includes specific provisions for cybersecurity, focusing on the protection of critical infrastructures and the defense of information systems. This law underscores the importance of cybersecurity in national defense strategies.

- LPM (Military Programming Law):
  - The LPM includes specific provisions for cybersecurity, focusing on the protection of critical infrastructures and the defense of information systems. This law underscores the importance of cybersecurity in national defense strategies.

Leading Companies

- Large Enterprises:
  - Companies like Thales, Airbus CyberSecurity, and Orange Cyberdefense are global leaders in cybersecurity, offering advanced solutions and operating internationally. Their presence reinforces France's position in the global cybersecurity market.

- Innovative SMEs:
  - France is home to numerous innovative small and medium-sized enterprises (SMEs) and startups in cybersecurity, such as Stormshield, Wallix, and Thetris. These companies develop cutting-edge technologies and contribute to the diversity and dynamism of the cybersecurity ecosystem.

Awareness and Communication

- FIC (Forum InCyber) :
  - Organized annually in Lille, the FIC is one of Europe's largest cybersecurity events. It attracts professionals from around the world to exchange best practices and showcase innovations, fostering a vibrant community and knowledge sharing.

- Awareness Campaigns:
  - ANSSI and other organizations regularly conduct campaigns to educate the public and businesses about cybersecurity challenges and best practices. These initiatives aim to raise awareness and promote a culture of cybersecurity vigilance across all sectors.

Weaknesses

Talent Shortage:

- Like many countries, France faces a shortage of qualified cybersecurity professionals. This shortage restricts companies' ability to recruit the necessary experts to address growing threats effectively.

Market Fragmentation:

- The French ecosystem is characterized by fragmentation, with numerous small and medium-sized enterprises (SMEs) and startups. This situation can lead to a dispersion of resources and difficulties for some companies to reach a critical mass necessary to compete on an international scale.

Limited Access to Funding:

- French cybersecurity startups may struggle to access sufficient funding to support their growth and innovation, especially when compared to their American or Israeli counterparts, who often benefit from more substantial financial support.

Strict Regulation:

- French regulations, while essential for protecting data and privacy, can sometimes be perceived as obstacles by businesses. Smaller companies, in particular, may find it challenging to comply with all legal requirements, hindering their operations and growth.

International Visibility:

- Compared to the United States and Israel, the French ecosystem may lack visibility and international recognition, which can limit opportunities for partnerships and expansion abroad.

Slow Adoption of New Technologies:

- Some French companies may be slower to adopt new technologies and approaches in cybersecurity, making them more vulnerable to evolving threats and reducing their competitiveness in the market.

Public-Private Cooperation:

- Although efforts exist to improve cooperation between the public and private sectors, this collaboration can still be strengthened to provide a more coordinated response to cyber threats.

Conclusion

France has successfully established itself as a significant player in the cybersecurity arena through a coherent and well-articulated strategy that includes government support, a dynamic startup ecosystem, advanced training programs, and close collaboration between the public and private sectors. Initiatives such as ANSSI, the "France Cybersecurity" label, and events like the FIC have enabled France to position itself as a leader in this crucial field.

American Ecosystem

Strengths

Advanced Technological and Industrial Ecosystem

- Silicon Valley:
  - As the global hub of technological innovation, Silicon Valley hosts numerous leading cybersecurity companies, such as Palo Alto Networks, Symantec, FireEye, and many others. This concentration fosters a vibrant environment for cybersecurity advancements and collaborations.

- Major Technology Companies:

- Tech giants like Google, Microsoft, IBM, and Amazon have robust cybersecurity divisions, investing heavily in research and development to create advanced solutions. Their substantial resources and global reach enhance the overall strength of the American cybersecurity ecosystem.

Massive R&D Investments

- Venture Capital:
  - The United States benefits from significant venture capital access, enabling cybersecurity startups to grow rapidly. In 2020 alone, the cybersecurity sector attracted over $7.8 billion in venture capital, fueling innovation and expansion.

- Continuous Innovations:
  - R&D investments drive ongoing innovations in areas such as artificial intelligence, machine learning, advanced cryptography, and the security of critical infrastructures, keeping the U.S. at the forefront of cybersecurity technology.

Government Support and National Strategies

- NSA and Cyber Command:
  - The National Security Agency (NSA) and the United States Cyber Command play crucial roles in protecting national interests and developing advanced cybersecurity technologies. Their efforts provide a strong foundation for national cybersecurity resilience.

- Policies and Regulations:
  - Initiatives like the Cybersecurity Information Sharing Act (CISA) encourage the sharing of threat information between the private sector and the government, enhancing collective security measures and response capabilities.

- Federal Funding:
  - Agencies such as the Defense Advanced Research Projects Agency (DARPA) fund advanced cybersecurity research projects, fostering cutting-edge developments and technological breakthroughs in the field.

Education and Training

- Top-Tier Universities:
  - The United States is home to some of the world's leading universities, including MIT, Stanford, and Carnegie Mellon, which offer top-notch cybersecurity training and research programs. These institutions produce highly skilled professionals and drive significant advancements in cybersecurity.

- Professional Certifications:
  - The U.S. boasts a wide range of globally recognized professional certifications, such as CISSP, CEH, and CISM, which enhance the competencies of cybersecurity professionals and ensure high standards within the industry.

Dynamic Startup Ecosystem

- Incubators and Accelerators:

- Programs like Y Combinator and Techstars support innovative cybersecurity startups by providing essential resources, mentorship, and networking opportunities. These incubators and accelerators play a vital role in nurturing new ventures and fostering innovation.

- Strategic Acquisitions:
  - Large technology companies frequently acquire cybersecurity startups to integrate their technologies and talent, promoting continuous innovation and strengthening the overall ecosystem.

Proactive Private Sector

- Sensitive Industries:
  - Sectors such as finance, healthcare, and energy invest heavily in cybersecurity to protect their critical infrastructures. This proactive approach ensures that these industries remain resilient against cyber threats and contribute to the overall strength of the cybersecurity ecosystem.

- Cyber Threat Intelligence:
  - Many American companies possess advanced threat intelligence capabilities, enabling them to respond swiftly to cyberattacks and mitigate potential damages effectively. This expertise enhances national and corporate cybersecurity defenses.

Awareness and Information Sharing

- Information Sharing and Analysis Centers (ISACs):
  - ISACs facilitate the sharing of information about cyber threats among companies within the same sector, improving collective resilience and enabling more effective responses to emerging threats.

- Conferences and Events:
  - Events like the RSA Conference and Black Hat attract cybersecurity professionals from around the world, fostering knowledge exchange and driving innovation through collaborative discussions and presentations.

Weaknesses

Talent Shortage:

- The United States faces a critical shortage of qualified cybersecurity professionals. The growing demand for experts far exceeds the supply, complicating the recruitment and retention of competent staff.

Regulatory Complexity:

- The American regulatory landscape is fragmented, with varied laws and regulations at the federal, state, and local levels. This complexity can lead to compliance difficulties for companies, especially those operating in multiple jurisdictions.

Highly Fragmented Market:

- While the U.S. market is vast, it is also highly fragmented with numerous companies ranging from startups to tech giants. This fragmentation can dilute the coordination and collaboration efforts necessary for effective defense against cyber threats.

Challenges in Protecting Critical Infrastructure:

- U.S. critical infrastructures such as energy, transportation, and finance are frequent targets of cyberattacks. Protecting these infrastructures is a constant challenge due to their complexity and interdependence.

Internal Threats:

- In addition to external threats, the U.S. must also contend with internal threats, including disgruntled or negligent employees who can compromise system security.

Slow Innovation and Updates:

- Some large organizations may be slow to adopt new cybersecurity technologies or update their systems, making them vulnerable to new threats.

High Cost of Cybersecurity:

- The cost of implementing and maintaining cybersecurity measures is high, which can be a barrier for small and medium-sized enterprises. These costs include technology, training, and regular security audits.

Dependence on Foreign Suppliers:

- Part of the technologies and components used in cybersecurity systems come from foreign suppliers, posing risks to national security and supply chain integrity.

Conclusion

The United States dominates the global cybersecurity sector thanks to an advanced technological and industrial ecosystem, massive investments in R&D, strong government support, leading academic institutions, and a proactive private sector. This combination of factors allows the U.S. to remain at the forefront of cybersecurity innovation and effectively respond to growing cyber threats.

German Ecosystem

Strengths

Expertise in Industrial Security

- Industrie 4.0:
  - Germany is a pioneer in Industry 4.0, integrating cyber-physical systems and Internet of Things (IoT) technologies into industrial processes. This has led to the advanced development of cybersecurity solutions to protect critical infrastructures.

- Siemens, Bosch:
  - Industrial giants like Siemens and Bosch invest heavily in cybersecurity, developing solutions to secure industrial environments and critical infrastructures. Their substantial resources and expertise contribute significantly to the robustness of Germany's cybersecurity landscape.

Research Centers and Universities

- Fraunhofer Institute:
  - Fraunhofer is one of Europe's leading applied research organizations, with specialized centers in cybersecurity, such as the Fraunhofer Institute for Secure Information Technology (SIT). These institutes drive innovation and provide cutting-edge research in cybersecurity technologies.

- Renowned Universities:
  - Universities like the Technical University of Munich (TUM) and the University of Darmstadt offer advanced programs in cybersecurity, producing highly qualified researchers and professionals. These institutions play a crucial role in fostering talent and advancing cybersecurity knowledge.

Government Support

- BSI (Bundesamt für Sicherheit in der Informationstechnik):
  - BSI is Germany's federal cybersecurity agency, playing a central role in protecting critical infrastructures, regulating the sector, and raising awareness about cybersecurity threats and best practices.

- National Initiatives and Strategies:
  - The German government has implemented several national strategies to strengthen cybersecurity, including investments in research and development and the establishment of robust cybersecurity policies. These initiatives aim to enhance national resilience against cyber threats and support the growth of the cybersecurity industry.

Startup Ecosystem

- Berlin and Munich:
  - Berlin and Munich are major technology hubs in Europe, home to numerous innovative cybersecurity startups. These cities benefit from a strong venture capital ecosystem and incubators that provide essential support and resources for startup growth and development.

Weaknesses

Talent Shortage

- Lack of Qualified Professionals:
  - Like many countries, Germany faces a shortage of qualified cybersecurity professionals. This talent gap can slow down the growth of cybersecurity companies and limit their ability to respond effectively to increasing cyber threats.

Regional Fragmentation

- Regional Disparities:
  - The development of cybersecurity in Germany can vary significantly across different regions. Some areas are more advanced in terms of infrastructure and innovation support, while others lag behind, leading to uneven growth and resource distribution within the country.

Complex Regulations

- Regulatory Compliance:
  - Companies must navigate a complex regulatory framework, which can pose challenges, especially for small and medium-sized enterprises (SMEs) and startups. The intricacies of compliance can be resource-intensive and may hinder the ability of these businesses to focus on innovation and growth.

Main Actors

Companies

- Siemens:
  - A leader in industrial cybersecurity solutions, Siemens develops technologies to protect critical infrastructures and industrial systems.
- Bosch:
  - Bosch also invests in cybersecurity solutions for the industrial, automotive, and connected devices sectors.
- SAP:
  - As a giant in enterprise software, SAP develops solutions for data and application security within businesses.

Startups and SMEs

- Cure53:
  - Specializing in penetration testing and security audits, Cure53 is renowned for its thorough assessments of web applications and systems security.
- Rohde & Schwarz Cybersecurity:
  - Provides comprehensive cybersecurity solutions for the protection of networks, applications, and data.
- Cysmo:
  - Develops solutions for online fraud detection and protection against cyberattacks.

Research Institutes

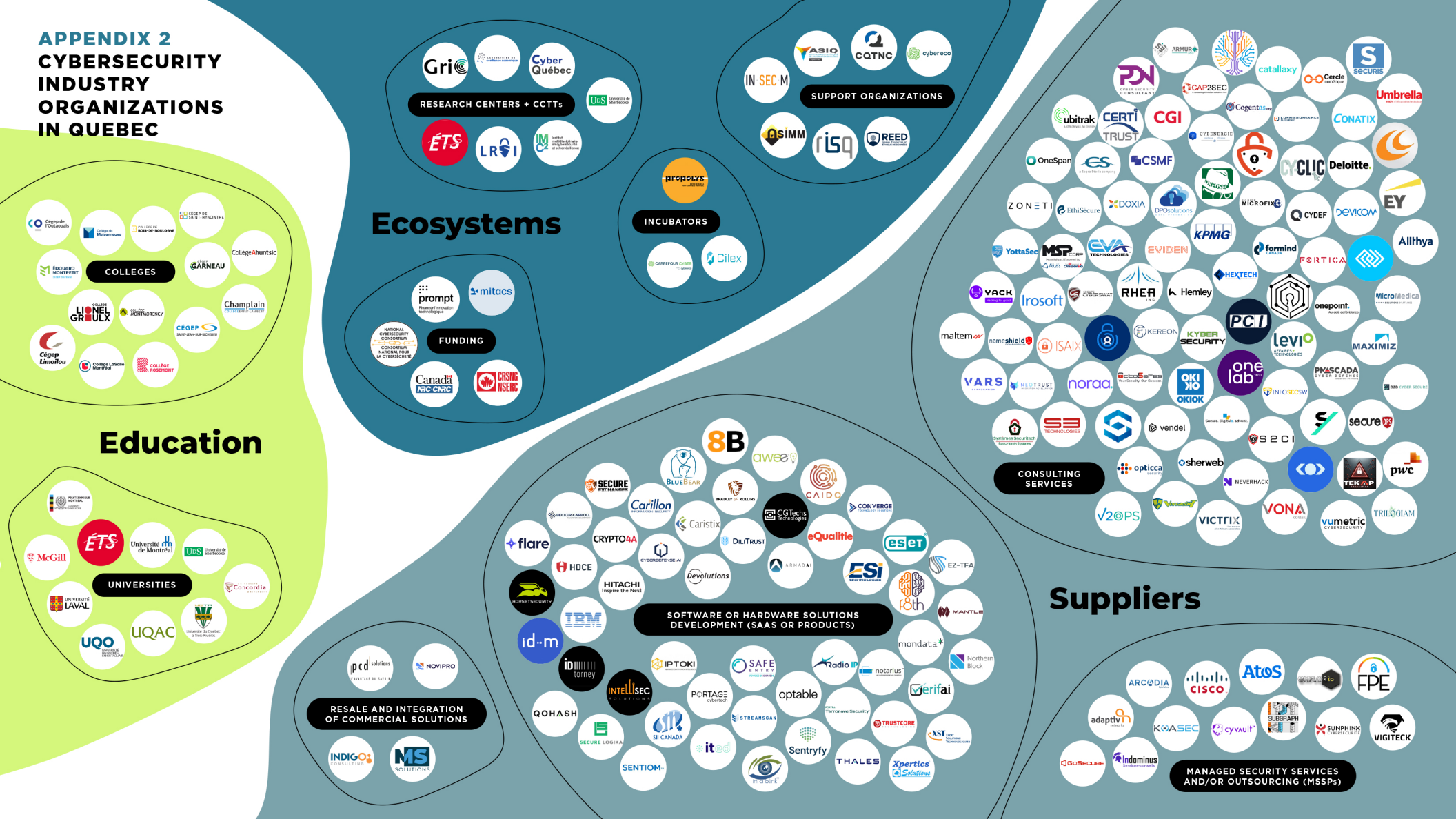
- Fraunhofer SIT:
  - Conducts applied cybersecurity research, developing technologies to secure IT systems and networks.
- Helmholtz Center for Information Security (CISPA):

- One of the leading research centers in computer security, CISPA works on advanced projects in cryptography, network security, and data protection.

Conclusion

Germany boasts a robust cybersecurity ecosystem, supported by strong expertise in industrial security, world-class research centers, and substantial government support. However, challenges such as talent shortages and regional fragmentation must be addressed to maintain and strengthen its position as a cybersecurity leader. The emphasis on securing critical and industrial infrastructures reflects the country's economic and technological priorities, making Germany a key player in the global cybersecurity landscape.

APPENDIX 2
CYBERSECURITY INDUSTRY ORGANIZATIONS IN QUEBEC



CYBERSECURITY INDUSTRY ORGANIZATIONS IN QUEBEC

Ecosystems

RESEARCH CENTERS + CCTTs

Cyber Québec
GRIC - Groupe de Recherche Interdisciplinaire en Cybersécurité
IMC2 - Institut Multidisciplinaire en Cybersécurité et Cyberrésilience
Laboratoire de confiance numérique
LCSec - Laboratoire de CyberSécurité - ÉTS
LRSI - Laboratoire de Recherche en Sécurité Informatique - UQO
Pôle d'expertises en cybersécurité - UdeS

FUNDING

CNC - Consortium National pour la Cybersécurité
CNRC - Conseil National de Recherches du Canada (PARI)
CRSNG - Conseil de Recherches en Sciences Naturelles et en Génie du Canada
MITACS
PROMPT

INCUBATORS

Carrefour Cyber
CILEX
Propolys

SUPPORT ORGANIZATIONS

ASIMM - Association de Sécurité de l'Information du Montréal Métropolitain
ASIQ - Association de la Sécurité de l'Information du Québec
CQTNC - Centre Québécois en Transformation Numérique et Cybersécurité
CyberÉco
In-Sec-M - Innovation Sécurité Marché
REED - Réseau d'Expertise en Éthique de Données
RISQ - Réseau d'Informations Scientifiques du Québec

Education

COLLEGES

CÉGEP de l'Outaouais
CÉGEP de Saint-Hyacinthe
CÉGEP Édouard Monpetit
CÉGEP Garneau
CÉGEP Limoilou
CÉGEP Saint-Jean-sur-Richelieu
Collège Ahuntsic
Collège Champlain Saint-Lambert
Collège de Bois-de-Boulogne
Collège de Maisonneuve
Collège LaSalle
Collège Lionel Groulx
Collège Montmorency
Collège Rosemont

UNIVERSITIES

ÉTS - École de Technologie Supérieure
Polytechnique Montréal
UdeM - Université de Montréal
UdeS - Université de Sherbrooke
UL - Université Laval
Université Concordia / Concordia University
Université McGill / McGill University
UQAC - Université du Québec à Chicoutimi
UQO - Université du Québec en Outaouais
UQTR - Université du Québec à Trois-Rivières

Suppliers

SOFTWARE OR HARDWARE SOLUTIONS DEVELOPMENT (SAAS OR PRODUCTS)

8Brains
Awee Inc.
Becker-Carroll (Converge)
Bluebear LES
Bradley & Rollins
Caido
Carillon Information Security
Caristix
CGtechs
Converge Technology Solutions
Crypto4A
CYBERDEFENSE.AI
Devolutions Inc.
DiliTrust Canada Inc.
EasyPatternZ Incorporated (IKAR-Holding/ArmadAI)
eQualitie Inc.
ESET Canada Research
ESI Technologies Inc.
EZ-TFA
F8th
Flare Systems Inc.
HDCE Inc.
Hitachi Systems Security Inc.
Hornet Securité
IBM Canada
Id-m.me (IDM Gestion identité INC)
IDtorney LAW - TECH Inc. - CAPITAL LP.
Intellisec Solutions
IPtoki
KrowdX
Logiciels Radio IP Inc.
Mantle Blockchain
Mondata / Groupe Elucidia
Northern Block
Notarius Solutions
Portage CyberTech
QoHash
Secure Exchanges Inc.
Secure Logika
Sentiom
SII (Société Informatique Industrielle) Canada
Solutions ITED
StreamScan Security
Technologies In A Blink
Technologies Optable
Technology Sentryfy
Terranova Security (Fortra)
Thales Digital Solutions
Trustcore
Verif AI (Solutions I Agree Inc.)
Xpert Solutions Technologiques
Xpertics

RESALE AND INTEGRATION OF COMMERCIAL SOLUTIONS

Groupe NOVIPRO
Indigo Consulting
MS Solutions conseil
PCD Solutions (Converge)

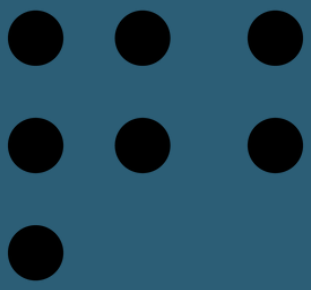
CONSULTING SERVICES

Agence PDN
Alithya
Armur360 - Expérience S3I
B2B Cyber Secure
Brainstorm CyberRisque
Cap2sec
Catallaxy (RCGT)
Cercle numérique
Certi-Trust
CGI
Cogentas Inc
Commissionnaires du Québec
Conatix
Conseils CeptBiro Inc.
CS Group Canada
CSMF - Cyber Securité Mathieu Fluet
Cybenergie
CyberEspoir Inc.
CyberShell
CY-CLIC
CYDEF
Deloitte
Devicom
Doxia
DPO Solution Inc.
Dredsec
Équipe MICROFIX
Ernst & Young (EY)
EthiSecure Services
EVA Technologies (Logicnet)
Eviden
Formind Canada
Fortica (KPMG)
Groupe Access (Groupe MSP)
Groupe CyberSwat
Groupe RHEA
Hemley
Hextech (Technologies Hexadécimales)
ILIR
Infosecsw
INSSATAD
Irosoft
IsaiX
Kéréon
KPMG
Kyber Sécurité
Levio
Maltem Canada
Maximiz
Micromedica
Nameshield Cybersécurité
Neotrust Cybersécurité
Noraa
Octosafes
OKIOK Data
One Lab Technologies
OnePoint
OneSpan
PCI 360
PM SCADA
PWC
Resolock
RMDS Innovation
S2Ci - Société de Conseils en Cybersécurité et Informatique
S3 TECHNOLOGIES
Secure Digitale
SecureOps
Securis Canada
Sécurité Opticca
Sherweb Inc.
Sia Partners
Solutions NeverHack (Silicom Inc / Seela)
Sonder Sécurité
Systèmes Securitech
Tekap
Trilogiam
Ubitrak (Kerson Wallaw)
Umbrella Technologies
V2OPS Solutions d'Entreprise Inc.
VARS
VersagiliT Inc.
Victrix Conseil
Vona
Vumetric
Yack Sécurité Inc.
YottaSec
ZoneTI Securité

MANAGED SECURITY SERVICES AND/OR OUTSOURCING (MSSPs)

Adaptiv Networks
Arc4dia
ATOS
Cisco Systems Canada
CYVAULT
Explorio
FPE Consultant Inc.
GoSecure (CounterTack)
Indominus Inc.
Koasec

February 2025. This mapping is based on our knowledge of the industry. If you would like to request a change to a category or logo, please contact Prompt by filling out this form.



Prompt
1200 McGill College Ave suite 1650, Montreal,
Quebec H3B 4G7

promptinnov.com

Avec la participation financière de

prompt

Québec