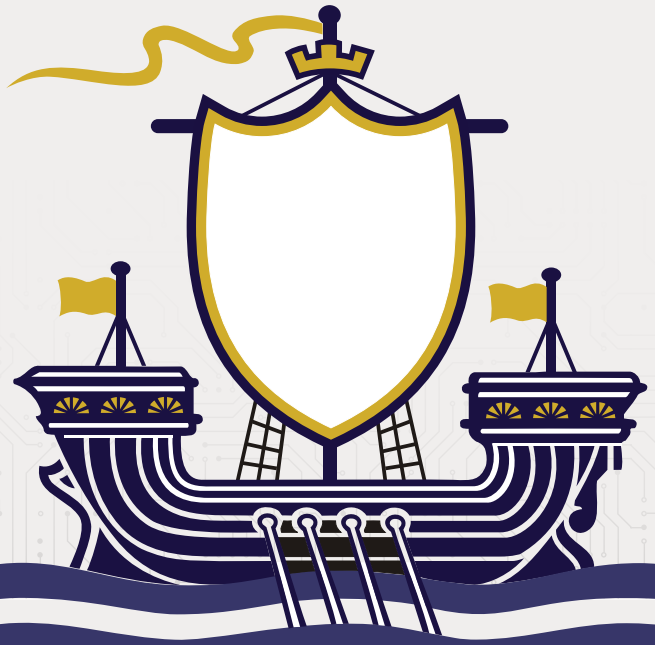
Searching for hidden talent

EXPERIENCE AND EXPERTISE IN NEW BRUNSWICK'S CYBERSECURITY COMMUNITY



ICTC CTIC

Research by

The Information and Communications Technology Council

This project is funded by the New Brunswick Department of Post-Secondary Education, Training, and Labour

Preface

As a not-for-profit, national center of expertise, ICTC strengthens Canada's digital advantage in a global economy. Through trusted research, practical policy advice, and creative capacity-building programs, ICTC fosters globally competitive Canadian industries enabled by innovative and diverse digital talent. In partnership with a vast network of industry leaders, academic partners, and policy makers from across Canada, ICTC has empowered a robust and inclusive digital economy for over 25 years.

To cite this report:

Herron, C., Rice, F., Snider, N. (April 2020), Searching for Hidden Talent: Experience and Expertise in New Brunswick's Cybersecurity Community, Information and Communications Technology Council (ICTC), Ottawa, Canada.

Researched and written by Nathan Snider (Manager of Policy and Outreach), Faun Rice (Research and Policy Analyst), and Chris Herron (Junior Research Analyst) with generous support from Arun Sharvirala (Data Scientist), Rob Davidson (Manager, Data Analysis and Research), Olivia Lin (Junior Data Analyst), and the ICTC research and policy team.

The opinions and interpretations in this publication are those of the authors and do not necessarily reflect those of the Government of New Brunswick.

Abstract

The purpose of *Searching for Hidden Talent: Experience and Expertise in New Brunswick's Cybersecurity Community* is to evaluate the magnitude and type of demand for cybersecurity personnel in the province of New Brunswick, a recognized cybersecurity hub within Canada. To this end, this study used an employer survey; key informant interviews with employers, workforce development organizations, and educational institutions; found data from job boards; and extensive secondary data from Statistics Canada and other sources. Using the National Initiative for Cybersecurity Education (NICE) Framework (an international cybersecurity workforce classification system) to compare the different data sources informing this research, the study concludes that the level of demand for cybersecurity talent in New Brunswick varies by type of role as well as each role's degree of specialization. Jobs that typically come with greater experience requirements, such as those roles that design and oversee cybersecurity programs, are in higher demand in New Brunswick than roles that could be filled by an entry-level candidate. This conclusion is reinforced by an analysis of in-demand skillsets. Addressing the challenge of a dearth of highly skilled, experienced professionals is a complex topic that hinges on a holistic understanding of the cybersecurity ecosystem and career pathways; accordingly, this study also examines cybersecurity supply, including educational institutions and workforce demographics. The report concludes by identifying several constructive opportunities to bridge the gap between supply and demand in cybersecurity in New Brunswick.

Importantly, this study concluded immediately prior to the outbreak of COVID-19 in Canada, with all primary research tools closed by February 1st, 2020. Accordingly, the statistics and figures in this report are based on stable growth experienced in the Canadian economy prior to the COVID-19 crisis. Labour demand is likely to be adversely impacted in the short term (2020), although given the continuing importance of the cybersecurity sector, it is expected to normalize again in 2021. ICTC intends to pursue continued follow-up research and will publish an addendum to this report on the impact of COVID-19 in Fall 2020.

Key Terms: Cybersecurity, Labour Market Research, National Initiative for Cybersecurity Education (NICE), New Brunswick, Workforce Development

Acknowledgements

ICTC gratefully acknowledges the time and expertise of the individuals and organizations who supported or contributed to this study, including:

Paul Archer: Director of Security, Kognitiv Spark

Atlantic Canada Opportunities Agency (ACOA)

Stanley Barnaby, Senior Manager,
Joint Economic Development Initiative

Andrew Brewer, President: CMS Consulting, Inc.

Shannon Brittany-Pollock: Workforce Strategist, CyberNB Inc.

Bulletproof

Kathryn Cameron: Chief Operating Officer, Beauceron Security Inc.

Ian Daly: IT Project Coordinator, Joint Economic Development Initiative; Co-founder & President, Kinap Solutions

Dillon Donahue: Education Framework Specialist, CyberNB Inc.

Harrison Duffley: Coordinating Instructor, Information Technology-Cybersecurity, New Brunswick Community College

Mohamed Elghazouly: Cybersecurity & Privacy Leader

Faruk Ener: Business Development Officer, Canadian Institute for Cybersecurity

Anthony English: VP/CISO, Mariner Innovations

Gerry Fairweather: Assistant Deputy Minister/ Chief Information Officer, Government of New Brunswick: Finance and Treasury Board

Daniel Hoyles: Investment Analyst,
New Brunswick Innovation Foundation

Sarah Corey Hollohan: Director, Ignite Fredericton

Susan Holt: Vice President, Strategy,
Professional Quality Assurance Ltd.

Andrew Jefferies: Cyber Consultancy Executive, Deloitte Canada

Richard Jones: Entrepreneur-in-Residence, Propel ICT Inc.

Chris Kantor: Campus Director, Eastern College

Jessica Kennedy: Program Manager,
Talent Services, Venn Innovation

Chris Lincoln: Senior Manager,
Security Practice, Bell Canada

Andrew Lockhart: Economic Development Specialist, Ignite Fredericton

Ian MacKinnon: Chief Security and Privacy Officer, Cirrus9

Jean-Marie Pelletier: Manager, Aboriginal Partnerships (Continuing Education)
The Collège communautaire du Nouveau-Brunswick

Adam Mosher: Founder and CEO,
Global Intelligence Inc.

Frank Post: Senior Director, Difenda

Jamie Rees: Enterprise Information Security Officer, WorkSafeNB

Dr. Laura Richard: Director of Research,
New Brunswick Innovation Foundation

Krista Ross: Chief Executive Officer,
Fredericton Chamber of Commerce

Larry Shaw: CEO, Knowledge Park

Cathy Simpson: CEO, TechImpact

Paul Van Iderstine, CPA, CA, CISSP, GSEC, GCCC

Table of Contents

Executive Summary

Alongside our international partners, Canada's demand for cybersecurity talent continues to increase. With each new innovative cybersecurity product entering the market, the pioneers leading the charge behind the scenes represent an increasingly diverse and specialized set of technical skills. In addition, longstanding institutions and sectors in finance, utilities, healthcare, among others increasingly require in-house cyber-security personnel to help them guard against digital attacks. Around the world and in Canada, the resounding message from employers is that it is difficult to find these skilled personnel, and this is also true for the province of New Brunswick, one of Canada's cybersecurity hubs. With a healthy cybersecurity industry, the province is seeing high demand for talented recruits, particularly those with advanced skills and ample experience.

The demand for cybersecurity personnel can be measured in numerous ways, and this study provides an overview of several different metrics for examining and comparing cybersecurity demand, both between New Brunswick and the rest of Canada, and between different types of cybersecurity jobs. Looking broadly at occupations, it is evident that cybersecurity-related roles have far lower unemployment rates than the information and communications technology sector, both in New Brunswick and Canada as a whole. Tellingly, about two-thirds (67%) of New Brunswick cybersecurity industry representatives surveyed in this study seek to expand their cybersecurity workforce in the next year. Job postings confirm a high volume of cybersecurity job openings compared with the province's population.

Using the National Initiative for Cybersecurity Education (NICE) Framework (an international cybersecurity workforce classification system) to compare different data sources informing this study, it becomes clear that the level of demand varies by type and degree of specialization of role. NICE categories with slightly greater experience needs—such as "Securely Provision" and "Oversee and Govern"—are in higher demand in New Brunswick than roles that could be filled by an entry-level candidate. However, these highly skilled, experienced professionals can be hardest to find: only about a third of New Brunswick's job postings in these categories are filled within a month, and they request an average of 6.7 minimum years of experience.

A further analysis of the skillsets that employers are looking for, as well as the barriers that they encounter in hiring, sheds additional light on this trend. While finding skilled personnel is the number one challenge employers face, this is complicated by additional considerations like high cybersecurity salaries and a lack of a clear career path for new graduates. Only one in ten (11%) surveyed employers felt that New Brunswick suffered from a lack of cybersecurity candidates: accordingly, hiring challenges expand far beyond just raw supply.

Indeed, the provincial output of entry-level cybersecurity graduates is growing as colleges and universities are quickly producing and refining their targeted programs. This study also provides an overview of the number and variety of cybersecurity programs in the province. Much like the issue of scarcity of talent for mid-career roles, there is also a dearth of diversity in New Brunswick's cybersecurity community. In this study, 28% of surveyed employers reported that their cybersecurity workforce was entirely Caucasian and male-identifying. Just over half (52%) reported having no women in cybersecurity-related roles.

Addressing the challenge of a dearth of highly skilled, experienced professionals is a complex issue that hinges on a holistic understanding of the cybersecurity ecosystem and career pathways. Nevertheless, this study identifies several constructive opportunities, such as increasing the number of experiential work-integrated learning opportunities and formalizing clear career trajectories for new graduates. As New Brunswick's cybersecurity industry continues to gain international recognition, its well-networked and collaborative ecosystem is primed for continued expansion. With a few critical considerations and adjustments, the province can confidently continue punching far above its weight in the field of cybersecurity in a national context and around the world.

Introduction

Cybercrime is an increasingly salient issue for Canada and the world. As organizations across Canada begin to adopt cloud computing, Internet of Things (IoT) devices, and increasingly integrated digital systems, nationwide vulnerability to cybercrime also increases. Cyberattacks can range from denial-of-service attacks (where the attacker renders an IT system unresponsive, possibly to demand a ransom), to phishing (messaging to trick users into providing personal or other information), to malware (malicious software installed on a user's computer without consent), etc. Familiar threats such as data breaches have broader ramifications as more data is collected and available to be compromised. New technologies such as wearable smart devices, autonomous vehicles, interconnected and smart infrastructure, cloud computing, automation, AI, and malware-for-hire are but a few of the emerging trends causing increasing alarm in the cybersecurity sector.[1]

Understanding Cybersecurity

Cybersecurity can be broadly defined as the practice of protecting oneself and one's organization from digital attacks.[2] This includes network, system, and program security; training personnel to be cyber-aware; and planning for and responding to incidents. As such, businesses in the cybersecurity industry have been under pressure to expand and innovate as cybercrime grows in size and sophistication.

In 2017, just over one-fifth (21%) of all Canadian businesses of all sizes[3] were impacted by a cybersecurity incident,[4] and Canada ranked third worldwide for the number of data breaches in the country, next to the United States and the United Kingdom.[5] Furthermore, the Canadian Internet Registration Authority (CIRA) reported in 2018 that four in 10 Canadian SMEs experienced phishing and virus attacks: about a third experienced Trojans and spyware, while 27% had been attacked by ransomware.[6] As attacks increase in frequency and sophistication worldwide, so too does the need for skilled and responsive talent. In one 2017 international study, 66% of information security workers responded that they did not feel adequately staffed to address these growing threats.[7]

Cybersecurity professionals are responsible for protecting organizations and individuals from digital attacks. People with the skills to design, operate, and maintain secure systems while responding to threats are in demand not only across Canada but also throughout the United States and the world at large. This study specifically focuses on the demand for cybersecurity personnel in New Brunswick, situating the province within a larger national and international context.

[1] *Center for Cyber Safety and Education, 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Frost & Sullivan, 2017, https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf, p. 2; Deloitte and the Toronto Financial Services Alliance, The changing faces of cybersecurity: Closing the cyber risk gap, 2018, https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF, p. 5.*

[2] *Cisco, "What Is Cybersecurity?" n.d. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html*

[3] *In 2012, Public Safety and Emergency Preparedness Canada noted that businesses with fewer than 250 employees were the largest growth area for targeted cyber attacks; furthermore, in 2012, 69% of surveyed Canadian businesses with under 500 employees reported a cyber attack, with an average of $15,000 per attack lost. The same report suggested developing internal policies, training an internal employee to be responsible for cybersecurity, and consulting cybersecurity professionals externally where necessary. (Department of Public Safety and Emergency Preparedness Canada, Get Cyber Safe Guide for Small and Medium Businesses, https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx.)*

[4] *Statistics Canada, Impact of cyber crime on Canadian businesses, 2017. https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-eng.htm*

[5] *Symantec Corporation, Internet Security Threat Report, 2017. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf, p. 50.*

[6] *Canadian Internet Registration Authority (CIRA), Fall 2018 Cybersecurity Survey, 2018, https://cira.ca/2018-cybersecurity-survey-report.*

[7] *Center for Cyber Safety and Education. 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, 2017, p. 2.*

Cybersecurity in the Province of New Brunswick

In Canada, the province of New Brunswick is a significant centre of cybersecurity activity, and Fredericton in particular has been identified as one of the country's seven academic cybersecurity hubs.[8] The Canadian Institute for Cybersecurity (CIC), a research cluster that features cybersecurity training and entrepreneurial as well as academic development, is housed at the University of New Brunswick, Fredericton.[9] Furthermore, Opportunities New Brunswick and its subsidiary, CyberNB, have made significant investments in the province to subsidize job-creating organizations such as the Canada Nuclear Laboratories (CNL) National Innovation Centre for Cybersecurity[10] and the Siemens Cybersecurity Centre.[11] Government and local investor funding (such as Ignite Fredericton, the New Brunswick Innovation Foundation, and the Technology Venture Corporation) complement the province's academic expertise, making it an ideal place for cybersecurity startups to get off the ground.[12]

As a foundational part of this study, ICTC spoke with industry representatives from across the province who were able to comment on New Brunswick's unique and complex cybersecurity ecosystem.[13] Several of the themes identified by these interviewees provide important context to this report's focus on supply and demand in cybersecurity.

Strong relationships between academia and private industry often promote healthy economic development, and in New Brunswick this relationship is visible on numerous levels.

Universities work directly on innovative research and development projects; colleges correspond with industry through program advisory committees to ensure that programming remains innovative, and industry connects directly with elementary and secondary schooling to provide mentorship opportunities for young men and women. Several characteristics unique to the province work together to create these connections, including size.

> *Due to the expanding industry, [New Brunswick] has a lot of activity here from well-recognized businesses. There is a great link between education, industry, and government that is rare to see. Connections with ministry officials and other policymakers are much easier to foster than in urban centres.*
>
> - Dillon Donahue, CyberNB

[8] *Deloitte and the Toronto Financial Services Alliance, The changing faces of cybersecurity: Closing the cyber risk gap, 2018, p. 15.*
[9] *Canadian Institute for Cybersecurity, "About the Canadian Institute for Cybersecurity," University of New Brunswick, accessed May 22, 2019, https://www.unb.ca/cic/about/index.html*
[10] *"New National Innovation Centre for Cybersecurity opens in New Brunswick," DCN News Services, June 1, 2018, https://canada.constructconnect.com/dcn/news/projects/2018/06/new-national-innovation-centre-cybersecurity-opens-new-brunswick*
[11] *"Siemens to open cybersecurity centre in Fredericton, create up to 60 jobs," CBC News, May 30, 2018, https://www.cbc.ca/news/canada/new-brunswick/siemens-cybersecurity-centre-fredericton-jobs-1.4684636.*
[12] *"Why New Brunswick is Canada's Cybersecurity Hub," Media Planet Industry and Business, September 2017, http://www.industryandbusiness.ca/insight/why-new-brunswick-is-canadas-cybersecurity-hub.*
[13] *The sixteen key informant interviews included industry, government, and not-for-profit executives, and the most common roles were CISOs, CTOs, Chief Security Officers, and Talent Managers.*

Another respondent explained that New Brunswick's relatively early consideration of cybersecurity (with provincial investments in relevant infrastructure beginning as early as the 1990s)[14] allowed public policy initiatives to mature alongside industry. Other interviewees suggested that the province's ability to come to the table and meet with industry for coordinated planning was key to early success.

Strategic investments from the provincial and federal governments aided in the creation of a strong industry foundation; however, industry felt a commitment to proactively help shape policy whenever possible. Interviews overall found that industry players felt a strong sense of support and encouragement for continued growth, both within the private sector and from the public sector.

> *When we talk about threats to the cybersecurity industry in New Brunswick, one of the benefits New Brunswick industry has over larger metropolitan areas, like Toronto or Vancouver, is that there is less raiding of cybersecurity talent. Since there are fewer competing industries within the province, the cybersecurity practitioners tend to be more collaborative.*
>
> – Paul Van Inderstine, CPA, CA, CISSP, GSEC, GCCC

Respondents also cited a strong sense of community among their peers, often highlighting other organizations for their valuable contributions to the cybersecurity ecosystem. Nearly three-quarters of respondents explicitly mentioned successful workforce development efforts (both nationally and abroad) of non-profit organizations as well, such as CyberNB. Over a third of respondents also spoke of the province's support of early education programs, such as CyberTitan,[15] which help inspire and attract youth to the field. As additional evidence of the NB cybersecurity ecosystem's strong educational focus, 80% of interviewees mentioned their involvement in the K-12 and post-secondary space. Many promote workforce development programs, develop industry recognition, and about two-thirds of these respondents did so outside of their professional obligations. The strong connection between the cybersecurity industry and workforce development and training efforts comprises a foundational piece of context for understanding cybersecurity demand and supply in the province of New Brunswick.

[14] Kritsonis, Ted, Media Planet. Fredericton, NB – a National Leader in Cyber Security, 2017. http://www.industryandbusiness.ca/development-and-innovation/fredericton-nb-a-national-leader-in-cyber-security

[15] CyberTitan, "Canadian Youth Cyber Education Initiative," 2020. https://www.cybertitan.ca/

UNDERSTANDING CYBERSECURITY DEMAND

in Canada and New Brunswick

Business, governments, national and international industry associations are experiencing an increased need for employees with experience in cybersecurity. Cybersecurity personnel may have roles ranging from "ethical hackers," who test the limits of existing security strategies, to high-level cybersecurity strategists, to hardware or database experts. A 2017 study with nearly 20,000 respondents from cybersecurity professionals across 170 countries forecasted a global cybersecurity labour shortage of 1.8 million people by 2022, and a corresponding North American shortage of 265,000 people by the same year.[16] This paper seeks to understand the demand for cybersecurity personnel in New Brunswick, determine whether or not the province is facing a cybersecurity labour gap, and trace trends in cybersecurity employment and skills needs.

Cybersecurity Demand: Magnitude & Trends

By all metrics, cybersecurity demand is high both in Canada and New Brunswick, however, different approaches to measuring cybersecurity demand reveal distinct trends. While an assessment of employment using Statistics Canada data highlights low unemployment rates in cybersecurity-related roles and can illustrate trends over time. More specific tools, such as ICTC's New Brunswick Cybersecurity Employer Survey,[17] a detailed analysis of cybersecurity job postings, and insights from key industry informants, paint a more granular picture of the forces at play in cybersecurity hiring in the province.

Measuring Employment through National Occupational Classifications (NOCs)

Currently, there is no single National Occupational Classification (NOC)[18] that represents all cybersecurity roles. However, ICTC has identified several cybersecurity-related occupational codes in the national data to map trends in cybersecurity jobs across Canada and by province.[19] These are:

0213 Computer and information systems managers

2172 Database analysts and data administrators

2283 Information systems testing technicians

2281 Computer network technicians

2171 Information systems analysts

[16]Center for Cyber Safety and Education, 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, 2017, p. 2.
[17]ICTC's employer survey was distributed in autumn 2019. The target population for this survey was any company in New Brunswick that employed personnel in the cybersecurity sector, and outreach targeted cybersecurity consulting firms, large technology-related employers, and other related sectors. For more information about the ICTC employer survey, see Appendix I.
[18]This is the standard measurement of the labour force used by Statistics Canada in products such as the labour force survey and census.
[19]Information and Communications Technology Council of Canada (ICTC), "Forecasting Demand for Cybersecurity Workers in Canada: 2017-2023," https://www.ictc-ctic.ca/wp-content/uploads/2019/02/ICTC_Forecast-Cybersecurity_1.31.19.pdf

The Government of New Brunswick estimated that the number of people working in Cybersecurity NOCs in New Brunswick was 4,732 in 2018, or 0.6% of the province's total population in that year.

International reports on the cybersecurity labour gap tout global unemployment rates as low as 0%,[21] and a province-specific look at unemployment is key to understanding cybersecurity trends.

It is clear that while New Brunswick's cybersecurity-related unemployment rate is not as low as 0%, employment in the cybersecurity subsector outperforms both the wider tech (ICT) sector and employment in general. **Figure 1** highlights the differences between New Brunswick's cybersecurity unemployment rate, its ICT unemployment rate, and the provincial and national averages for unemployment. Despite a slight upward trend in unemployment over the last five years, New Brunswick's cybersecurity-related workers are much less likely to be unemployed than the rest of the province's workforce, as are employees in the ICT sector. Furthermore, New Brunswick's ICT and cybersecurity-related workers have far lower unemployment than the Canadian average across all industries: in 2019, New Brunswick had 1.24% unemployment for cybersecurity-related workers and 2.94% for ICT workers, as compared to the Canadian average of 5.66% and the New Brunswick provincial 7.95% (for all sectors).

Unemployment Rates Over Time

New Brunswick: ICT Sector & Cybersecurity and Canada Overall

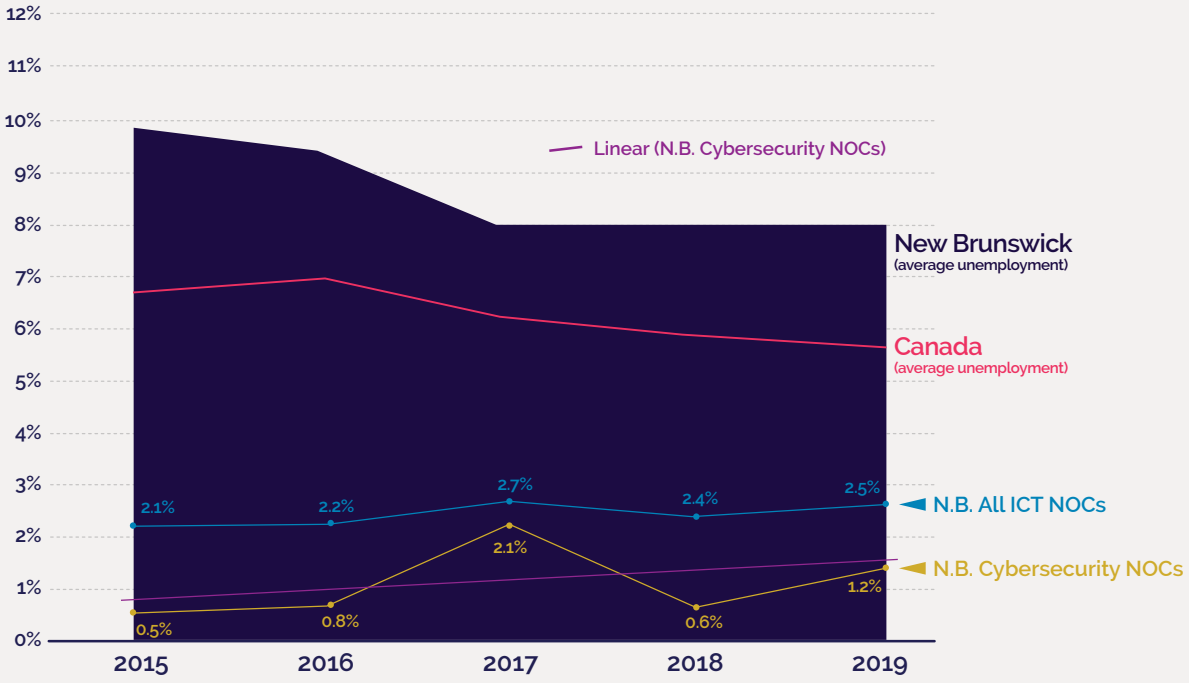


Figure 1: Unemployment Rates: New Brunswick ICT and Cybersecurity NOC groups compared with Canada and New Brunswick average unemployment, 2015-2019, Statistics Canada Labour Force Survey. Data suppressed by Statistics Canada is excluded from this chart in determining annual averages. see Appendix I for further details.

[21] *See, for example, stories like: Mack Gelber, "This tech filed just hit an astonishing 0% unemployment rate," Monster, n.d. https://www.monster.com/career-advice/article/tech-cybersecurity-zero-percent-unemployment-1016*

The slight upwards trend in cybersecurity-related unemployment over the last five years is an interesting pattern. Importantly, this trend may or may not be linked to the jobs within each NOC that pertain to cybersecurity specifically, as each of the five NOCs contains numerous job titles, some directly related to security, others not related (for example, an IT manager may or may not be responsible for the digital security). In order to understand the demand for cybersecurity-specific jobs, the section New Brunswick's Cybersecurity Marketplace: In-Demand Jobs and Skills delves further into cybersecurity-specific roles using evidence other than what is available from Statistics Canada. Regardless, as **Figure 2** below illustrates, the five cybersecurity-related occupations have experienced a compound annual growth rate of 3.0% over the last 15 years in the province. Accordingly, if both unemployment and the number of jobs in cybersecurity are trending up (albeit only very slightly in the case of unemployment), it is possible that overall labour supply in one or more of these NOCs exceeds demand. As this paper explores in later sections, this may be partially explained by the types of in-demand jobs we see in cybersecurity, which tend to be roles that demand a higher degree of professional experience than a recent graduate can offer. As the section New Brunswick's Cybersecurity Marketplace: In-Demand Jobs and Skills explores, while numerous types of cybersecurity roles are in very high demand, these roles are also the most difficult to fill without a high degree of specialization. In addition, these trends may again be explained by the number of jobs within each NOC that are not cybersecurity specific.

Jobs in Cybersecurity-Related Fields Over Time

New Brunswick

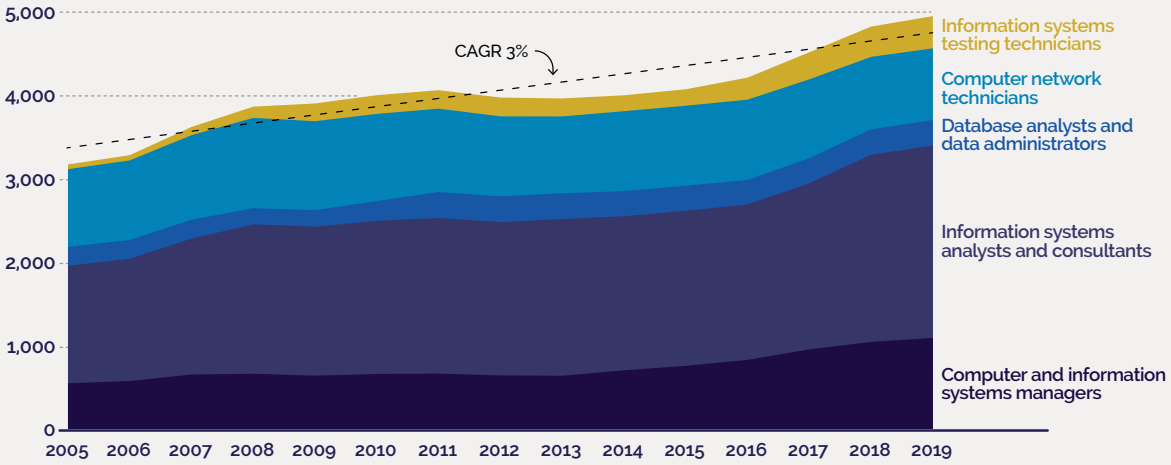
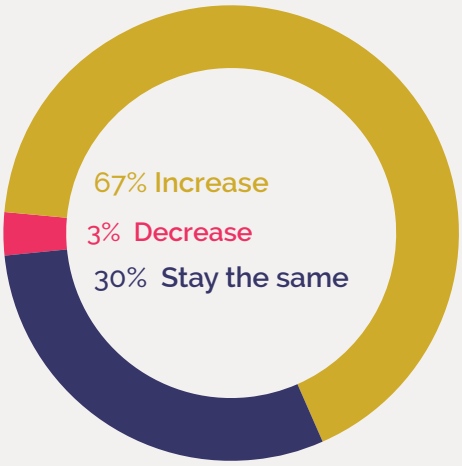


Figure 2: The number of jobs in each of five cybersecurity related NOCs in the province of New Brunswick from 2005 to 2019, representing 15 years of job growth with a CAGR of 3.0%.

Other evidence, more specific to cybersecurity than NOCs, points towards a growing number of jobs for individuals who fight and prevent cybercrime in New Brunswick. In ICTC's 2019 employer survey, two-thirds of respondents (67%) felt that their cybersecurity workforce would increase over the next year, and of that more than half (60%) believed it would increase by 2 or more employees (see **Figure 3**).

Over the next year, do you expect that your cybersecurity workforce in New Brunswick will...



How many cybersecurity personnel would you ideally like to hire in New Brunswick over the next year?

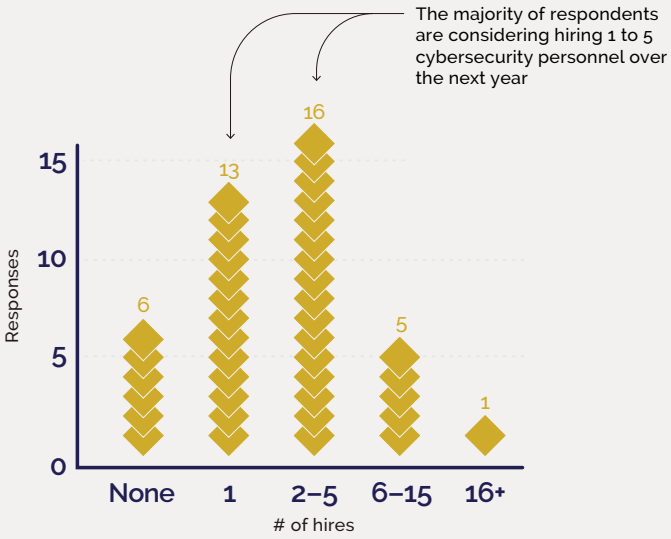


Figure 3: Cybersecurity employers' evaluations of the number of staff they intend to hire in the coming year. On the left, employers' reasonable expectations are portrayed, while the right features employers' ideals. Source: ICTC

Just as numerous employers expect to increase their workforces over the next year, even more striking is the fact that only 3% of employers anticipate a decrease in personnel.

Employers expectations to expand their workforces are seconded by an analysis of job postings in the province. Over the course of six months, ICTC collected information from job boards in New Brunswick on the frequency and types of cybersecurity jobs being posted. While a detailed analysis of job postings by type of role follows later in this report, **Figure 4** illustrates some key fast facts about cybersecurity job postings in New Brunswick. The number of new posts by month suggests a pre-Christmas lag in hiring, but there is an average of approximately 7.5 new roles posted per month over the half year that ICTC collected data. Looking at job postings by city, Fredericton and Saint John are clear leaders in the province for cybersecurity jobs, complemented by the presence of key employers in their regions: IBM leads for hiring in Fredericton, Irving Oil in Saint John, and Mariner in both Saint John and Moncton.

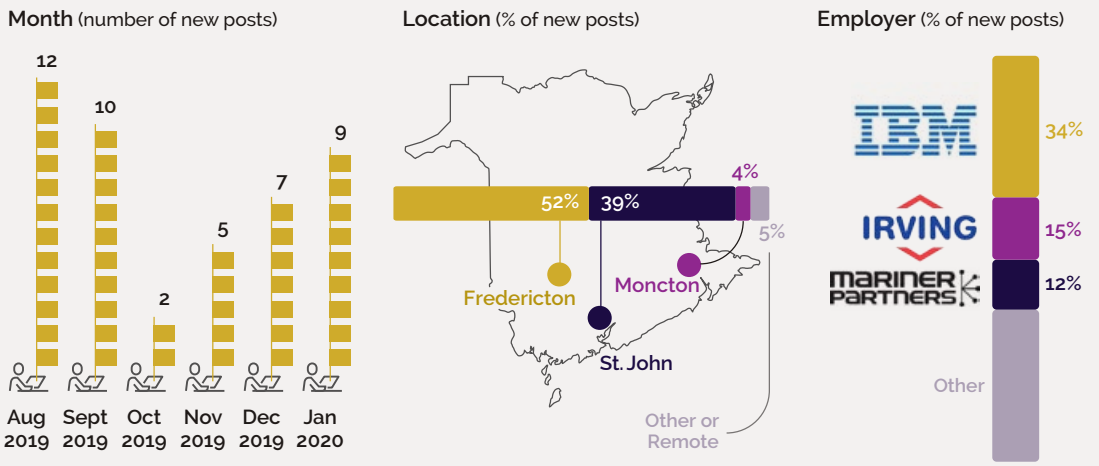


Figure 4: Source, ICTC

ICTC also collected cybersecurity-related job board information from the rest of Canada. **Figure 5** illustrates a trend that New Brunswick shares with other Canadian provinces: across the board, a dip in the number of cybersecurity-related job postings can be seen in the fall, particularly in October, with an increase seen in the new year. New Brunswick's portion of postings by month closely matches the Canadian median (monthly median taken from all provincial postings).

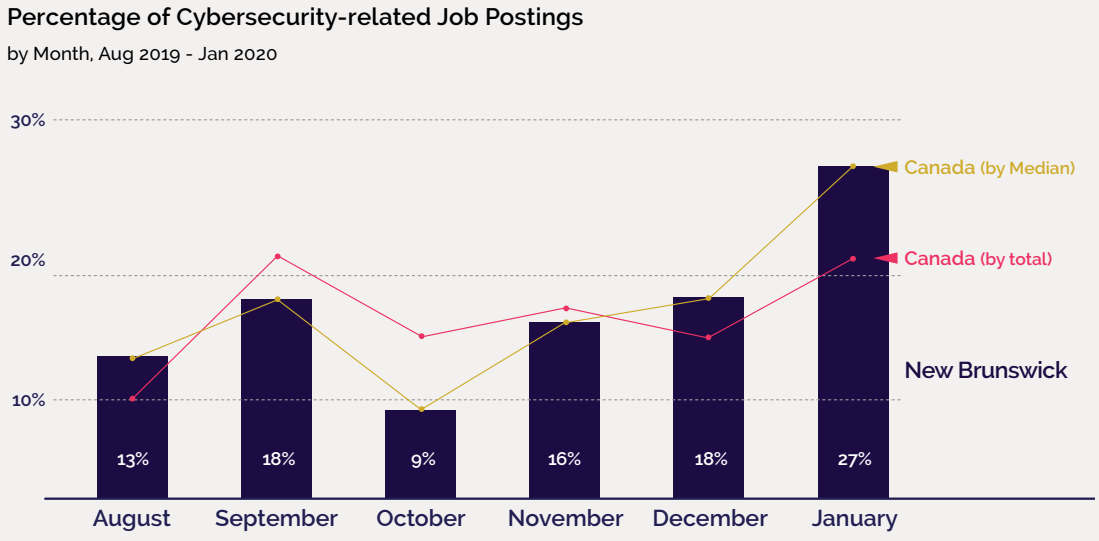


Figure 5: A comparison between the raw number of postings (new and old) by month: New Brunswick, Canada by total postings, Canada by median (from all provinces). Source: ICTC, 2020

Another way to examine this job-posting data is through each province's share of the Canadian population compared to its share of cybersecurity job postings, revealing that Ontario, Nova Scotia, PEI, and New Brunswick are performing on par with or higher than their population suggests they should.

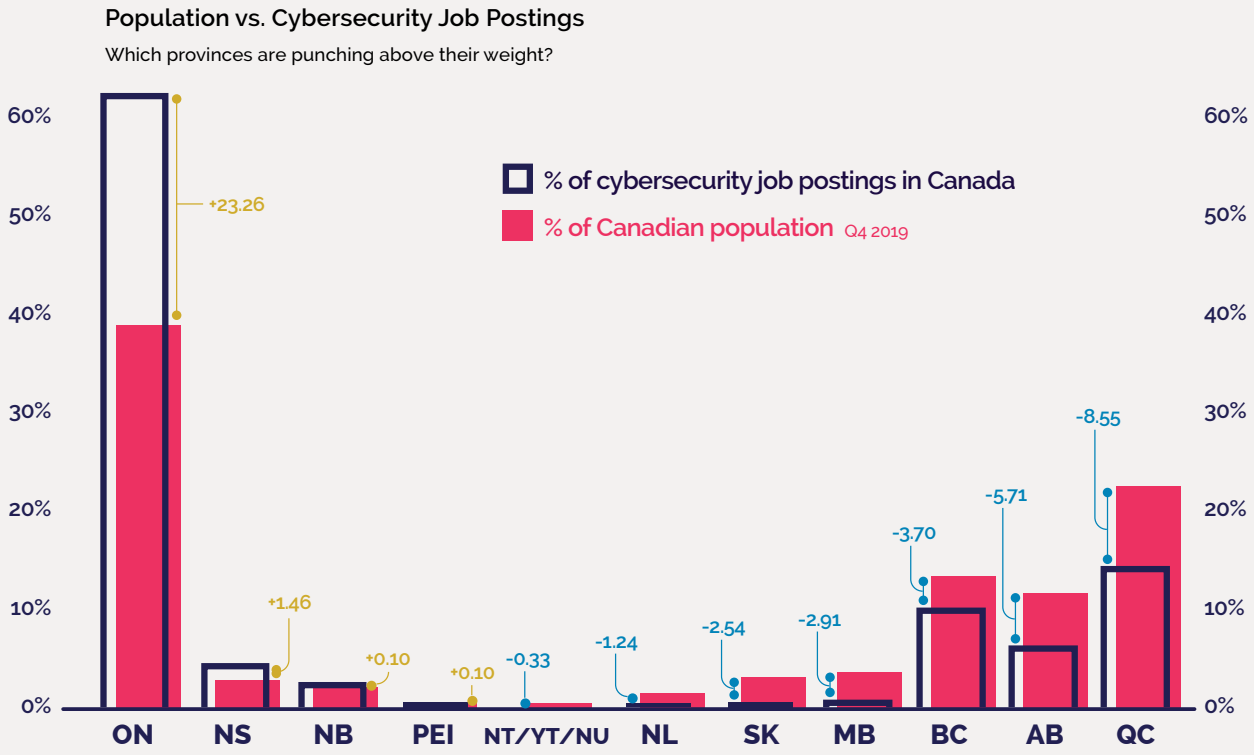


Figure 6: Provinces' and Territories' proportion of the Canadian population compared with their proportion of posted cybersecurity roles. Job posting data is from January 2020. Source: ICTC, Statistics Canada.

Cybersecurity Demand: Employers by Sectors and Size

Cybersecurity professionals may work for dedicated cybersecurity firms and organizations, academic institutions, government bodies, or be embedded specialists in a wide variety of sectors. On the other hand, many cybersecurity personnel are generalist IT staff members who have been assigned responsibility for cybersecurity. Perhaps unsurprisingly, investment in cybersecurity personnel is more common in larger organizations across Canada,[23] and this is also true for ICTC's survey respondents in New Brunswick: while nearly a third (29.6%) of small organizations (<100 employees) reported having no cybersecurity personnel, only one in 14 (7.4%) of medium and large organizations (100+) reported the same.[24]

Across Canada and in New Brunswick, numerous industries employ cybersecurity professionals. **Figure 7** identifies the industries most likely to employ at least some cybersecurity personnel, beginning with Finance and Insurance, where 91.6% of the sector in Canada has at least one employee designated to cybersecurity. Notably, in the Canadian context, utilities and natural resources (such as oil and gas or nuclear energy production) are significant additions to the list of potential cybersecurity employers, a trend with great relevance to the New Brunswick context.

Cybersecurity Workforce Strength in the Top Ten Industries Employing Cybersecurity Personnel in Canada

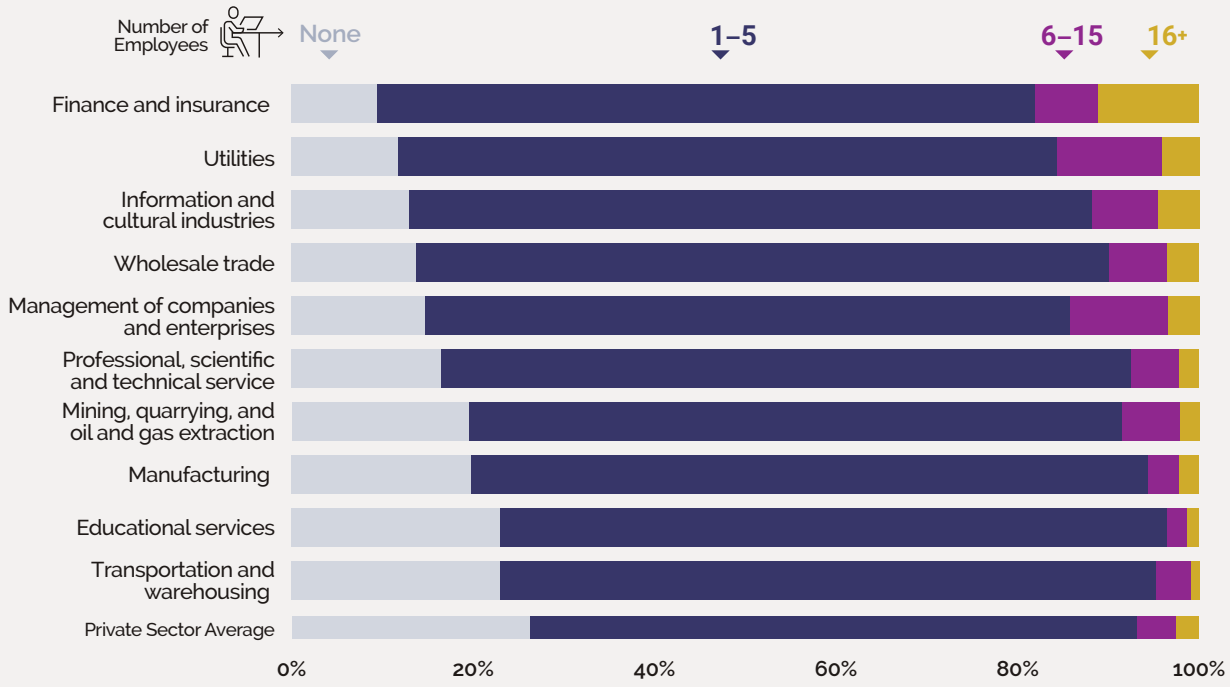


Figure 7: Percentage of businesses indicating the number of employees primarily responsible for overall cybersecurity, including the top 10 industries that are the most likely to have at least one employee responsible for cybersecurity, as well as the private sector average. Source: Statistics Canada 2017 Survey of Cybersecurity and Cybercrime.

[23]These emerging cybersecurity professionals work across all sizes of enterprise, but are most commonly found in larger organizations. The Canadian Chamber of Commerce's ICT Adoption Survey of 2017 found that a business' size played a significant role in their degree of investment in cybersecurity: while 85% of large organizations surveyed had conducted staff training in cybersecurity within a three period, only 26% of "micro" businesses and 45% of small businesses had done the same.
[24]Source: New Brunswick Cybersecurity Employer Survey, ICTC, 2019.

Not all industries are rushing to hire cybersecurity personnel, however. In the same Canada-wide survey, businesses that did not hire any cybersecurity personnel reported two main reasons for this: (a) using external consultants rather than their own staff, and/or (b) not feeling that cybersecurity was a high enough risk to their business. Cybersecurity consulting comprises a significant portion of the cybersecurity sector, and many organizations use consultants if and when they do not have the resources or perceived need to hire their own dedicated staff members. The two main reasons that respondents gave for not hiring cybersecurity personnel are broken down by industry in **Figure 8**.

Two Main Reasons for not Having Employees Responsible for Cybersecurity by industry, Canada 2017

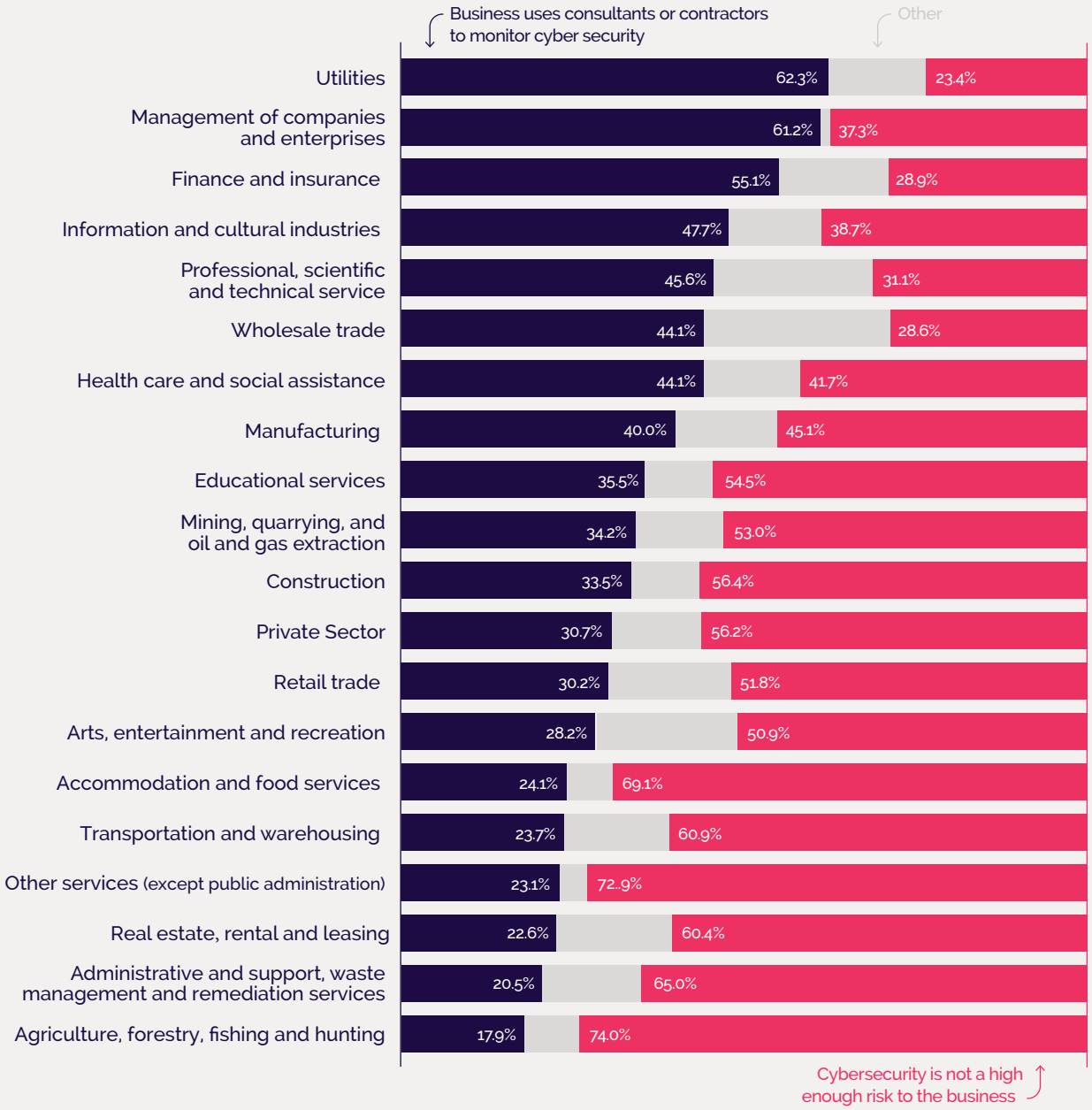


Figure 8: Source: Statistics Canada, Canadian Survey of Cyber Security and Cybercrime, 2017.

Across the entire private sector in 2017, 74% of Canadian businesses had employees primarily responsible for cybersecurity, and this was more common among large- and medium-sized businesses.[25] Similarly, in New Brunswick, 75% of employer survey respondents had at least one employee primarily responsible for cybersecurity, and the majority of organizations without cybersecurity staff (80%) had fewer than 100 employees overall.[26] In other words, smaller organizations, both in New Brunswick and in Canada, are less likely to have dedicated cybersecurity personnel.

Among the Canadian businesses who did not have anyone dedicated to cybersecurity (26%), about half indicated that they were not worried enough about cybersecurity risks (though no New Brunswick respondents made the same comment, see Figure 9)[27] while about a third used consultants or contractors in place of embedded staff (31%).[28] In Figure 9, New Brunswick survey respondent reasons for not hiring cybersecurity personnel are compared with the Canadian private sector and ICT sector averages. Overall, awareness of cybersecurity risks, likelihood of using cybersecurity contractors, and the use of cyber liability insurance was much higher among New Brunswick survey respondents, although this is likely due to the type of respondent inclined to respond to a cybersecurity-themed survey. While more New Brunswick organizations reported having inadequate resources to employ a cybersecurity professional, neither New Brunswick nor Canadian businesses felt that they were simply unable to find an adequate hire.

Main Reasons for Not Employing Personnel Primarily Responsible for Cybersecurity

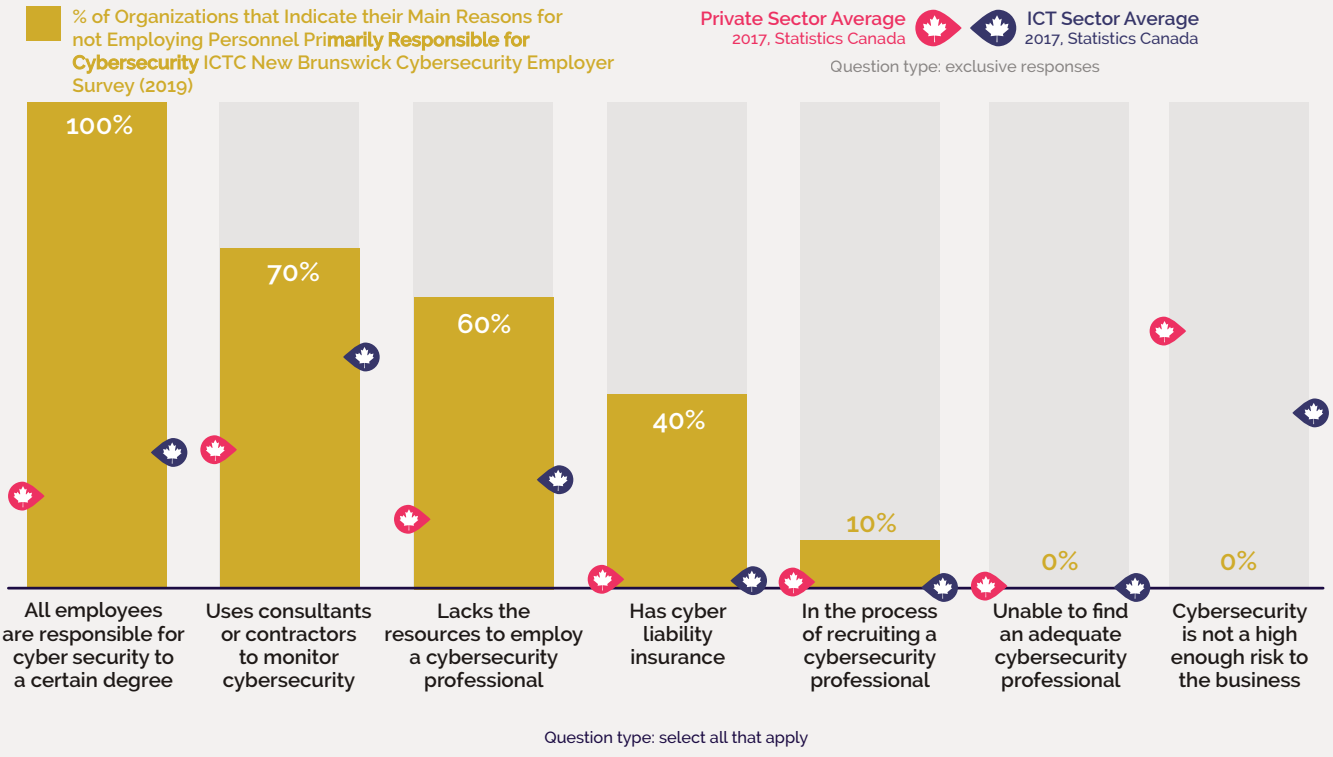


Figure 9: Of the industries less likely to have cybersecurity personnel, the main reasons for not hiring any are compared. Source: Statistics Canada, Canadian Survey of Cyber Security and Cybercrime, 2017.

[25] *Statistics Canada, Impact of cybercrime on Canadian businesses, 2017.*
[26] *New Brunswick Cybersecurity Employer Survey, ICTC, 2019.*
[27] *Note, however, that this comparison is drawn from two very different data sources. While the ICTC New Brunswick Cybersecurity Employer Survey and Statistics Canada's Survey of Cybersecurity and Cybercrime used the same response options, ICTC's survey was targeting organizations known to employ cybersecurity personnel, whereas Statistics Canada sampled the entire private sector.*
[28] *Statistics Canada, Impact of cybercrime on Canadian businesses, 2017.*

NEW BRUNSWICK'S CYBERSECURITY MARKETPLACE:

In-Demand Jobs and Skills

Understanding Workforce Composition and Demand through the NICE Framework

Cybersecurity personnel are becoming increasingly essential investments for Canadian organizations: overall, businesses across Canada spent $8 billion on salaries for employees, consultants, and contractors in 2017.[29] One way to understand the breakdown of cybersecurity staff by role is through the categories supplied by the National Initiative for Cybersecurity Education (NICE) Framework.[30] This American framework is adopted by organizations across the world with the intention of adopting standardized terminology for cybersecurity jobs and skills, and it breaks the workforce into seven key types of roles used to understand workforce composition and demand in the analysis to come.[31]

> *We want cybersecurity to be one language across the world. If you're taking an education course in Australia, it's going to match the education being offered in Canada and the US. When jobs are being posted, everything properly matches up. [The framework] really encourages a common lexicon.*
>
> - Dillon Donahue, CyberNB

Another interviewee suggested that the province's adoption of NICE is due in large part to the leadership of academic partners. Having taken the time to better understand and evaluate the value of a consistent industry framework, academia began changing program outcomes to align more closely with NICE naming and skills criteria.

[29]Statistics Canada, Impact of Cybercrime on Canadian Businesses, 2017.
[30]This framework was originally developed by the U.S. Department of Commerce as a collaborative effort between industry and academia to better define, assess and understand the diversity attributed to the cybersecurity workforce. Newhouse W., Keith S., Scribner B., & Witte G., National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, National Institute of Standards and Technology, 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf pg. 11.
[31]National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, National Institute of Standards and Technology, 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf, At the time of writing, CyberNB has stated that they intend to create a New Brunswick-specific version of the NICE Framework. In turn, the Information Technology Association of Canada (ITAC) has been commissioned by Employment and Social Development Canada (ESDC) to create a Canadian version of the same.

	Categories	Descriptions[32]	Common Job Titles in Canada[33]
SP	Securely Provision	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.	• Security/Risk Manager • Systems/Security Architect • Software/Systems Developer/Planner • Security Analyst
OM	Operate and Maintain	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.	• Data/Database or Security Administrator • Knowledge or Security Risk Manager • Technical Support or Customer Assistance Representative • Network/Systems Administrator/Analyst
OV	Oversee and Govern	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.	• Chief Information Security Officer • Cyber Strategy Analyst • Cyber Policy Analyst • Cyber Communications Analyst • Cyber Program Manager • Project and Acquisitions Managers
PR	Protect and Defend	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.	• Cyber Analyst • Security/Cyber Defense Infrastructure Engineer • Cyber Incident Responder • Vulnerability Analyst • Security Operations Centre Manager
AN	Analyze	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.	• Threat Intelligence Analyst • Cyber Analytics Manager • Data Scientist • Language Analyst/Computational Linguist
CO	Collect and Operate	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.	• Ethical Hacker/Collections Operator • Cyber Operational Planner • Threat Hunter/Cyber Operator
IN	Investigate	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.	• Cyber/Digital Forensics Analyst • Cyber Investigator

Figure 10: NICE Framework Workforce Categories

[32]National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, National Institute of Standards and Technology, 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf
[33]Based on information from CyberNB, as well as a 2018 publication by Deloitte that connected the NICE framework to the Canadian context: Deloitte and the Toronto Financial Services Alliance, The changing faces of cybersecurity: Closing the cyber risk gap, 2018.

A small number of industry partners voiced concerns regarding the framework's US origin (and therefore its applicably to the Canadian context), particularly with regard to the Canadian market's tendency to advertise broad roles that overarch multiple NICE categories. Industry leaders from small- to medium- sized companies voiced concern that should the NICE framework be broadly adopted, it would lead to restrictive and often overly specific job descriptions that would curtail the hiring of internationally skilled talent or those from non-academic or non-technical backgrounds. However, interviewees also noted that this problem could be solved if there were greater international consensus over the framework's use.

> *We all need to work together and figure out that it's not just New Brunswick, Ontario or even the rest of Canada who need to sign on to this [the NICE framework] … We simply don't want to run into a problem where someone is highly educated from Europe or the Middle East, but because we don't understand their education, they end up in an unrelated role that they're overqualified for.*
>
> - Dillon Donahue, CyberNB

The benefits of using a framework that is increasingly consistent around the world seemed to outweigh the concerns shared by industry representatives. Many respondents have already begun redeveloping their programming outcomes and hiring processes to better reflect the industry standard. Additionally, organizations with strong ties to the US or international markets (via other office locations, clients, or partners) noted that adopting NICE added clarity and ease-of-access related to immigration processes and visas.

Growth Rates in Cybersecurity-Related Occupations

While unemployment is low for the cybersecurity workforce in New Brunswick (as illustrated by Figure 1 above), some occupations are clearly more in-demand than others. **Figure 11**, below, shows each NOC across two different values: the raw number of jobs in that NOC in New Brunswick in 2019, and the five-year annual average growth rate (AAGR, 2015-2019) that shows to what extent that job has been growing over time. For example, while Information Systems Testing Technicians only comprise 386 jobs, they have exhibited very high average growth (15.7%) over the last five years. Balancing raw number of jobs and growth rate, it is clear that there are three NOCs that are performing well (with regard to employment numbers and growth in future) in New Brunswick, and two that are underperforming in comparison.

Database Analysts and Data Administrators have low employment numbers and low growth, and Computer Network Administrators have relatively high numbers but a negative growth rate year over year, suggesting that the numbers of jobs in these occupations with either stay low or slowly shrink over time.

Number of Jobs and 5-Year AAGR in New Brunswick

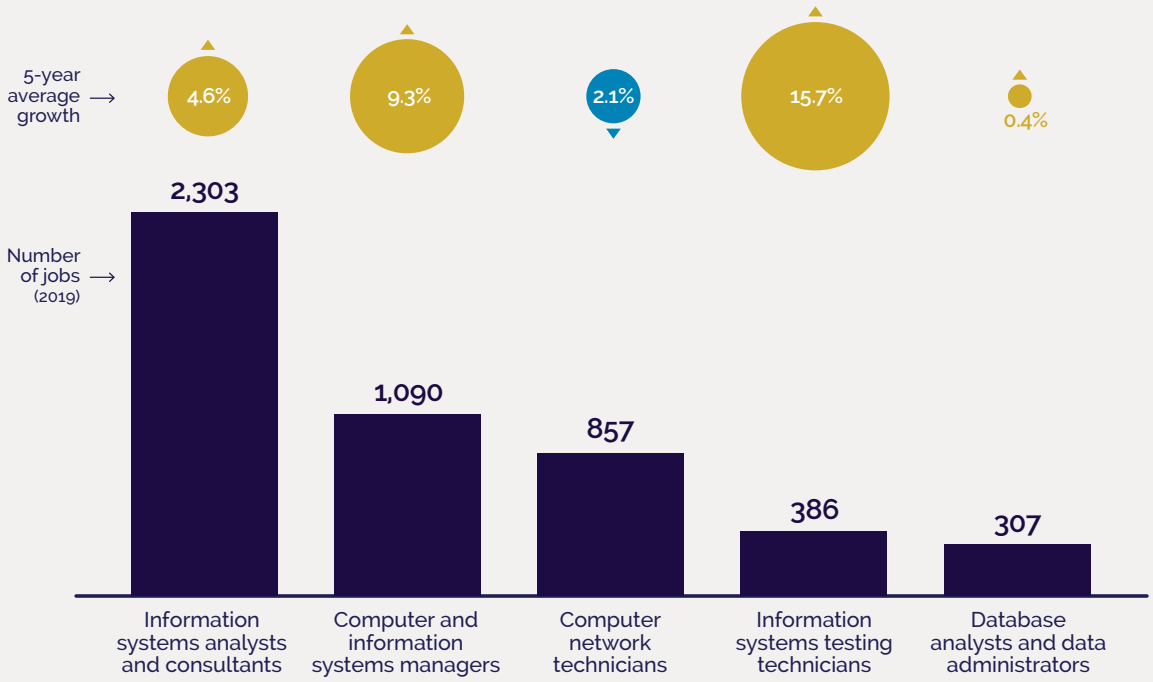


Figure 11: Comparing the raw number of jobs in 2019 for each of the five cybersecurity-related occupations and 5-year AAGR of each role. Source: Statistics Canada.

To compare findings from Statistics Canada with other data sources, each NOC can be roughly mapped to the NICE framework. It is important to note that this comparison is illustrative but not conclusive, as it is not a one-for-one match: the NOCs and NICE framework are not directly paired, and the many job titles that fall within each Canadian NOC might be attributed to a variety of NICE categories. As such, **Figure 12** below represents a model of best fit. When the five cybersecurity-related NOCs are paired with NICE framework categories, as in **Figure 10**, it is evident that the three higher-performing NOCs are best placed within two NICE categories: Securely Provision (1) and Oversee and Govern (2).

NOC	Category Title	Illustrative Cybersecurity Related Job Titles[34]	NICE Equivalent[35]
0213	Computer and information systems managers	• Manager, Information Technology • Manager, Computer System Operations • Manager, Network Design	OV — Oversee and Govern
2171	Information systems analysts and consultants	• Security Analyst or Consultant • Systems Security Planner • QA Analyst or Auditor	SP — Securely Provision
2172	Database analysts and data administrators	• Database Architect or Analyst • Systems Analyst, Electronic Data Processing • Data Administrator	OM — Operate and Maintain
2281	Computer network technicians	• Local Area Network Manager or Technician • Network Administrator	OM — Operate and Maintain
2283	Information systems testing technicians	• Software or Application Tester • Systems Testing Technician	SP — Securely Provision

Figure 12: Cybersecurity-related NOCs from Statistics Canada and high-level NICE categories matched in a "best fit" approach by similar job titles.

In mapping each New Brunswick data source to the NICE framework, a common pattern emerges. As **Figure 13** illustrates, the employer survey also emphasizes the category Securely Provision. Interestingly, employers also highlight Operate and Maintain as an important category. While Oversee and Govern appears lower, most survey respondents fall into that category themselves and may simply not foresee hiring additional personnel in their own role.

To what extent are the following cybersecurity roles in demand for your organization, when hiring in New Brunswick?

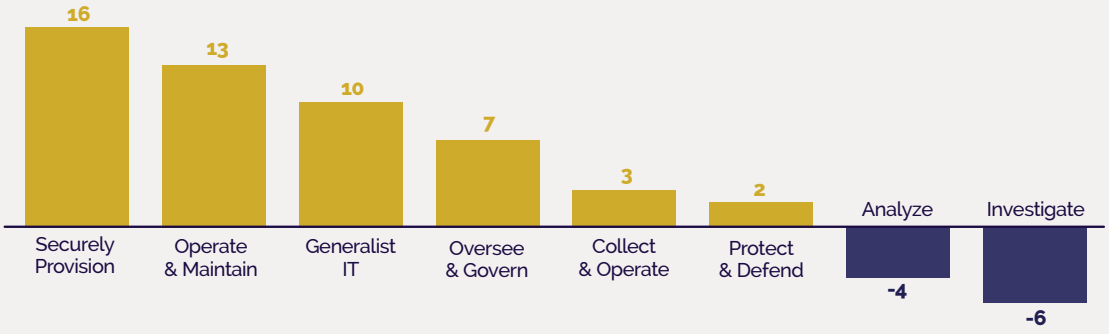
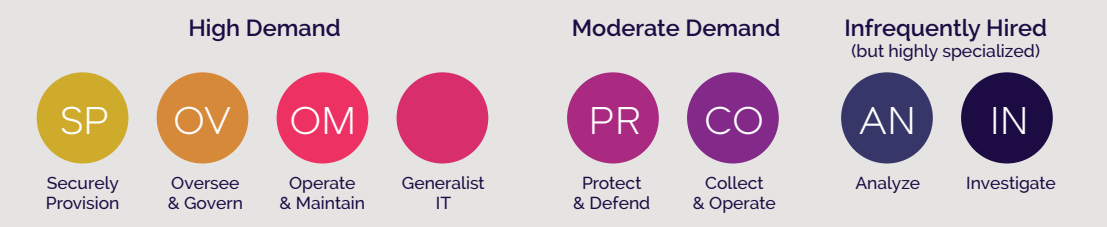


Figure 13: ICTC New Brunswick Employer Survey Respondents identify in-demand cybersecurity roles in the province. Note that in the survey, respondents were presented with descriptions of each role rather than the short-form NICE category provided here. Source: ICTC, 2020 (calculated by respondent rating, +2 "Urgent demand," +1 "Moderate demand," -1 "No demand").

[34]The job titles in this section are selected from Statistics Canada's publication "National Occupational Classification (NOC) 2011," https://www.statcan.gc.ca/eng/subjects/standard/noc/2011/introduction.
[35]Determined by matching security-related job titles from Statistics Canada to the NICE Framework Supplement: NICE Speciality Areas, Work Roles, and Task, 2018.

In addition to the New Brunswick Employer Survey, the Labour Force Survey analysis, and Key Informant Interviews, ICTC identified cybersecurity-related job postings in the province to inform its identification of in-demand roles. The table that follows draws a broad comparison between all the data sources informing this study to rank in-demand jobs and skills in cybersecurity in New Brunswick. It is possible to see that, if coded by rough match to the NICE framework, three tiers of in-demand jobs emerge. While there is some variation by source, roles that fall into the "Securely Provision" bucket are clearly the roles most frequently advertised, with high growth rates. Though surveyed employers report "Operate & Maintain" as second most urgent, secondary data suggests that senior-level roles in the "Oversee & Govern" category are also difficult to find, and the two roles compete for second most in-demand. Notably, for example, most "Operate & Maintain" coded roles are filled within a single month (as shown in **Figure 14**), suggesting that while organizations are still hiring for these roles, they are not excessively difficult to fill. A second tier of moderately in-demand roles, "Collect & Operate" and "Protect & Defend," are also somewhat in-demand, and "Analyze" and "Investigate" roles (often highly specialized) are seen as sometime hard to fill but are less frequently in demand. Furthermore, many organizations may wish to hire a Generalist IT representative who can also assist with cybersecurity, rather than equipping themselves with specialized personnel.



NB Employer Survey

By urgency ranking

- A high-level security advisor, architect, or analyst
- A preventative role responsible for risk-management administration, systems maintenance, and infrastructure security
- A generalist IT employee who has been assigned responsibility for cybersecurity
- A high-level cybersecurity executive, who provides direction, management, and strategy
- An "ethical hacker" who tests your infrastructure security
- An incident manager responsible for identifying and responding to threats
- A data scientist, cryptographer, or intelligence analyst
- A computer forensics specialist responsible for collecting digital evidence after an incident has occurred, identifying threat source or nature

Key Informant Interviews

Order not significant – mentioned as "hardest to fill in New Brunswick"

- Information/ Systems Architects
- Security Analysts
- Cloud Security Specialists
- AI Cybersecurity Product Developers
- Security Engineers
- Security Administrators
- Governance: Risk and Compliance
- Senior Cybersecurity Talent
- Software Developers (General)
- Vulnerability/ Penetration Testers
- Data Scientists
- Forensic Analysts
- Threat Hunters

NB Job Postings

By frequency of posting, similar titles aggregated

- Security Software Developer
- Manager, Director, Governance
- Security Architect or Engineer
- Security Quality Assurance
- Security Operations Centre (SOC) Personnel
- Analyst, Incident Detection and Response
- Analyst, Intelligence
- Cyber Operator

Labour Force Survey

By 5-year AAGR in NB

- Information Systems Testing Technicians
- Computer and information systems managers
- Information systems analysts and consultants
- Database analysts and data administrators
- Computer network technicians

Figure 14: In-Demand Jobs Ranked by Importance: Employers, Job Posting Analysis, Labour Force Survey, Key Informant Interviews, coded by NICE Framework.

A detailed breakdown of cybersecurity job postings in the province can shed further light on these rankings. **Figure 15** illustrates two key findings about the types of cybersecurity roles posted in New Brunswick: the number of postings by umbrella category, and the percentage of roles in each category that were filled in a single month of going live.[36] In addition, average desired years of experience (based on the minimum figure when a range was provided) illustrates the variation between these categories: it is clear that some roles require a higher degree of specialization and experience than others, most notably those in the "Securely Provision" and "Oversee & Govern" categories.

	Number of unique cybersecurity job postings in New Brunswick (Aug 2019 to Jan 2020)	Percent of roles filled within one month (Analysis excludes co-ops & jobs posted in the last month of data collection)	Average minimum desired years of experience (Analysis excludes co-ops)
Securely Provision (SP)	20	36%	5.6
Oversee & Govern (OV)	6	33%	7.8
Operate & Maintain (OM)	6	75%	3.3
Protect & Defend (PR)	5	50%	3.4
Collect & Operate (CO)	2	0%	For two roles listed, all training is provided by posting agency
Analyze (AN)	2	100%	5.5
Other (e.g., cybersecurity instructor or sales representative)	4	100%	5*

*In areas of focus other than technical cybersecurity roles

Figure 15: Breaking down cybersecurity job postings in New Brunswick, Aug 2019 – Jan 2020. Source: ICTC.

In-Demand Skillsets in Cybersecurity

As several key informants noted, job titles and descriptions in the cybersecurity ecosystem aren't always easy to categorize, as employers will, with some regularity, write very broad job descriptions so as to attract a diverse array of applicants. It was also noted that industry representatives intentionally oversaturate the skills requirements (both human and technical) for postings as limited or narrowly required qualifications, which often discourages suitable candidates. Skillsets are, therefore, both specific to particular roles and frequently cross-sectional and applicable across a wide array of job titles.

[36]Note: This analysis is based on the assumption that when a job posting is taken down, it has been filled. In addition, the analysis assumes one job per unique posting, and that a job posting from the same company, for the same role, that remains live over multiple months is for a single job rather than for rolling applications.

The analysis below inverts skillsets from least to most specific, first examining the human and transferable skills emphasized by employers in two ways: through key informant interviews and in job posting descriptions. The skillsets are roughly ranked using the order of importance assigned by respondents to ICTC'S New Brunswick Employer Survey. While skillsets will necessarily vary significantly by role, the following ranking and comparison reflects a certain degree of cross-sectional importance (particularly for less specialized skills) because both interviewees and survey respondents were naming skills that were not attached to a particular job title. Accordingly, the analysis in Figure 16 is a big-picture look at the priorities of New Brunswick employers and the transferable skills that can assist hopeful entrants to the workforce to succeed.

With regard to human and transferable skills, survey respondents ranked responsibility and professionalism, teamwork, and communication skills as the most important. Interestingly, these multiple response options are shown to be much more granular in the webscraping and interview analysis, where employers focused on independent, experienced, dedicated, and organized personnel. This emphasis on experienced and responsible professionals reinforces the overall finding that employers are frequently looking for cybersecurity personnel who have several years of relevant work experience. Similarly, teamwork, interpersonal skills, and adaptability/flexibility are regarded as quite important in the workplace.

While the survey multiple choice option of "creativity" had a slightly lower ranking, interviewee and job posting results shed some light on the semantic differences that may be causing this: rather than "creativity," cybersecurity employers may look for critical thinking, analysis, problem-solving, and strategic thinking. Similarly, while a strong EQ (emotional quotient, i.e. "empathy") was not a favourite survey response, employers volunteered priorities around emotional intelligence and situational awareness, and the lower rank of leadership is belied by the importance of mentorship, good teamwork, business competencies, prior experience, and the cumulative sum of many of these human skills that together create a good leader.

In addition to human skills, **Figure 16** lists the technical cybersecurity skills that were mentioned in each of these data sources. Skills are grouped and ordered again by survey respondents' importance rankings. Two professionals with technical cybersecurity expertise were asked to independently code and group the skillsets in these categories, and their analyses were combined (though were largely in agreement) for the purposes of the visualization below. While this chart maintains a high degree of granularity, several takeaways are clear. In particular, several skillsets are reinforced across the board and useful in a number of applications, including Communications and Network Security; Security Engineering; Network Architecture, Security, Tools, & Protocols; and Protection Concepts, among many others. The two coders noted that, due to the combination of many data sources (i.e., multiple job postings and multiple interviewees), there was significant overlap between many of the skills listed below. Figure 16 retains the original wording from these sources wherever possible, however, to showcase the actual requests of employers.

A Human and transferrable skills

	Skills ranked in order of importance from ICTC's New Brunswick Employer Survey[37]	Skills directly mentioned in interviews or specific to qualifications mentioned in interviews	Skills scraped from job postings in New Brunswick (aggregated when similar)
1	Responsibility/Professionalism	• Self-motivated • Strong work ethic • Familiarity with enterprise-level systems • Passion/interest in cybersecurity • Professional curiosity	• Independence • Enterprise environment experience • Project management
	Teamwork	• Collaboration & interpersonal skills	• Interpersonal skills • Mentorship, training & capacity-building for colleagues
	Communication	• Presentation skills • Communication skills (written & verbal)	• Written and verbal communication
2	Flexibility	• Adaptability	• Time management, flexibility
	Creativity	• Critical thinking skills	• Problem-solving, analysis, strategic thinking • Human behaviour analytics
3	Courtesy/Empathy	• Emotional Intelligence (Empathy) • Customer service skills	• Emotional intelligence • Situational awareness
	Leadership	• Leadership skills • Volunteer/Internship experience	• Client and customer service • Leadership, managerial, supervisory skills

[37]Respondents were asked: "When hiring cybersecurity personnel in New Brunswick, which of the following [A: human or B: technical] skillsets are most important?" The ranked groupings are based on respondent ratings from most to least important, with skills that have very similar ratings clustered. These survey questions had 40 complete individual responses.

B Cybersecurity-specific Technical Skills

Skills ranked in order of importance from ICTC's New Brunswick Employer Survey

Group one
(highest-ranked in survey)

- (A) Network Security
- (B) Knowledge of Cloud Computing Security

Group two:
(second-highest)

- (C) Systems and Network Engineering
- (D) Integrating Technologies, Systems, and Services
- (E) Information Security & Knowledge of Best Practices for Systems Architecture
- (F) Governance and Compliance
- (G) Penetration and Vulnerability Testing
- (H) Incident Investigation and Response

Group three:

- (I) Risk Assessment and Management
- (J) Knowledge of IoT Security
- (K) Encryption and Cryptography, Quantum-safe Cryptography

Skills directly mentioned in interviews or specific to qualifications mentioned in interviews

- (A)(B)(C)(D)(E)(G)(H)(J)(K) Communications and Network Security
- (C)(D)(E)(G)(H)(J) Identity and Access Management
- (A)(C)(D)(E)(K) Security Engineering
- (F)(G)(H)(I)(J) Security Analysis
- (F)(G)(H)(I) Auditing Information Systems
- (F)(H)(I)(J) Risk Management
- (B)(H)(J) Cloud Security
- (C)(H) Information Systems Operations
- (D)(G) Software development security
- (F)(H) Security Operations
- (G)(I) Security Assessment and Testing
- (F) Asset Security
- (F) Information Systems Acquisitions
- (F) Management Responsibility
- (F) Information Security Governance
- (H) Incident Management
- (H) Threat Hunting

Skills scraped from job postings in New Brunswick
(aggregated when similar)

- (A)(B)(C)(E)(F)(G)(H)(I)(J) Protection Concepts
- (A)(C)(D)(E)(G)(H)(J) Network Architecture, Security, Tools, & Protocols
- (D)(E)(H)(K) Data Protection and Encryption
- (G)(H)(I)(J) Vulnerability Evaluation & Management
- (G)(H)(I)(J) Threat Evaluation Analysis
- (F)(H)(I) Risk Mitigation and Management
- (A)(H) Firewall Management
- (E)(H) Automation (Configuration, Management, Security Systems)
- (E)(H) SOC Processes and Concepts
- (E)(H) Managing Enterprise-Level Security Systems
- (F)(I) Security Metrics and Reporting
- (G)(K) Knowledge of Attack Methods
- (F) Governance and Compliance
- (G) Penetration Testing
- (H) Event Monitoring
- (H) Digital Forensics
- (H) Incident Response
- (H) Handling Compromised Systems
- (H) Detecting Complex and Advanced Breaches
- (H) Developing Hunting and Detection Routines
- (H) Running SIEM & Data Loss Prevention (DLP) Systems

C Other Technical Skills

Skills ranked in order of importance from ICTC's New Brunswick Employer Survey	Skills directly mentioned in interviews or specific to qualifications mentioned in interviews	Skills scraped from job postings in New Brunswick (aggregated when similar)
Understanding of Network Communications and Protocols		• Server Administration & Infrastructure • Knowledge of Mobile Tech & Radio Telephony
Foundational Software Development	• Foundational Programming • AI/ML experience	• Agile Methodologies • Foundational & Advanced Programming • Knowledge of Memory & Data Structures
Outliers (uncategorized by coders)	• IT management • Documentation • Auditing, continual improvement • Familiarity with enterprise systems (ERPs)	• Database administration • Records, document management • Data integration & warehousing

Responses given to open-ended alternative, "another important skillset (please specify)"

Employer Perspectives on Training & Education in Cybersecurity

Cybersecurity employers in New Brunswick voice an avid preference for personnel with significant work experience, but that experience is created on a foundation of training: formal, informal, certification-based, and post-secondary. Respondents highlighted that while academic qualifications are problematic when used exclusively, they can act as proxies for streamlining qualified candidates. The degree to which employers value different types of training and experience is roughly shown by the survey findings exemplified in Figure 17.

Which of the Following Credentials is Most Important?

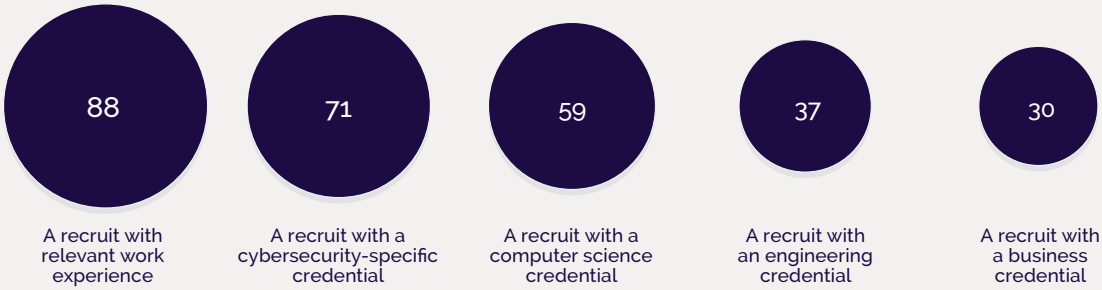


Figure 17: Credentials ranked by importance in the ICTC New Brunswick Cybersecurity Employer Survey. Employers were asked, "Please rate the following options in terms of importance. When hiring cybersecurity personnel, do you have a preference for..." (scores assigned by weighted ranking).

Figure 17 makes it clear that employers value tangible cybersecurity-specific training (either through former work experience in cybersecurity, or through a cybersecurity-specific credential such as a professional certificate) more highly than foundational degree programs. Employers were able to shed some light on this in interviews, noting a trend in the cybersecurity education landscape that moves away from valuing traditional degrees to valuing professional certifications. The desire for candidates who possess professional certifications was a consistent theme amongst respondents, with several commenting that industry recognized certifications (CMPA, CISSP, SANS certifications, etc.)[38] were strongly encouraged for prospective talent, both regionally and abroad. Organizations weighed certifications as strongly as formal academic training and, in some cases, preferred the prior.

> *60% of the people in our company are computer scientists, while 40% are a patchwork of credentials or have a master's in something unrelated. That something different is usually biology or chemistry. Out of the people with a patchwork of credentials, some come from other university programs, while about a third have various certifications and a strong work history.*
>
> - Andrew Jefferies, previously Bulletproof, now Deloitte

[38] Certifications found in New Brunswick job postings analysis include (no particular order) TOGAF, SABSA, ITIL, ISSAP, ISEP, CISA, CISSP, GCFA CEH, ISACA Cybersecurity Fundamentals Certification, ISA, NIST, CISM, CGEIT, CRISC, CBCP, PCIP, ISO27001, CCNA, MCSE, Security+, C|CISO, GIAC, CBCP, CIPP/C, SANS, COBIT, Agile, FIPS, and STIG.

Despite this insight, cybersecurity job postings continue to request that applicants have either undergraduate or graduate degrees in traditional cybersecurity-related fields: Computer Science, Engineering (typically electrical or software), IT, Information Systems, Networking, Automation, Computer Science, IT, Information Systems, Networking, or Related Fields. Some roles that were either higher-level/managerial or related to client interactions also requested an MBA.

Interviewees also noted that the province's network of colleges, with their speed and agility to remain receptive to industry feedback, were viewed very positively. The ability to ensure that content remained relevant and that training with innovative products was kept modern was appealing. Industry representatives strongly encouraged the province to continue streamlining and innovating cybersecurity programs due to the dynamic yet fluid nature of the industry.

Several New Brunswick cybersecurity employers regularly hire interns or co-op students who are still in school or who have just graduated. Candidates with strong extra-curricular backgrounds are given preference for this type of role: volunteer experiences and involvement in community-based activities[39] were viewed as networking and skill-building initiatives.

Mysterious Recruitment: The Hidden Job Market and Acquiring Talent

In a field where finding skilled talent is naturally difficult, the ability to find candidates who possess specific, niche or specialized training becomes even more challenging. Without a strong influx of seasoned professionals, the ability to scale a business in a high-demand sector presents challenges that impact growth and economic potential. These challenges often translate into the recruitment of skilled talent, not from the available talent pool but those employed elsewhere. Accordingly, New Brunswick industry consultants noted that job postings might represent trends in hiring but were almost undoubtedly not accurate reflections of the absolute number of jobs that were actually available. Many jobs may not be posted, with several respondents admitting that they might post a job as a last resort:

> *I'll reach out to industry partners and say, "Do you have anybody looking for work because we're looking to hire a certain position." I'll usually wait for one to two weeks to see if I get any tips back from that. If not, then we'll do the more traditional route. We'll go to the universities and say, "Do you have anybody coming out of the program looking for work?" We'll even go to the bigger software companies to ask if there is anybody that they know who might be looking to leave their organization. Generally... that's a pretty good conversation to have. Then finally, if either of those methods are unsuccessful, then we'll do that Indeed or Career Beacon approach.*
>
> – Adam Mosher, Global Intelligence Inc.

[39] *Such as the aforementioned program CyberTitan.*

The hidden job market is a symptom of a well-networked ecosystem with numerous personal connections, and it also carries additional benefits that range from keeping organizational secrets confidential (i.e., new research and development areas, business services, etc.) to identifying higher-caliber talent that is fully employed elsewhere.

Reasons for Cybersecurity Demand in Canada and New Brunswick

> *We have absolutely have to be competitive against huge organizations like IBM and Microsoft that are able to pay really good salaries. We can't leverage those types of dollars so what we do, for example, for the young men and women coming out of university who are on average 23 and 24 years old, is we're paying them generally between $85,000 and $95,000 per year. At that point, we're providing them with anywhere between four to five weeks of vacation with full medical, dental paid, and some other perks on top of that. So that's how we offset not being able to pay them in the $125,000 to $140,000 range, which the larger companies can offer.*
>
> – Adam Mosher, Global Intelligence Inc.

Workforce gaps are often caused by a complex combination of variables. In the existing research on the demand for cybersecurity professionals, employers identified a wide range of reasons for the difficulties they were facing in hiring, including skill gaps, retention, unclear career paths, salary expectations, and diversity as key challenges. As a part of ICTC's employer survey, respondents were asked which challenges they had faced. Interestingly, while the top challenge appears to be finding skilled personnel (experienced by nearly a third of employers), only 11% of respondents thought that this problem might be due to a dearth of cybersecurity candidates in the province overall, implying that the New Brunswick cybersecurity labour gap is specific to highly skilled positions. Furthermore, high salaries and a lack of a clear career path for recent graduates are also key issues, experienced by approximately one-fifth (22% and 17%, respectively) of employers.

Which of the following cybersecurity hiring challenges have you experienced in NB?

% of employers who have experienced challenge

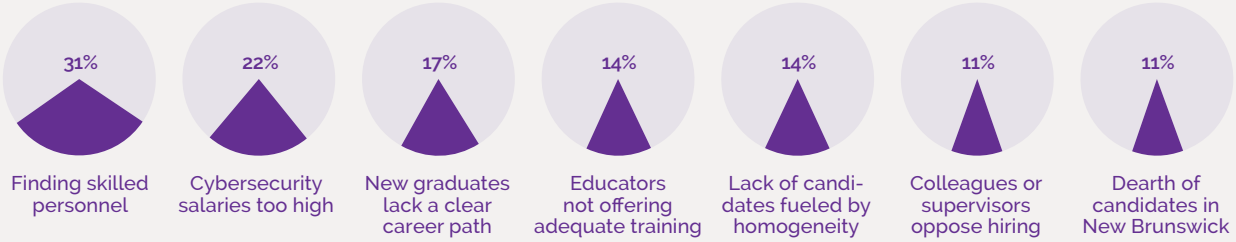


Figure 18: Employers' perspectives on challenges to hiring in New Brunswick. Note: The survey responses are here condensed for readability

New Brunswick employers' experiences are reinforced by national and international literature. Across the board, qualified and experienced personnel are difficult to find. In a 2018 Canadian study by Deloitte, the vast majority of Chief Information Security Officers (CISOs) noted that "finding the right mix of technical, analytical, and soft skills" (76%) was a significant challenge to recruiting cybersecurity staff.[40] ISACA, an international cybersecurity organization, also polled organizational respondents on this issue, and most employers felt that the majority of cybersecurity applicants were not well qualified for the positions to which they were applying.[41] High cybersecurity salaries are also a nearly universal challenge for businesses. A third of Canadian CISOs felt that cybersecurity compensation packages have been inflated by demand,[42] and when extended to North America, this impression is held by 41% of respondents.[43] In Canada, 27% of companies polled by the CIRA reported that they lacked the resources to employ a cybersecurity professional, and businesses who were hiring external cybersecurity consultants were devoting 19% of their total IT budgets on average.[44]

Finally, as will be explored in the subsequent section on supply, the cybersecurity sector lacks diversity. While few (15%) surveyed employers in New Brunswick identified ethnic and gender homogeneity as a "challenge," it is possible that there exists an untapped supply of workforce entrants. ISACA found that when asked about gender disparity in opportunity, only 41% of female cybersecurity employees felt that women were offered the same options for career advancement as men (vs. 79% of male respondents).[45] Globally, in 2016, women in cybersecurity earned less than men at every level of employment,[46] even though women typically enter cybersecurity with higher levels of education than men.[47] Canadian CISOs noted the underrepresentation of women as a factor contributing to the low number of experienced cybersecurity professionals.[48]

[40]Deloitte and the Toronto Financial Services Alliance, The changing faces of cybersecurity: Closing the cyber risk gap, 2018, pp. 12-14.
[41]ISACA, State of cybersecurity 2019: Current trends in workforce development, 2019, p. 8.
[42]Deloitte and the Toronto Financial Services Alliance, The changing faces of cybersecurity: Closing the cyber risk gap, 2018, pp. 12-14
[43]Center for Cyber Safety and Education, 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Frost & Sullivan, 2017, p. 4.
[44]CIRA, Fall 2018 Cybersecurity Survey Report, 2018, p. 10.
[45]ISACA, State of cybersecurity 2019: Current trends in workforce development, 2019, p. 14.
[46]Center for Cyber Safety and Education, 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Frost & Sullivan, 2017, p. 5.
[47]Idem, p. 10.
[48]Deloitte and the Toronto Financial Services Alliance, The changing faces of cybersecurity: Closing the cyber risk gap, 2018, pp. 12-14

UNDERSTANDING CYBERSECURITY LABOUR SUPPLY

in Canada and New Brunswick

> *We want to build the community here [in New Brunswick] because we're part of [it], and that's important. We need to match our recruitment to our growth and it is difficult to find, attract, and keep skilled talent in this sector. So, it makes sense to bring as many channels as we can into that equation.... We look to K to 12, University Co-ops, and we hire a lot of new immigrants.*
>
> - Andrew Jefferies, previously Bulletproof, now Deloitte

Demographics of the Cybersecurity Sector

Both in New Brunswick and around the world, the cybersecurity sector lacks diversity, with severe implications for the available supply of skilled personnel. This trend is brought home in New Brunswick through surveyed employers' estimates of the number of women, first generation Canadians, Indigenous peoples, visible minorities, and persons with disabilities in their cybersecurity workforces, as illustrated by Figure 19. For example, over half (52%) of New Brunswick's surveyed employers report no women in their cybersecurity workforce, while a third (34%) are entirely white-identifying.

Diversity of Cybersecurity Personnel in Cybersecurity Respondents' Workplaces

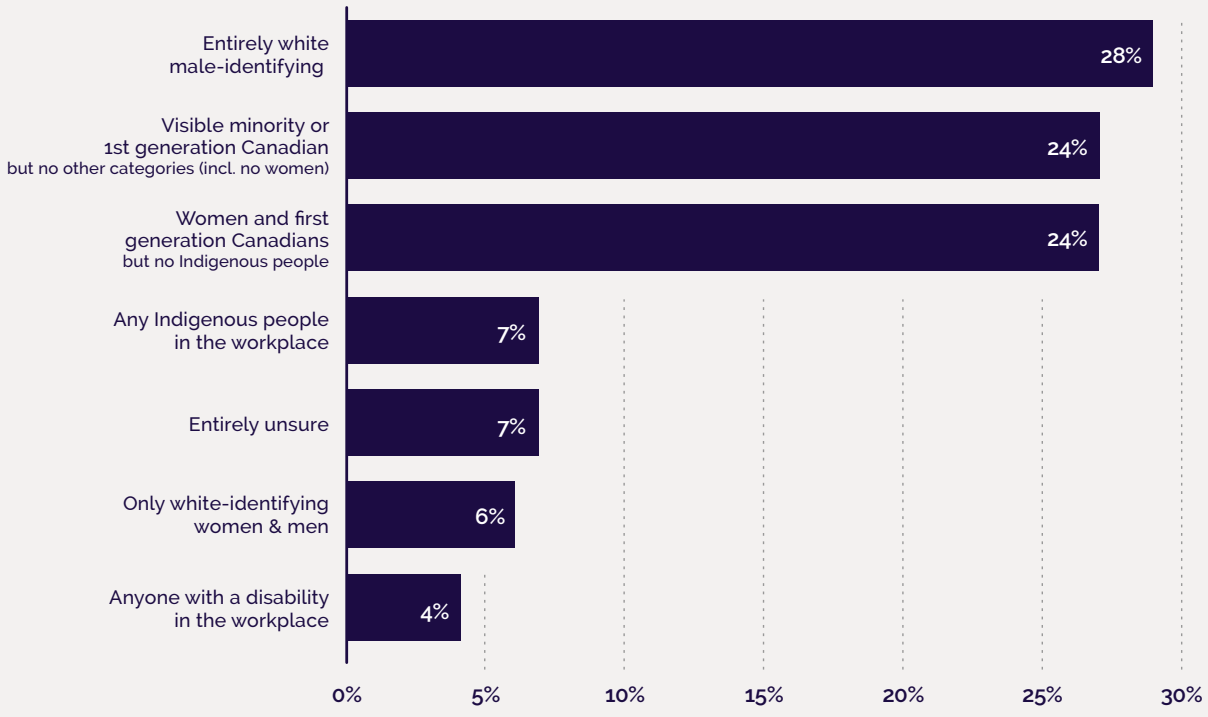


Figure 19: The makeup of cybersecurity workforces in New Brunswick, ICTC New Brunswick Cybersecurity Employer Survey.

The section that follows examines general and provincial demographic trends, specific to cybersecurity personnel.

Gender

Internationally, approximately 11% of the cybersecurity workforce is made up of women.[49] While in North America this figure becomes 14%, the highest regional concentration worldwide, women remain significantly underrepresented in cybersecurity.[50] Furthermore, men are four times more likely to hold C-suite and executive positions, and nine times more likely to hold management positions, than women in North America.[51] An American study found that while ethnic minorities were proportionally well-represented in the cybersecurity sector, they were also less likely to hold senior positions, and women of colour in particular were underpaid by an average of nearly $10K in comparison with white male colleagues of the same status.[52]

Provincially, it can be seen in Figure 20 that women make up a disproportionately small number of New Brunswick's cybersecurity-related personnel, and there tend to be fewer women in managerial roles with higher median salaries, with only 22.5% of computer and information systems managers identifying as women in 2015.

Sex and Median Salary in New Brunswick Cybersecurity

2015, CAD

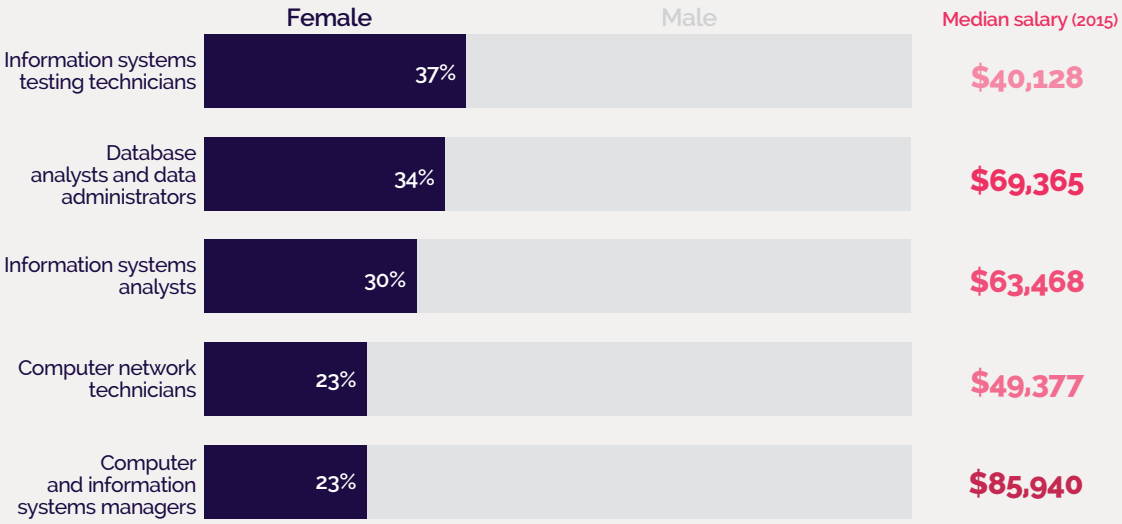


Figure 20: Sex and Median Salary in New Brunswick's cybersecurity-related NOCs, 2015 Source: Government of New Brunswick, www.nbjobs.ca

[49] *Center for Cyber Safety and Education, The 2017 Global Information Security Workforce Study: Women in Cybersecurity, Frost & Sullivan. 2017. https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf, p. 6.*
[50] *Ibid.*
[51] *Idem, p. 5.*
[52] *Ibid.*

Age and Salary

Similarly, as is evident in Figure 21, cybersecurity salaries tend to rise for roles with proportionally older groups of employees. The role with the greatest number of young participants, Information systems testing technicians, had the lowest median salary at $40,128 in 2015. This trend may be related to education, as the roles with the two lowest salaries are also the least likely to require a University degree of the five roles listed in the figure. In addition, New Brunswick has a slightly higher median age than Canada (43.6 as compared with 41.0 in Canada in 2016).[53] While Canada is experiencing an increase in average age as healthcare prolongs lives and fertility rates drop, New Brunswick is experiencing that transition even faster; the average age in Canada increased by 0.9 years during the 2011-2016 period, and New Brunswick's increase was 1.5.[54] In addition, the tech sector in New Brunswick skews younger: for example, as of December 2019, 43% of New Brunswick's total workforce was between the ages of 45 and 64, compared with only 35% of the tech sector labour force.[55] As such, the province's unique demographics imply the need for clear career paths for younger workers to begin to fill higher-skilled, higher-salary roles and measures to retain young people in the province.

Age and Median Salary in New Brunswick Cybersecurity Employment

2015, CAD

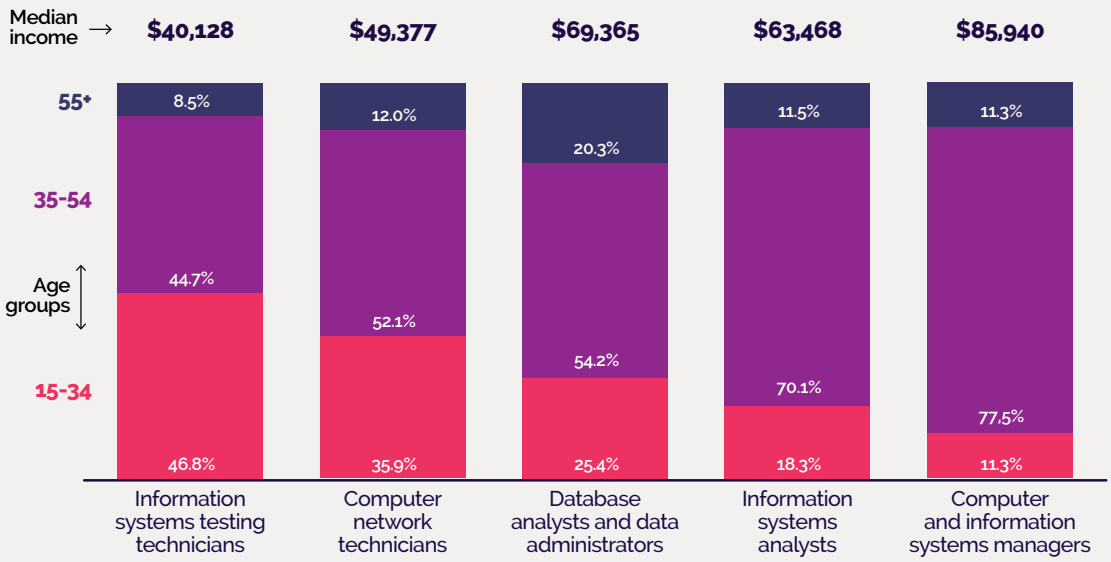


Figure 21: Age and Median Salary in New Brunswick Cybersecurity Employment (2015, CAD). Source: Government of New Brunswick, NB Jobs.

[53] *Statistics Canada, 2016*
[54] *Government of New Brunswick, 2016*
[55] *Statistics Canada, 2019*

Indigenous People

Interviewees noted that New Brunswick's Indigenous labour force has experienced noticeable growth from changes related to self-identification (a positive culture shift), natural population growth, and migration. However, gaps still remain in education, where Indigenous people remain less likely to hold postsecondary qualification, compensation, and other important social indicators. Based on the small size of the cybersecurity industry, the relatively low percentage of New Brunswickers who self-identify as Indigenous (4% in 2016),[56] and formidable barriers to entry such as location and access to urban centers, there are likely few Indigenous people employed in cybersecurity across New Brunswick. Approximately 90% of surveyed employers confirmed that their industry did not employ any self-identified Indigenous people, as portrayed in Figure 19. Workforce development organizations, discussed in a subsequent section, are seeking to remedy this gap and make the cybersecurity industry, with its high-paying and in-demand jobs, more accessible for Indigenous peoples in the province.

Newcomers/Immigration

Newcomers to Canada comprise a significant proportion of the country's tech labour force. While little data on the national composition of the cybersecurity workforce in New Brunswick is available, questions related to newcomers and immigrants into New Brunswick were met with mixed reviews by interviewees. Some respondents cited challenges related to security clearances outside of the Five Eyes for highly qualified experts. One interviewee highlighted additional security clearance hurdles as they related to visas for staff assigned to US-client projects. Another industry leader commented that due to security concerns, any international talent (outside of the Five Eyes) assigned to work with American companies would encounter barriers to securing temporary travel visas. Other respondents noted the province's historical lack of ethnic diversity as an ongoing barrier to new entrants, challenges related to remote contact and communication, and immigration processes resulting in a long recruitment process:

> *The hiring process takes way longer in New Brunswick [for international candidates]. Instead of taking two weeks, it takes two months, four months, or more.*
>
> – Anonymous

[56] *Statistics Canada, 2019.*

Interviewees did, however, highlight a growing shift in industry culture. The shortage of domestic skilled talent required hiring managers to look abroad for high-quality solutions. Some organizations also said that their successful international hiring practices were a credit to their current workforce. Respondents emphasized the value of culturally diverse workspaces in the cybersecurity field, as they correspond to a better understandings of unique security-related challenges. International perspectives, they added, could provide better clarity on the motivations and methodologies of various threat actors.

Interviewed organizations were given the opportunity to highlight place of origin for their international talent. Beyond the US and EU, interviewees identified several countries, including Nigeria, the Philippines, India, the United Arab Emirates, Mexico, Venezuela, South Korea, and Egypt. Between 2011 and 2016 the population of New Brunswick dropped by 0.5%, while Canada as a whole grew by 5%. This disparity signals a need to diversity the province's population supply. Immigration programming may be one way to streamline international talent that can support industry growth.

Educational Programs for Cybersecurity in New Brunswick

Globally, most cybersecurity workers begin with a computer science or engineering degree, and many also transition into their field from a previous career in IT, finance, defence, marketing, business, accounting, or other industries.55 The province of New Brunswick has a variety of academic programs intended to supply cybersecurity-trained graduates, and this work begins at the elementary school level. The list below provides a survey-level list of cybersecurity programs and workforce development efforts in New Brunswick from grade school to post-secondary programs but is intended to be illustrative rather than exhaustive:

Elementary to Secondary School: Interviewees noted that a wide range of cybersecurity-related material is included in New Brunswick K-12 curricula, due in part to a partnership between CyberNB and the Department of Education and Early Childhood Development. Respondents noted that several countries leading the cybersecurity sector, such as Israel, viewed New Brunswick's academic integration with cybersecurity favourably and regarded it as an international example.

Post-Secondary Short-Term and Certificate Programs in Cybersecurity:

The Collège Communautaire du Nouveau-Brunswick offers an 80-week Cybersecurity program, including an internship that addresses cryptology, risk management, ethical hacking, Java and Python programming and security for applications, databases, networks, and systems. The program specifically seeks to produce workers in the Information Systems Analysts and Consultants role (NOC 2171).[59]

The Francophone Université de Moncton offers an 8-course (24 credit) certificate in Business Information Security, around half of which is centred on cybersecurity-related topics.[60]

New Brunswick Community College offers a one-year diploma of advanced studies in cybersecurity. The program includes 14 cybersecurity-related courses spanning risk management, endpoint security, ethical hacking, incident response and forensics, human and software security, and enterprise security products. It is specifically geared towards making Information Systems Analysts and Consultants (NOC 2171) and Computer Network Technicians (NOC 2281).[61]

Private institution Oulton College offers a Systems Management and Cybersecurity Program, a 10-month program concluding with a four-week practicum. The program is geared toward systems management rather than cybersecurity and includes no training in Java or Python.[62]

Private institution Eastern College offers an 81-week program in Advanced Systems Management and Cybersecurity, which is aimed at employment for Computer Network Technicians (NOC 2281) and User Support Technicians (NOC 2282). The program concludes with a 16-week field placement.[63]

Bachelor's Level Cybersecurity-specific Options: The University of New Brunswick offers an option to specialize in cybersecurity as part of the Bachelor of Computer Science program.[64] The cybersecurity specialization is 12 credits in length and includes a class in Software Security, Digital Forensics, and a 6-credit Capstone Project including a thesis.[65] Students can also participate in a co-op. In addition, several post-secondary institutions in the province, such as Mount Allison, offer individual classes in cybersecurity-related skills like cryptography as coursework options for computer science, mathematics, or engineering students.

[59]CCNB, "Cybersecurity," Our Programs, https://ccnb.ca/programme-detudes/nos-programmes.aspx?SectorId=9417243f-3b20-42ed-91de-82bb-281c8134&ObjectType=1&Id=b3ae566b-d545-4212-a8da-b386d7184913
[60]UMoncton, "Bachelor in Information Management," https://www.umoncton.ca/umcs-bgi/node/55
[61]NBCC, "Information Technology: Cybersecurity," https://nbcc.ca/programs-courses/program-details?baseCurriculumId=dd3a4616-5e03-4a27-b585-d074efdd4178
[62]Oulton College, "Systems Management and Cybersecurity," https://oultoncollege.com/systems-management-and-cybersecurity/
[63]Eastern College, "Advanced Systems Management and Cybersecurity," https://www.easterncollege.ca/programs-courses/technology/advanced-systems-management-and-cybersecurity/
[64]University of New Brunswick, "Areas of Specialization," https://www.unb.ca/fredericton/cs/undergrad/bcs/specialization.html
[65]Ibid.

Graduate Level: The University of New Brunswick (UNB) offers a Master's Degree in Applied Cybersecurity. The one-year program includes nine courses (including computer labs) and an R&D Capstone project with an industry partner. Graduates of the program can acquire additional experience through Research Intensive Cyber Knowledge Studies, an addendum that lasts four months and begins immediately after graduation. The additional four months also includes models in Cybersecurity Project Management and Product Development and additional work experience with an industry partner.[66]

Auxiliary Programs:

The Joint Economic Development Initiative (JEDI)'s Cybersecurity Training program is a training-to-employment initiative for Indigenous peoples within New Brunswick. On July 19th, 2019, six learners supported through the program graduated with a Cybersecurity certification from the Community College of New Brunswick.[67]

The Canadian Institute of Cybersecurity at the University of New Brunswick offers Cybersecurity 101, an intensive, 4-day training on cybersecurity for IT Professionals from outside the field. The course includes lectures, labs, activities, and demonstrations. It provides an overview of cybersecurity risks, risk management practices, intrusion prevention and detection, and incident response.[68]

As illustrated by this extensive list of programs, New Brunswick is a clear centre for cybersecurity education in Atlantic Canada. On a national level, the province punches above its demographic weight in terms of its educational offerings, with four public post-secondary institutions offering programs specific to cybersecurity. In this regard, it ranks fourth in Canada to Ontario, Quebec, and Alberta. New Brunswick is also one of only three provinces to offer a Master's degree in Cybersecurity (the other two being Ontario and Quebec). New Brunswick's educational offerings in Cybersecurity are particularly impressive when considering the Central and Western provinces. New Brunswick offers around half as many university-level programs in cybersecurity as Quebec does, and around a quarter of what Ontario does, but both these provinces have populations over 10 times that of New Brunswick. New Brunswick's offerings of college and university programs are comparable to the more populous Western provinces.

New Brunswick benefits from recognition as a cybersecurity hub even by major international firms. The University of New Brunswick, host of the Canadian Institute for Cybersecurity, is one of only eight Universities in North American (including three in Canada) selected by IBM to work on Watson, a cognitive cybersecurity technology.[69]

[66] *University of New Brunswick, "Experiential Addendum: Research Intensive Cyber Knowledge Studies (RICS)," https://www.unb.ca/fredericton/cs/grad/masters/macsec/rics.html*

[67] *Bulletproof, "The Joint Economic Development Initiative Announces the Graduation of the Inaugural Cohort of Indigenous Cybersecurity Professionals," https://www.bulletproofsi.com/blog/the-joint-economic-development-initiative-announces-the-graduation-of-the-inaugural-cohort-of-indigenous-cybersecurity-professionals/*

[68] *University of New Brunswick, "Cybersecurity 101," https://www.unb.ca/cic/cybersecurity-101.html*

[69] *University of New Brunswick, "UNB is Canada's cybersecurity research hub," https://www.unb.ca/cic/about/hub.html*

New Brunswick's Cybersecurity Workforce Development Efforts: Beyond Formal Academic Training

Workforce Development: External to Businesses

The development of a strong and sustainable workforce relies on the collective effort of education, government and private industry. Over 70% of interview respondents explicitly mentioned the successful workforce development efforts of CyberNB, the province's non-profit industry association. Specifically, 40% of these respondents highlighted CyberNB's commitment to the Grade 6-12 educational program CyberTitan. CyberTitan, an Information and Communications Technology Council initiative, is a comprehensive online educational competition designed to prepare students with highly sought-after cybersecurity skills desired by industry recruiters.[70] Additionally, two respondents mentioned JEDI (Joint Economic Development Initiative), a cybersecurity training program designed to promote New Brunswick's Indigenous peoples, fill labour shortage issues and use an integrated-learning approach to build inclusive talent-supply pipelines.

One of the largest benefactors of K-12 and post-secondary cybersecurity investment is private industry. The vast majority (about 80%) of interviewees from the private sector claimed to be engaged in educational programming, whether through industry awareness projects, training, program advisory committees at the college level or mentorship programs. More than half of these respondents mentioned that they personally volunteered, outside of work arrangements, to assist workforce development projects. These events include educator and student awareness programs (e.g., class talks, seminars, extra curricular activities), one-to-one mentorship, industry networking events, girls-focused STEM projects, student and industry conferences, and projects designed for underrepresented groups.

Internally Provided Training or Professional Development

As the need for specialized skillsets continues to increase in a widening cybersecurity profession, an organization's staff must remain equally dynamic. Staff who were once fully trained as a vulnerability analyst might now have to consult with their department as a security systems architect, requiring additional skills they may not have originally possessed. Accordingly, many organizations may opt to train their staff in new disciplines rather than test New Brunswick's talent pool.

[70] *For more information, visit https://www.cybertitan.ca/*

One industry respondent explained that their organization's increasing need for specialized skillsets made the hiring process too challenging. Their organization opted to design specialized internal training programs for staff at various levels of complexity and difficulty. In all, about half of interviewees confirmed that they invested in training and professional development as a means of retaining skilled talent.

Other interesting feedback derived from industry leaders regarding training and professional development include the following:

- University and college graduates are often provided with work integrated learning (WIL) opportunities if they're lacking specific credentials/expertise.[71]
- Organizations encourage internal mentorship programs to allow new staff to learn from seasoned industry experts.
- It is important to provide specialized legal, policy, and strategy training to help staff better understand federal and international regulations and governance.
- Incentivizing education with financial subsidies for training certifications and vendor training (SANS certifications, CISSP costs and ethical hacking certifications) has shown promise.

[71] *Such as https://www.wil-ait.digital/en/*

Opportunities:

BRIDGING THE CYBERSECURITY LABOUR GAP

New Brunswick's cybersecurity supply pipeline is robust, including work placements in several college and university programs, as well as various upskilling opportunities for trained IT professionals interested in transferring into a cybersecurity specialization. Despite these opportunities, there is only limited evidence that this has positively influenced the labour market over the last four years. As illustrated in Figure 1, the province's employment in Cybersecurity-related NOCs is lower now than it was five years ago. Indeed, a variety of other data sources that explore cybersecurity-related roles more deeply all show a tendency towards a greater demand for skilled talent, that is, demand for jobs that require years of experience. Furthermore, employers have continually reinforced the need for hires with preexisting industry experience (both through the ICTC employer survey and during interviews). Accordingly, it is clear that demand is high but not across the board—it varies by role, and new graduates may not be able to immediately complete programs and fill employers' needs. In addition, some workforce development efforts may inadvertently be designed to bolster a supply of entry-level candidates to low-growth areas.

Industry respondents suggested the narrative of a talent pipeline out of step with industry needs, noting that despite receiving a healthy volume of applicants, few had reliable field experience, such as co-ops or work-integrated learning opportunities. Among all interviewees, finding applicants with specific skills was deemed the greatest challenge as the field increasingly becomes more diverse with various roles and subfields, making it increasingly difficult for generalist, entry-level programs to provide students with a satisfactory degree of industry exposure.

Accordingly, what opportunities exist to create highly skilled cybersecurity talent in New Brunswick?

A variety of recommendations emerged from interviews and secondary data.

Improve professional development and cybersecurity training for existing professionals.
The majority of international employers (57%) have indicated that they are increasing staff training as a way to improve their cybersecurity record.[72] In addition, New Brunswick's cybersecurity workforce development efforts appear to be more geared towards entry-level training than upskilling current workers who may need additional experience or skills to compete for senior-level positions.

Identify mid-career professionals with relevant training and transferable skills.
As one example relevant to New Brunswick, Veterans Affairs Canada (VAC) estimates that more than 30,000 skilled individuals reside in New Brunswick, 25,000 of which are likely to be well within working age.[73] Their experience working collaboratively, under strict deadlines and immense pressure fits within the scope of cybersecurity industry needs regarding skilled labour. In the US, tech companies have begun establishing direct hiring pipelines from the military into skilled roles, realizing that the volume of new graduates doesn't equate with the rising need for quality applicants.[74]

[72] *ISACA, State of cybersecurity 2019: Current trends in workforce development, 2019, p. 12.*
[73] *veterans.gc.ca/eng/about-vac/news-media/facts-figures/1-0*
[74] *https://www.itprotoday.com/strategy/it-reaps-benefits-military-veteran-hiring-programs*

Legitimize and formalize well-defined cybersecurity career paths that new graduates can use to build necessary skills and experience, understand opportunities for advancement, and plan for their careers. Rather than searching for cybersecurity professionals well versed in everything, identifying compartmentalized skillsets and clear career paths will improve training and clarify key skillsets required by recruits today.[75] Importantly, in New Brunswick this may include increasing the number and duration of co-op or work-integrated learning opportunities available. This measure is particularly important given the province's aging workforce.

Address the underrepresentation and uneven advancement opportunities of cybersecurity personnel who identify as women and minorities.[76] The issue of female underrepresentation has been difficult to shake throughout the history of the cybersecurity industry, and in North America the number of organizational diversity programs (most frequently gender-oriented) may be declining year by year, trending downward alongside employees' perceptions of their effectiveness.[77] However, the increase in the number of young women with ICT degrees may lay the groundwork for employers to actively recruit more female cybersecurity staff, pay them equitably, and provide them with the same opportunities for promotion as their male peers.[78] As discussed earlier, better diversity and equal opportunity in the cybersecurity sector would increase the pool of potential hires.

Conduct further inquiry into clear pathways for international hires. As discussed in the section discussing newcomers and immigration, several interviewed employers voiced difficulties and lengthy wait times in immigration processes because of security clearance needs and dealings with international partners such as the United States. Further inquiry is merited into what can be done to improve the experience of newcomers, the advocacy efforts of provincial associations, and the challenges cybersecurity employers face during the recruitment process. It is possible that key policy changes in this area could drastically improve the pool of readily skilled, mid-career talent.

Improve the loyalty of young workers, who are most likely to leave their jobs and express dissatisfaction with existing roles,[79] by offering workplace training, role diversity, organizational payment for certification, and support for remote/flexible working.[80] While retaining young workers is a common challenge in New Brunswick, the creation of better career pathways and prospects will support this key demographic to stay in their province of origin, while attracting new entrants.

Use new technologies to create augmented security that reduces risk.[81] Overall, 18% of ISACA survey organizations indicated that they were beginning to rely more heavily on artificial intelligence to reduce their organization's cybersecurity gap.[82] This theme was echoed by interviewees and is a key supplement to workforce development efforts, though not the primary purpose of this study.

[75] *Deloitte and the Toronto Financial Services Alliance, The changing faces of cybersecurity: Closing the cyber risk gap, 2018.*
[76] *Center for Cyber Safety and Education, 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Frost & Sullivan, 2017, p. 6.*
[77] *ISACA, State of cybersecurity 2019: Current trends in workforce development, 2019, p. 16.*
[78] *Center for Cyber Safety and Education, The 2017 Global Information Security Workforce Study: Women in Cybersecurity, Frost & Sullivan. 2017.*
[79] *Center for Cyber Safety and Education, 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Frost & Sullivan, 2017, p. 6.*
[80] *Center for Cyber Safety and Education & (ISC)2, "Meet the Millennials," Frost & Sullivan, 2017, https://iamcybersafe.org/research_millennials/*
[81] *Deloitte and the Toronto Financial Services Alliance, The changing faces of cybersecurity: Closing the cyber risk gap, 2018, p. 6*
[82] *ISACA, State of cybersecurity 2019: Current trends in workforce development, 2019, p. 12.*

Conclusion

In the rapidly changing field of cybersecurity, the province of New Brunswick provides a unique perspective as a small, well-networked ecosystem with dedicated organizations playing a hands-on role in workforce development. The province is equipped with relative advantages, such as public sector investment, large industry players, and a high quality of life, and disadvantages, such remoteness and high unemployment. Overall, however, it has punched above its weight in important metrics such as the jobs-to-population ratio, workforce development, and training institutions. New Brunswick's in-demand roles include many highly skilled positions that are typically filled by an experienced but aging workforce, and all evidence suggests that these highly skilled, senior individuals are harder to locate and retain than entry-level roles. In addition to a number of demographic opportunities, the province's ample workforce development efforts are well-placed to respond to the challenges identified in this report, building strong and clear career paths to retain young workforce entrants, considering ways to streamline recruitment and immigration processes for international talent, and retaining and upskilling existing professionals.

Appendix

I Research Methods and Tools

This study included a comprehensive review of relevant literature and a secondary data scan, use of webscraped data, and two key primary research tools, described below.

Secondary Literature Review, Data Review, and Webscraped Data

An initial literature review focused on studies relevant to cybersecurity workforce development and labour needs in Canada, the US, and around the world, and a second literature review focused on career pathways and cybersecurity education options in New Brunswick. The secondary data review focused on existing cybersecurity-demand-related information, primarily from Statistics Canada. In addition, extensive webscraping was conducted to gather information on the number of cybersecurity job postings within New Brunswick, and with Canadian data for comparison, from August 2019 to January 2020. An extensive list of key webscraping search terms for cybersecurity job titles, skillsets, and certifications was generated through the study's **Advisory Committee**, a group of personnel with sector expertise who advised research progress through three Advisory Committee meetings: a launch meeting in July 2019, an interim meeting in November 2019, and a validation meeting in February 2020.

ICT Occupations – List of NOCs

Throughout this study, where unemployment rates are presented for the ICT sector either in Canada or in New Brunswick, the figures include the following NOCs:

NOC Code	Description
0015	Senior managers - trade, broadcasting and other services, n.e.c.
0211	Engineering managers
0213	Computer and information systems managers
0601	Corporate sales managers
1123	Professional occupations in advertising, marketing and public relations
1253	Records management technicians
2133	Electrical and electronics engineers
2147	Computer engineers (except software engineers and designers)
2148	Other professional engineers, n.e.c.

2161 Mathematicians, statisticians and actuaries
2171 Information systems analysts and consultants
2172 Database analysts and data administrators
2173 Software engineers and designers
2174 Computer programmers and interactive media developers
2175 Web designers and developers
2241 Electrical and electronics engineering technologists and technicians
2281 Computer network technicians
2282 User support technicians
2283 Information systems testing technicians
4163 Business development officers and marketing researchers and consultants
5223 Graphic arts technicians
5224 Broadcast technicians
5241 Graphic designers and illustrators
7241 Electricians (except industrial and power system)
7242 Industrial electricians
7243 Power system electricians
7244 Electrical power line and cable workers
7245 Telecommunications line and cable workers
7246 Telecommunications installation and repair workers
7247 Cable television service and maintenance technicians

Primary Research Tools

New Brunswick Cybersecurity Employer Survey. This survey, distributed by ICTC in autumn 2019, was shared with a purposive sample of 178 organizations identified as (a) headquartered or with a physical presence in New Brunswick and (b) hiring cybersecurity-related personnel, across a range of sectors and industries. The target respondent was a senior staff member familiar with cybersecurity hiring needs in the province. Organizations were encouraged to share and redistribute the survey where appropriate.

In total, the survey had 54 responses, eight of which were removed for data quality purposes. Of the 46 remaining responses, 41 were validated as complete and relevant, while the other five were only partially complete but came from relevant organizations and, as such, were considered for some components of the analysis (for a response rate of 23 – 26%, at 41 complete to 46 partial responses, respectively). The survey asked questions about the organization, its current cybersecurity workforce, its hiring needs, and its priorities for roles and skills.

Key Informant Interviews. The study involved 16 Key Informant Interviews (KIIs) with a range of senior cybersecurity personnel working in New Brunswick. A KII is a semistructured, in-depth interview with a professional with industry or policy expertise in the target region. Two respondents were different representatives of the same organization. All others were distinct. Interviews ranged from 45 minutes to one hour, and interviewees were given a detailed overview of confidentiality protocols and the study's parameters before interviews began. Interviewees were asked about the organizations' business cases, current and ideal cybersecurity workforces, recruitment efforts, and workforce development efforts. Conversations also explored the province of New Brunswick's cybersecurity ecosystem, public–private sector relationships, and unique economic opportunities for cybersecurity within New Brunswick.

Limitations and Opportunities for Future Research

A number of limitations were encountered in this study. With regard to secondary literature and data, a number of analyses are based on information from Statistics Canada that is suppressed below a certain threshold in order to protect participant anonymity: specifically, this applies to some of the Labour Force Survey (LFS) data for New Brunswick. When using LFS data, suppressed months were eliminated from the dataset in order to avoid artificially low figures. In addition, this study relies heavily on Statistics Canada's Survey of Cybersecurity and Cybercrime (2017), which only provides national figures. In consultations with the research team, Statistics Canada noted that this national survey was not designed for regional breakdowns, in part due to the borderless nature of cybercrime: as such, it is difficult to gather insights specific to New Brunswick from this particular source.

ICTC's webscraping process was conducted for six months, from August 2019 – January 2020, and in further research, it would be interesting to assess the number of jobs being posted in the spring and summer months. The webscraping analysis made several assumptions: (a) that one post = one job and (b) that the same job title, description, and company left up for more than one month = unfilled instead of a repost. In addition, as noted in the study, not all jobs are posted – accordingly, it is likely that this dataset missed some of the cybersecurity roles available in the province.

With regard to primary data collection, the employer survey enjoyed a response rate well within the standard range for external email distribution (at 23 – 26% for complete – valid responses, respectively, see above) but further research should attempt to engage a sample of a minimum of 100 employers with cybersecurity hiring expertise in New Brunswick to inform additional findings.

Finally, the project Advisory Committee identified several potential areas for fruitful future research.

While collecting extensive data on outsourcing was beyond the scope of this study, future research on the types of cybersecurity jobs that are outsourced, to which countries, and why, would be valuable for industry members and job seekers in Canada.

The number of women in cybersecurity has remained low for many years: further investigations into which sciences are and aren't successful in attracting women, and why, would be a productive study within the province.

During interviews, this study explored barriers to hiring skilled talent and the issue of extensive and problematic screening criteria and security protocols for immigrants was a consistent theme. Further research could explore effective ways of revising current processes for identifying and admitting new entrants to the Canadian labour force.

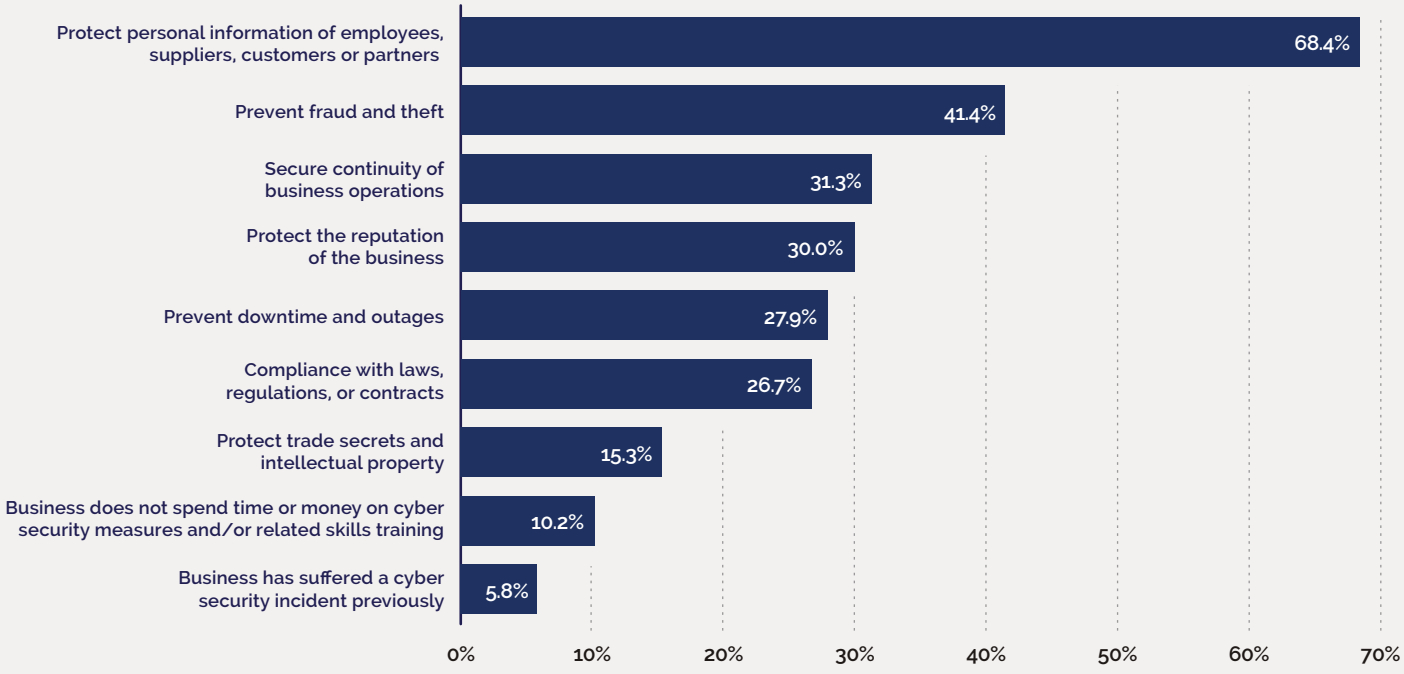
It would be interesting to know, in detail, where college and university students in cybersecurity come from (in terms of location and academic background) and where they are hired. In other words, while this study was primarily an analysis of demand for cybersecurity personnel, future research should seek to extensively explore both supply and demand, examining training, immigration, and career pathways in order to better understand the full picture of cybersecurity labour in New Brunswick.

II Additional Figures

In the section Cybersecurity Demand: Employers by Sectors and Size, this study explores the reasons why businesses in Canada's private sector do not have cybersecurity personnel. However, the same survey provides data on companies' reasons for having staff dedicated to cybersecurity, as illustrated below.

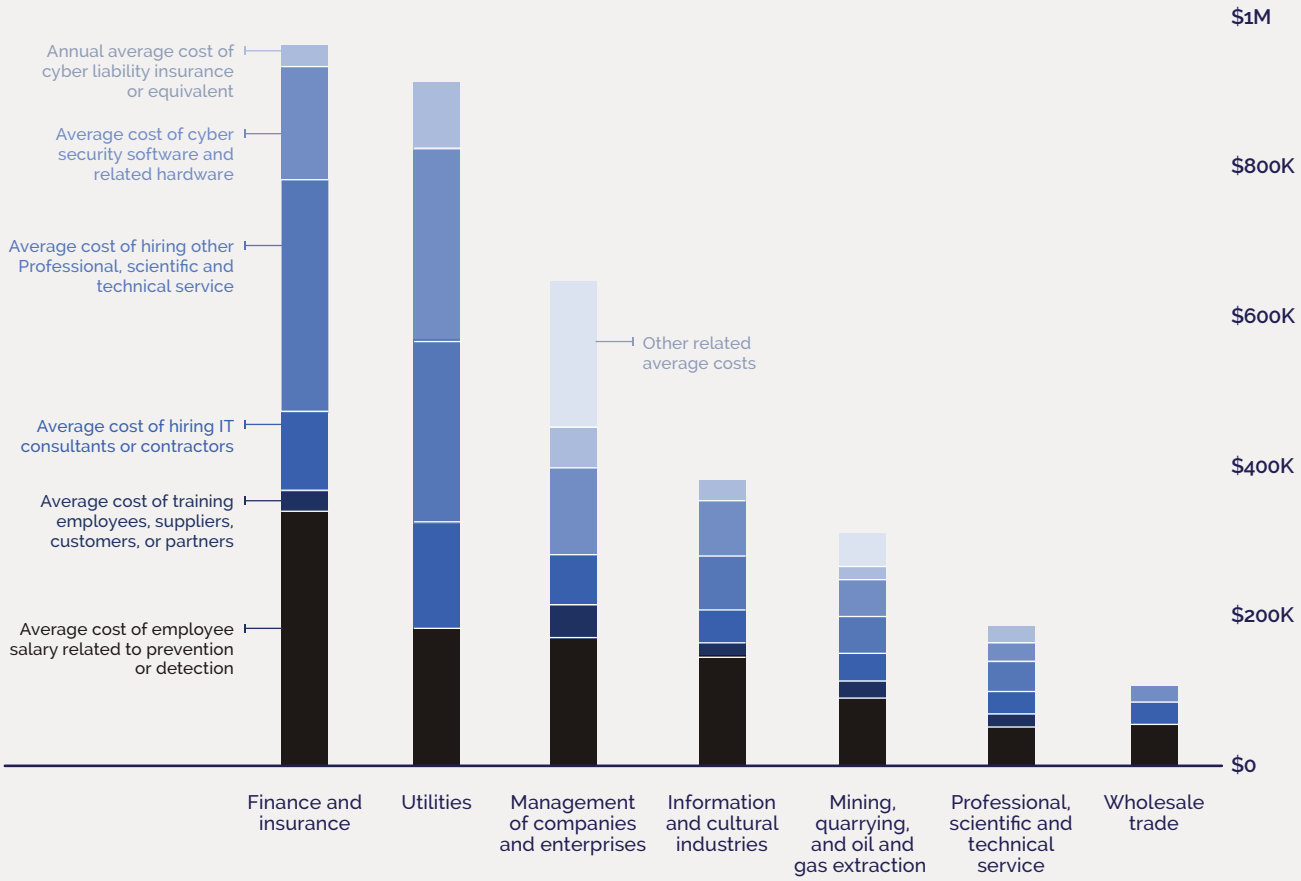
Reasons for Prioritizing Cybersecurity: Private Sector Average

by % of respondents who selected each reason



In addition, the Statistics Canada Survey of Cybersecurity and Cybercrime (2017) takes a look at the sectors spending the most money on cybersecurity, and where that money goes. It is clear that hiring and salaries are, above and beyond, the greatest expense, with cybersecurity software in second place (though with great variation in cost by industry).

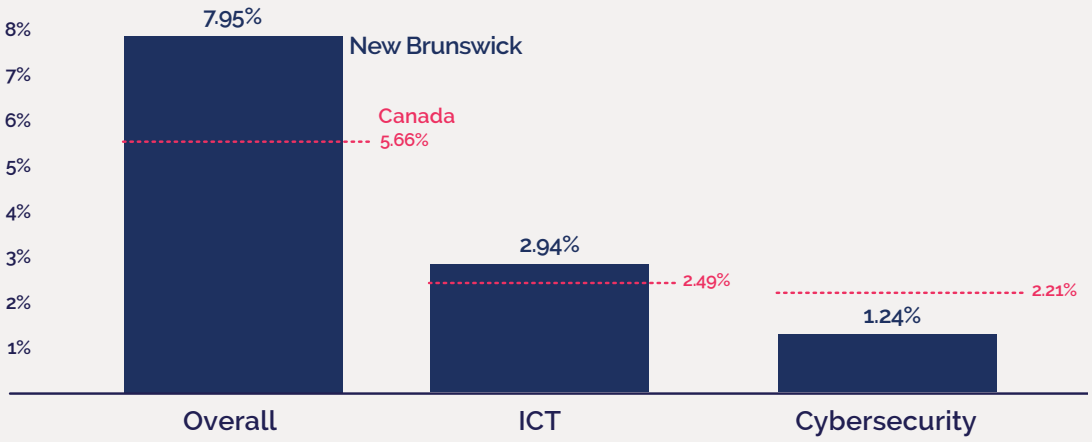
Reasons for Prioritizing Cybersecurity: Private Sector Average



Source: Statistics Canada, Canadian Survey of Cyber Security and Cybercrime, 2017

Finally, while Figure 1 in the study illustrates unemployment over time, the figure below provides a comparison between three different unemployment rates for Canada and New Brunswick for 2019, using the same NOC definitions of these sectors as described in text.

Unemployment Rates by Region, 2019



Source: Statistics Canada Labour Force Survey