CYBERSECURITY TALENT DEVELOPMENT:

PROTECTING CANADA'S DIGITAL ECONOMY

ICTC CTIC

Research by

The Information and
Communications Technology Council

Funded by the Government of
Canada's Student Work Placement
Program (SWPP).

Canada

IN PARTNERSHIP WITH THE ICTC NATIONAL ADVISORY COMMITTEE
ON CYBERSECURITY TRAINING (INACCT)

MAY 2022

PREFACE

The Information and Communications Technology Council (ICTC) is a not-for-profit, national centre of expertise for strengthening 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 an expansive network of industry leaders, academic partners, and policy makers from across Canada, ICTC has empowered a robust and inclusive digital economy for 30 years.

ICTC National Advisory Committee on Cybersecurity Training (INACCT):

To better understand the needs of the cybersecurity industry and the gaps in training that may exist in Canada, ICTC has invited a group of subject matter experts from academia, industry, government, and associations to examine the challenges and recommend solutions. The ICTC National Advisory Committee on Cybersecurity Training (INACCT) has been tasked to examine the gaps in post-secondary student skills and programs, the barriers to entry and diversity issues of the sector and the training delivery models most suited to meet the demand. INACCT's assumptions have been passed on to ICTC's Digital Think Tank for validation. Preliminary findings from both employer and post-secondary student surveys indicate that many of the Committee's assumptions were correct.

To cite this report:

Chris Herron and Trevor Quan, "Cybersecurity Talent Development: Protecting Canada's Digital Economy," (Ottawa, ON: Information and Communications Technology Council, March 2022).

Researched and written by Trevor Quan (Senior Research & Policy Analyst, ICTC) and Chris Herron (Research Analyst, ICTC) with generous support from Rob Davidson (Director, Data Science, ICTC), Xinyi Lin (Data Scientist, ICTC), and Alexandria Chiasson (Partnership Coordinator, ICTC).

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF ACRONYMS USED IN THIS STUDY

Acronym	Meaning
AI	Artificial Intelligence
ICTC	Information and Communications Technology Council
INACCT	ICTC (see above) National Advisory Committee for Cybersecurity Training
IoT	Internet of Things
IP	Intellectual Property
$(ISC)^2$	International Information System Security Certification Consortium
NICE	National Initiative for Cybersecurity Education (US)
NOC	National Occupation Code
NSA	National Security Association (US)
SME	Small to Medium Enterprise
UK	United Kingdom
US	United States
WIL	Work Integrated Learning

EXECUTIVE SUMMARY

Digitalization is rapidly transforming the global economy, but it has also spurred the rapid growth in the prevalence and intensity of cyber crime. Cybersecurity is a multifaceted field with numerous specializations, including Network Administration, General Cybersecurity Analytics, Incident Response, and Digital Forensics. Globally, there is a significant deficit in cybersecurity talent. In 2021, the international association for information security leaders (ISC)² reported a global cybersecurity workforce gap of 2.72 million workers, down from 3.12 million the previous year.[1] Canada is no exception to this trend. The same (ISC)² study found that there were 123,696 cybersecurity professionals in Canada, a large increase compared to two years earlier, but that there remains a talent shortage of 25,000 professionals in the field.[2] In short, in a field with close to no unemployment, about one in six postings go unfilled.

ICTC has formed INACCT, the ICTC National Advisory Committee for Cybersecurity Training, to provide an evidence-based approach to addressing the talent crisis in cybersecurity. This research report, focused on describing the talent situation in cybersecurity in Canada and proposing potential policy solutions, summarizes existing scholarship on the cybersecurity ecosystem domestically and abroad, and combines it with primary research data from both employers and students. The report considers the viability of alternative pathways to obtaining cybersecurity education, such as micro-learning experiences and work-integrated learning.

Our research confirms that cybersecurity is a rigorous, specialized field facing a sharp talent deficit. Due to high salaries driven by a talent shortage, many organizations cannot find the necessary personnel. And yet, despite very high compensation packages, there is widespread self-selection out of the field; close to a third of male respondents and around half of female students eventually leaving the field during their education. Among those who become fully-fledged cybersecurity employees, feelings of burnout are common. In some ways, Canada's cybersecurity talent situation may be more intense than in the United States for several reasons. Firstly, the absence of a nationally implemented skills framework (similar to the NICE in the United States) has impeded communication between employers and potential cybersecurity employees about the skills necessary to succeed. Secondly, there is a gap in communication between industry and academia. Finally, Canada faces the risk of "talent poaching" by the United States, where the tech industry typically offers even stronger compensation packages.

Nevertheless, the study also finds positive developments in Canadian cybersecurity education. Micro-learning and work integrated learning programs are well-received by former students in the field, with a majority indicating that these programs might have deterred their decision to leave the field. Since there is no significant gap between what cybersecurity students desire to study and the needs of industry, providing students with suitable educational programs should enable the workforce to grow while satisfying the needs of industry.

[1] "A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)² Cybersecurity Workforce Study, 2021," (ISC)², 2021, https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[2] "A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)² Cybersecurity Workforce Study, 2021," (ISC)², 2021, https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

INTRODUCTION

What is Cybersecurity?

Cybersecurity can be broadly defined as the practice of protecting oneself and one's organization from digital attacks.[3] Cybersecurity includes network, system, and program security responsibilities performed by specialists; planning for and responding to cyber incidents; as well as training personnel throughout one's organization to be cyber aware. Cybersecurity encompasses any measures taken to protect online information as well as any assets connected to a network, while securing the infrastructure that it resides on.[4] Cybersecurity is a multifaceted, multi-staged process that prevents threats as much as possible and then responds to them. Examples of common cyberattacks that cybersecurity must protect against include phishing, watering holes, ransomware, spear phishing, or the deployment of botnets.[5] To supplement the growing body of research on cybersecurity labour market research in Canada, ICTC has undertaken a national survey that encompasses both cybersecurity employers as well as cybersecurity students who will enter the future workforce. These findings, analysis, and future implications are discussed further in this report.

The Growing Threat of Cyber Crime

Digitalization is transforming the economy worldwide and has been accelerated by the COVID-19 pandemic. A 2018 study by Tech Pro estimated 70% of companies either have a digital transformation strategy in place or are working toward one.[6] A July 2020 survey of 800 company executives found that since the start of the COVID-19 pandemic, 36% of companies have accelerated the digitalization of their supply chain, 48% have accelerated digitalization of customer channels, 85% have accelerated digitalization of employee interaction and collaboration, and 67% have accelerated automation and artificial intelligence.[7] An estimated 80% of the value of Fortune 500 companies originates in intellectual property (IP), almost all of which is stored in digital form.[8]

With businesses becoming increasingly reliant on digital solutions, it is unsurprising that cyber crime is growing in sophistication, frequency, and impact. A World Economic Forum survey of global leaders in 2021 found 39% of respondents saw cybersecurity failures to be a clear and present

---

[3] Cisco, "What is cybersecurity" https://www.cisco.com/c/en_ca/products/security/what-is-cybersecurity.html#:~:text=Cybersecurity%20is%20the%20practice%20of,or%20interrupting%20normal%20business%20processes.

[4] "Spotlight on Cybersecurity" Government of Canada, accessed 2022: https://www.tradecommissioner.gc.ca/guides/spotlight- pleins_feux/spotlight_cybersecurity_pleins_feux_cybersecurite.aspx?lang=eng#TC1

[5] Ibid

[6] M. Wachsman, "Survey: Despite steady growth in digital transformation initiatives, companies face budget and buy-in challenges" *ZD Net*, 2018, https://www.zdnet.com/article/survey-despite-steady-growth-in-digital-transformation-initiatives-companies-face-budget-and-buy-in/

[7] S. Lund, W.-L. Cheng, A. Dua, A. De Smet, O. Robinson, and S. Sanghvi, "What 800 executives envision for the post-pandemic workforce" *McKinsey & Company, 2020*, https://www.mckinsey.com/featured-insights/future-of-work/what-800-executives-envision-for-the-postpandemic-workforce?utm_campaign=Digital%20Policy%20Salon&utm_medium=email&utm_source=Revue%20newsletter

[8] J. Desjardins. "Cybersecurity: Fighting a Threat That Causes $450B of Damage Each Year" *Visual Capitalist, 2017*, https://www.visualcapitalist.com/cybersecurity-fighting-450b-damage/

[9] "The Global Risks Report 2021." *World Economic Forum, 2021*, http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

INTRODUCTION

danger to the global economy, second only to climate change.[9] The global cost of cyber crime is predicted to reach $6 trillion USD by 2021.[10]

In response to the rise of cyber crime, cybersecurity has grown rapidly. Market research has estimated that the cybersecurity market has grown 35 times over 13 years, prior to the most recent five-year investment cycle.[11] Industry analysts estimate growth ranging from 8-15% year-over-year and, according to the research firm Gartner Inc., the global cybersecurity market could reach $170.4 billion in 2022.[12]

The Precarious Cybersecurity Labour Market

Despite increased spending in cybersecurity, there are numerous structural challenges facing the field. Even prior to larger issues of the "Great Resignation" post-2020, which is characterized by historic level of employee resignation and turnover,[13] there were concerns over cybersecurity staffing. A global information security systems survey found that a third of respondents believed a global skills shortage had a significant impact on their organization. Two-thirds of respondents said that skills shortages increased the workload on existing staff.[14] There is some evidence that increased pressure and staff shortages are leading to lower job satisfaction and regular solicitations by recruiters.[15]

Governments, which possess detailed and personal information about their citizens such as addresses, e-mails, and social security numbers, are prime targets for cyberattacks. Yet it is a particular challenge to recruit and retain cybersecurity professionals in the public sector. Identified issues in the public sector include lower levels of pay compared to the private sector, insufficient funding, bureaucratic hurdles, cumbersome hiring processes, background checks, and burnout.[16]

---

[10]"Cyber Crime Damages $6 Trillion by 2021," *2017, Cybercrime Magazine*, https://cybersecurityventures.com/hackerpocalypse-cyber crime-report-2016/

[11] Morgan, S., "Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021," Cyber crime Magazine, June 2019: https://cybersecurityventures.com/cybersecurity-market-report/

[12] Ibid.

[13] Liu, J. " A record 4.4 million people quit in September as Great Resignation shows no signs of stopping," CNBC, Nov 2021: https://www.cnbc.com/2021/11/12/a-record-4point4-million-people-quit-jobs-in-september-great-resignation.html

[14] Vizard, M. " Survey identifies root causes of cybersecurity staff turnover," Barracuda, May 2019: https://blog.barracuda.com/2019/05/10/survey-identifies-root-causes-of-cybersecurity-staff-turnover/

[15] Ibid.

[16] Rosenkrantz, H., "The Big Quit: Why Cybersecurity Pros Are Leaving Government," Endpoint, Nov 2021: https://endpoint.tanium.com/the-big-quit-why-cybersecurity-pros-are-leaving-government/

INTRODUCTION

In a 2017 international study, 66% of information security workers responded that they did not feel adequately staffed to address the increase in cyber threats.[17] In 2021, (ISC)² reported a global cybersecurity workforce gap of 2.72 million workers, down from 3.12 million in the previous year.[18] Close to a third of the demand for cybersecurity talent is in just three countries – Brazil, the United States, and Mexico. The following figure shows the large number of additional employees that are needed.

Given the mounting talent crisis in cybersecurity, this ICTC survey was designed to investigate challenges in the Canadian cybersecurity talent development pipeline. It will be crucial to address this labour shortage to ensure Canadian companies and public sector organizations are protected.

ICTC's previous research on cybersecurity has also found challenges around retaining cybersecurity talent in the face of competition from other provinces and the U.S., as well as a mismatch between workforce skills and the cybersecurity requirements of organizations. The single most salient challenge was a dearth of highly skilled, experienced cybersecurity professionals and a relative surplus of junior level talent.

NUMBER OF CYBERSECURITY PROFESSIONALS NEEDED WORLDWIDE IN 2021, BY COUNTRY

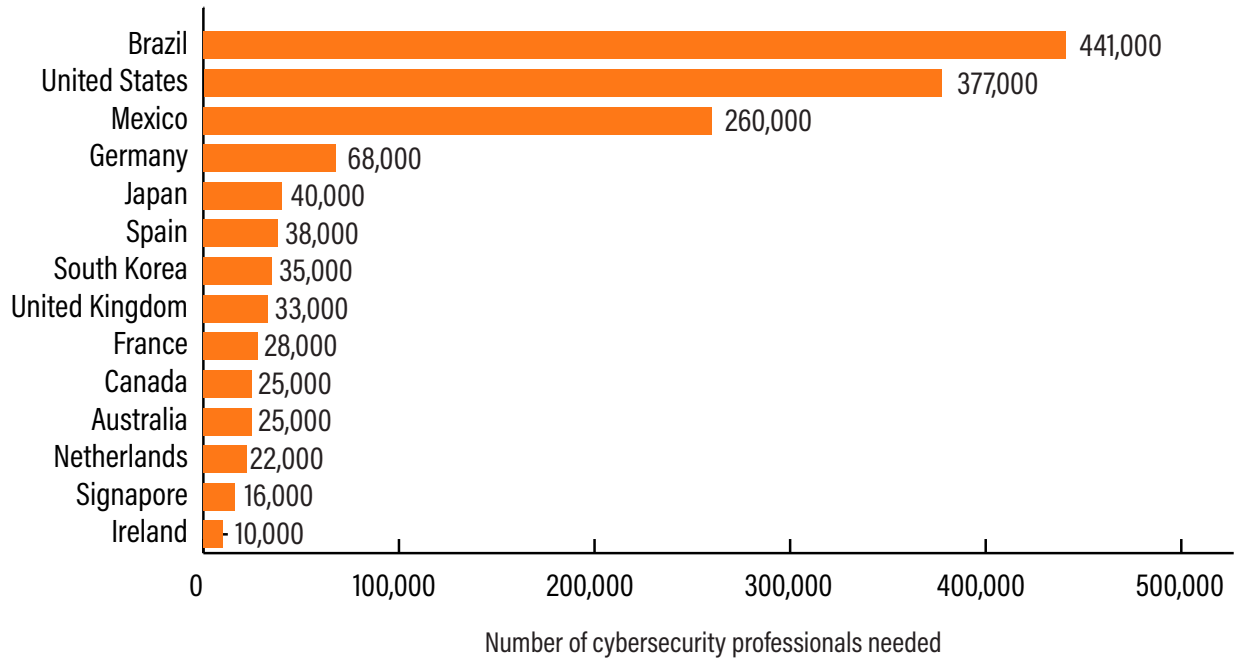


Figure 1: Number of cybersecurity workers needed worldwide.

[17] Frost & Sullivan, "2017 Global Information Security Workforce Study," Center for Cyber Safety and Education, https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx

[18] "A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)² Cybersecurity Workforce Study, 2021," (ISC)², 2021, https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

THE CYBER CRIME THREAT IN CANADA

Although cyber crime is a global problem, it is of particular significance to Canada. The 2018 National Exposure Index published by cybersecurity vendor Rapid7 declared Canada to be the third most exposed country to cyber crime out of 187 countries, following the United States and the United Kingdom.[19] Research by IBM found that data-breach incidents (frequently caused by cyberattacks) in Canada are among the most expensive in the world to fix, costing an average of $5.72 million per incident.[20] In 2017 alone, over one-fifth (21%) of Canadian businesses of all sizes were impacted by a cybersecurity incident. The Canadian Internet Registration Authority reported in 2018 that four in 10 Canadian small and medium size enterprises (SMEs) experienced phishing and virus attacks: about a third experienced Trojans and spyware, and 27% were attacked by ransomware. Meanwhile, a 2017 report noted that Canadian consumers lost $1.5 billion (USD) due to cyberattacks.[21]

Numerous factors make Canada vulnerable to cyber threats. One is deteriorating international relations; a 2020 Canadian government report stated the largest threat for Canadian cybersecurity is the rise of cyber crime from China and Russia, and warned that state-sponsored attacks against Canada would increasingly occur.[22] Another is sheer exposure to the internet. In 2019, the average Canadian spent 43.5 hours online per month, more than any other country.[23]

Since COVID-19, the threat of cyber crime has only increased in Canada—nearly half of Canadians (44%) are spending more time online compared to the start of the COVID-19 pandemic.[24] In a survey of Canadian security leaders in 2020, 86% said their organizations suffered a data breach in 2020. Nearly nine in 10 (88%) of those affected by data breaches experienced "material" impacts on the organization. Around four-fifths (78%) reported that their organizations were facing more attacks than in previous years, and a similar proportion indicated that attacks had become more sophisticated.[25]

---

[19] "National Exposure Index 2018," Rapid 7, 2018, https://www.rapid7.com/globalassets/_pdfs/research/rapid7-national-exposure-index-2018.pdf

[20] S. Randall. "Canada is top 3 for data breach costs warns IBM," Wealth Professional, 2021, https://www.wealthprofessional.ca/news/industry-news/canada-is-top-3-for-data-breach-costs-warns-ibm/358484

[21] 2017 Norton Cyber Security Insights Report Global Results, https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/reports/2017-ncsir-global-results-en.pdf

[22] "National Cybersecurity Threat Assessment 2020." Canadian Centre for Cybersecurity, 2020, https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf

[23] "National Cyber Security Strategy." Government of Canada, 2018, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

[24] "Canadians spend more money and time online during pandemic and over two-fifths report a cyber incident." Statistics Canada, 2020, https://www150.statcan.gc.ca/n1/daily-quotidien/201014/dq201014a-eng.htm

[25] "Canada Security Insights Report 2021," VMWare, 2021, https://www.carbonblack.com/resources/canada-security-insights-report-2021/

Canada's Cybersecurity Ecosystem

Comparitech named Canada among the countries with the best cybersecurity systems in 2021, based on an analysis of over 70 factors.[26] In 2017, Canadian businesses spent $8 billion on salaries for cybersecurity employees, consultants, and contractors alone.[27] Cybersecurity analysts were also identified as one of the top 10 digital roles for growth in ICTC's 2023 Outlook Report, based on consultation with experts in the ICT sector.[28] According to a 2020 the (ISC)² Cybersecurity Workforce Study report, Canada had 101,963 people working in cybersecurity-related professions and a talent shortfall of 16,552 individuals. This is an increase of 17,963 people in total employment for the profession compared to 2019. By 2021, (ISC)² reported that the Canadian cybersecurity workforce had grown to more than 123,696 people. However, the talent deficit grew even faster, jumping to 25,000.[29] Canada's cybersecurity shortfall represented 17% of its total cybersecurity postings. While this was lower than the United States (25%), it was higher than the UK (10%), Germany (13%), and around the same as both Australia and France (16%). The cybersecurity sector's rapid growth appears poised to continue.

In 2018, nearly three-quarters (73%) of Canadian executives predicted their number of full-time security staff would increase in the following three to five years, while one-quarter (25%) expected their cyber teams to grow by more than 25 percent.[30]

While there is limited literature available on the impact of the "brain drain" on the cybersecurity sector, the loss of Canadian talent to the United States demands attention and points to the fragility of Canada's cybersecurity ecosystem. The U.S. cybersecurity talent shortfall is nearly 15 times larger than Canada's (377,000 jobs versus 25,000 jobs). Furthermore, the United States offers considerably higher salaries to employees. The average cybersecurity analyst salary in Canada is $81,881 CAD per year in 2022.[31] By contrast, the salary for an "Information Security Analyst" (a classification which includes Cybersecurity Analyst) in the United States was $103,590 USD in 2020[32] (equivalent to $129,677 CAD[33]), a figure 58% higher. Any effective cybersecurity education strategy must consider the risk of substantial talent loss to the United States, particularly during administrations that enthusiastically embrace skilled immigration.

---

[26] P. Bischoff, "Which countries have the worst (and best) cybersecurity?" *Comparitech,* 2021, https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

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

[28] Ibid.

[29] "A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)² Cybersecurity Workforce Study, 2021," (ISC)², 2021, https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[30] "The Changing Faces of Cybersecurity: Closing the cyber risk gap," *2020, Deloitte*, https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF

[31] https://ca.talent.com/salary?job=cyber+security+analyst#:~:text=The%20average%20cyber%20security%20analyst%20salary%20in%20Canada%20is%20%2481%2C881,up%20to%20%24108%2C474%20per%20year.

[32] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[33] Based on the exchange rate reported on April 1, 2022

SIZE OF CYBERSECURITY WORKFORCE WORLDWIDE IN 2021, BY COUNTRY

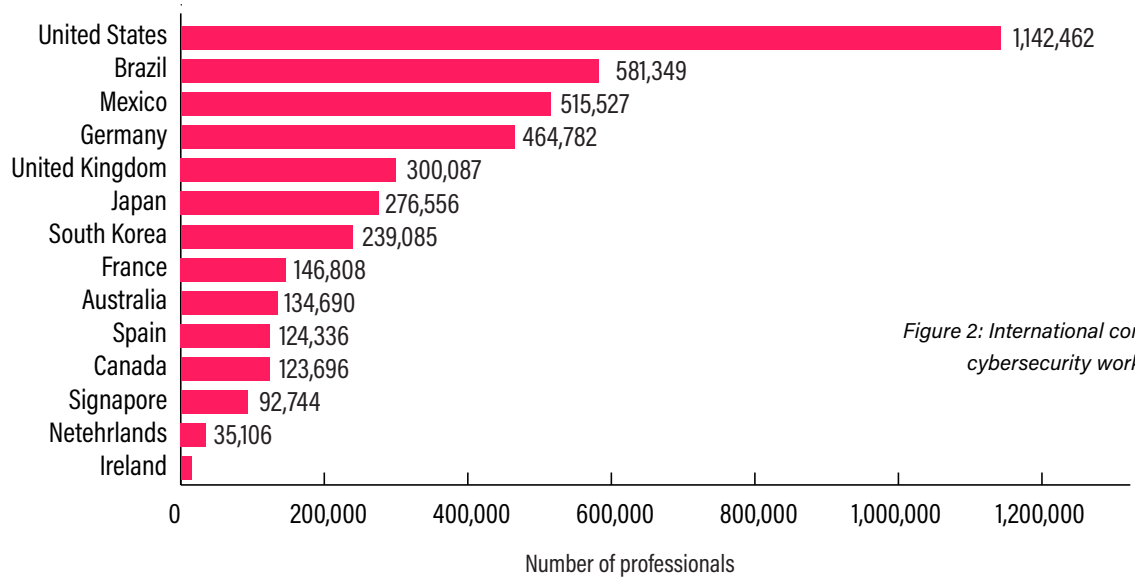


Figure 2: International comparisons of cybersecurity workforces, 2021

While Canada's workforce gap in cybersecurity is not as acute as some other countries, the industry is seeing severe shortages in cybersecurity personnel.

Organizations in Canada have numerous motivations for prioritizing cybersecurity, but the 2017 Canadian Survey of Cybersecurity and Cyber Crime found that the main motivation was protecting personal information. This was a motivation for 68.4% of respondents. Other key motivators were preventing fraud and theft (mentioned by 41.4% of respondents), securing the continuity of business operations (31.3%), protecting reputation (30.0%), and preventing down-time and shortages (27.9%). Only 10.2% of respondents reported that their business did not spend time or money on cybersecurity-related skills or training.

REASONS FOR PRIORITIZING CYBERSECURITY: PRIVATE SECTOR AVERAGE

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

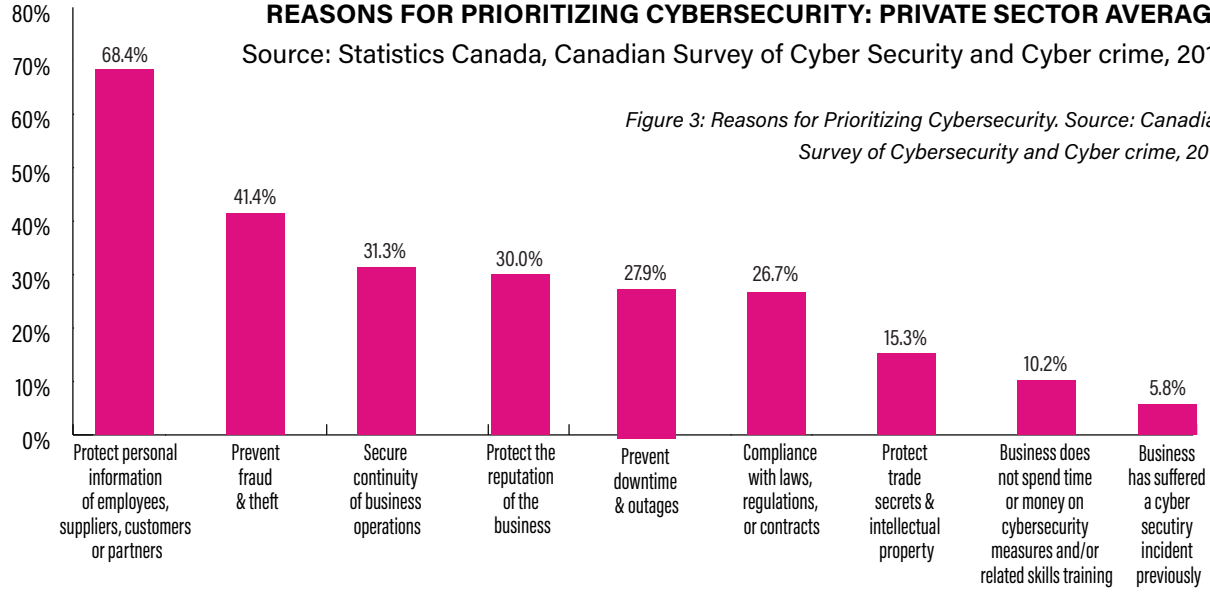


Figure 3: Reasons for Prioritizing Cybersecurity. Source: Canadian Survey of Cybersecurity and Cyber crime, 2017.

ICTC's in-house Employer Survey for this project also confirmed that while cybersecurity roles are in high demand among employers, they remain less in demand than software or business/finance roles. Cybersecurity roles were the fourth ranked category of technology employment, ahead of data roles or operations/logistics roles.

ROLES ORGANIZATION MOST ACTIVELY SEEKING TO HIRE

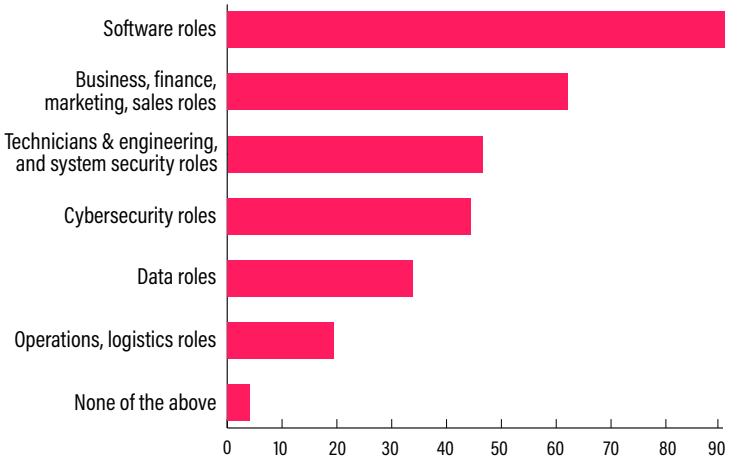


Figure 4: Most demanded role types among Canadian tech employers, 2022

Classifying Cybersecurity Roles

Cybersecurity is not a monolithic field; while the field certainly contains many generalists working in small to medium sized organizations, it also has numerous areas of specializations, particularly evident when one examines the teams of large organizations. Understanding the nuanced distinctions between subdisciplines of cybersecurity can inform policy, ensuring that resources are directed at the roles with the most growth potential.

The National Initiative for Cybersecurity Education (NICE) Framework is the dominant global framework for classifying cybersecurity roles. This American framework provides standardized terminology for cybersecurity jobs. This American framework has been adopted by organizations around the world with the intention of adopting standardized terminology for cybersecurity jobs and skills.[34] It classifies the field of cybersecurity according to the following:

- seven categories comprised of 32 specialty areas
- Over 1000 Tasks, including determining how continuous monitoring results will be used in ongoing authorization and identifying and directing the remediation of technical problems encountered during the testing and implementation of new systems
- Over 600 Knowledge Areas including Virtual Machine Technologies and White/Blacklisting
- Over 300 Skills, including Fusion Analysis and Anticipating New Security Threats
- 176 Abilities, including Maintaining Databases and Designing Incident Response for Cloud Service Models

[34] Ibid.

Below is a summary of the seven key types of roles.[35]

CATEGORIES	DESCRIPTIONS[36]	COMMON JOB TITLES IN CANADA[37]
Securely Provision (SP)	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
Operate and Maintain (OM)	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
Oversee and Govern (OV)	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
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal IT systems and/or networks	Cyber Analyst Security/Cyber Defence Infrastructure Engineer Cyber Incident Responder Vulnerability Analyst Security Operations Centre Manager
Analyze (AN)	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
Collect and Operate (CO)	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
Investigate (IN)	Investigates cybersecurity events or crimes related to IT systems, networks, and digital evidence	Cyber/Digital Forensics Analyst Cyber Investigator

Figure 5: NICE Framework Workforce Categories

[35] 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

[36] 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

[37] 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*.

Previous research by ICTC has uncovered a degree of comparability between the NICE Framework, the Deloitte Cybersecurity Personas, and NOC (National Occupation Code)-based system used by ICTC. For example, NOC 0213 corresponds to the Strategist/Oversee and Govern (OV) classification, while the remaining four NOC codes correspond to Advisor/Securely Provision (SP) and Defender/ Operate and Maintain (OM) classifications. Also, under the 2021 version of the NOC system, NOC 2122 – (Cybersecurity Specialists) includes job titles such as cybersecurity analyst, informatic security analysts, informatic security consultants, IT security analysts, and systems security analysts. As such, it straddles the "Securely Provision" and "Protect and Defend" categories of the NICE Framework.

That said, the NOC system in its current state does not have a meaningful equivalent for three remaining categories used by Deloitte and NICE, which could mean a substantial undercounting of cybersecurity roles using NOC-based approaches.

NOC	DELOITTE PERSONA	NICE CATEGORY	COMMON JOB TITLES
0213 – Computer and Information Systems Managers	Strategist	Oversee and Govern	Chief Information Security Officer Cyber Strategy Analyst Cyber Policy Analyst Cyber Program Manager
2171 – Information Systems Analysts and Consultants **2283 – Information Systems Testing Technicians** **2122 – Cybersecurity Specialists**	Advisor	Securely Provision	Security/Risk Manager Systems/Security Analyst Software/Systems Developer/Planner
2172 – Database Analysts or Data Administrators **2281 – Computer Network Technicians**	Defender	Operate and Maintain	Data/Database or Security Administrator Technical Support Representative Network/Systems Administrator Network/Systems Analyst
2122 – Cybersecurity Specialists	Firefighter	Protect and Defend	Cybersecurity Analyst Security/Cyber Defence Infrastructure Engineer Vulnerability Analyst
No equivalent	Hacker	Collect and Operate	Ethical Hacker/Collections Operator Threat Hunter/Cyber Operator Cyber Operational Planner
No equivalent	Scientist	Analyze	Threat Intelligence Analyst Cyber Analytics Manager Data Scientist Language Analyst/Computational Linguist
No equivalent	Sleuth	Investigate	Cyber/Digital Forensics Analyst Cyber Investigator

Figure 6: Correspondence between NICE Framework, Deloitte Cybersecurity Personas, and Cybersecurity related NOCs

CYBERSECURITY IN CANADA

Estimating the Size of the Cybersecurity Workforce

The 2019 Cybersecurity Workforce Study by (ISC)[2] estimated that there were 84,000 cybersecurity professionals in all of Canada in 2019.[39] The 2021 edition of the same study estimated 123,696 cybersecurity professionals in Canada. This represented a large increase compared to two years earlier, but there remained a talent shortage of 25,000 professionals in cybersecurity.[40]

A lower estimate of cybersecurity professionals can be generated based on Deloitte's report, The Changing Faces of Cybersecurity. Deloitte estimated that the number of cybersecurity professionals in Canada to be 20,000 in 2016 and predicted it would rise to 28,000 in 2021.[41] Deloitte's estimate assumes that cybersecurity roles represent 1.6% of all ICT professionals. Deloitte notes that their estimate is very conservative, adding that "industry analysts typically assume that cybersecurity professionals comprise between 5% to 6% of an organization's IT staff."

Geographic Distribution of Cybersecurity Roles

ICTC found in January 2020 that job postings focused on Cybersecurity were heavily clustered in Ontario. Ontario hosted three-fifths (60%) of Canada's cybersecurity postings, 23.26% more than its share of Canada's population. All of Canada's four Atlantic provinces except for Newfoundland and Labrador punched above their weight in cybersecurity posting share, and the difference was most noticeable in Nova Scotia. By contrast, several areas in Canada were cybersecurity "deserts," which posted significantly lower shares of cybersecurity jobs than their share of the Canadian population. These included Saskatchewan, Newfoundland and Labrador, Manitoba, and the Territories. Alberta and British Columbia both had noticeably lower shares of the Canadian cybersecurity postings, although as major population centres their absolute numbers of postings were still significant.[42]

---

[38] "The Changing Faces of Cybersecurity: Closing the cyber risk gap," 2020, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF

[39] "Strategies for Building and Growing Strong Cybersecurity Teams," 2019, ISC2, https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

[40] "A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)² Cybersecurity Workforce Study, 2021," (ISC)², 2021, https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[41] "The Changing Faces of Cybersecurity: Closing the cyber risk gap," 2020, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF

[42] Herron, C., Rice, F., Snider, N., "Searching for Hidden Talent: Experience and Expertise in New Brunswick's Cybersecurity Community," ICTC, 2020: https://www.ictc-ctic.ca/wp-content/uploads/2020/06/new-brunswick-cybersecurityFINAL.EN_.pdf

POPULATION VS. CYBERSECURITY JOB POSTINGS WHICH PROVINCES ARE PUNCHING ABOVE THEIR WEIGHT? Source: Statistics Canada, ICTC

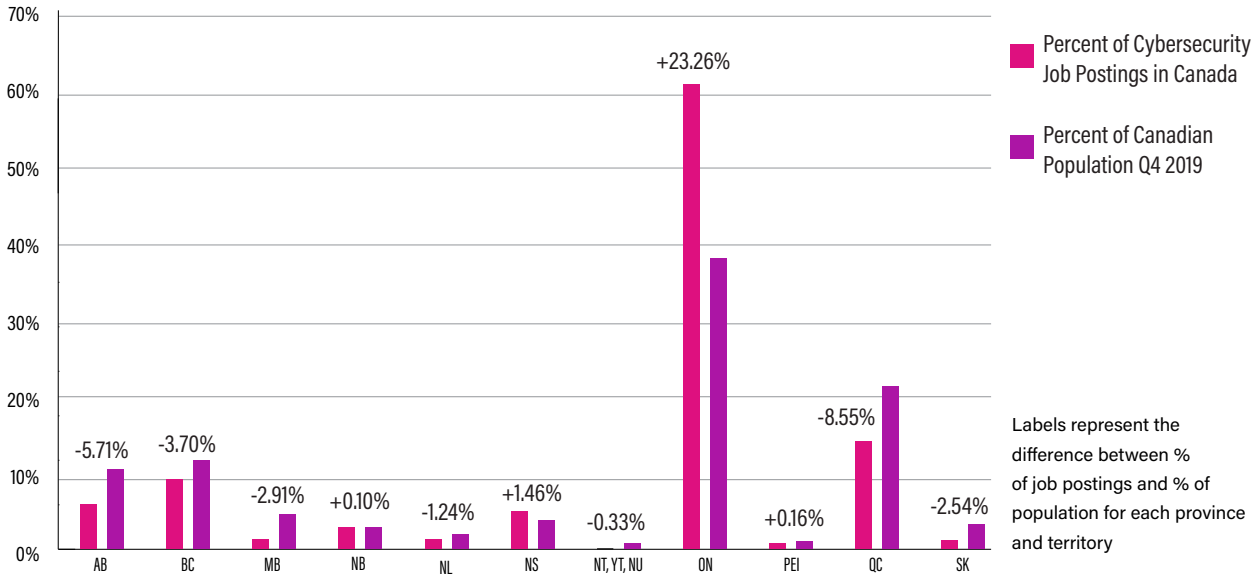


Figure 7: Provinces' and Territories' proportion of the Canadian population compared with their proportion of posted cybersecurity roles. Job posting data is from January 2020. Source: ICTC, Statistics Canada.

Sectoral Composition and Levels of Cybersecurity Employment

Cybersecurity professionals may work for dedicated cybersecurity firms and organizations, academic institutions, or government bodies. Alternatively, cybersecurity professionals may be embedded specialists in a wide variety of sectors. They may be specialists in a field of cybersecurity, cybersecurity generalists, or even generalist IT staff members who have been assigned responsibility for cybersecurity. Previous research has found that investment in cybersecurity personnel is more common in larger organizations across Canada, which could suggest that smaller organizations are more likely to task generalist IT staff with cybersecurity-related responsibilities. One study found that 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+ employees) reported the same.[43] This data is echoed by research by (ISC)², which finds that cybersecurity professionals are most frequently employed in IT services (22%), financial services (8%), and government (7%).[44]

Across Canada, numerous industries employ cybersecurity professionals. The following figure 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.

[43] ICT Adoption Survey, Canadian Chamber of Commerce, 2017

[44] "Strategies for Building and Growing Strong Cybersecurity Teams," 2019, ISC2, https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

TOP 10 INDUSTRIES EMPLOYING CYBERSECURITY PERSONNEL IN CANADA

Source: Statistics Canada, 2017 Canadian Survey of Cyber security and Cyber crime

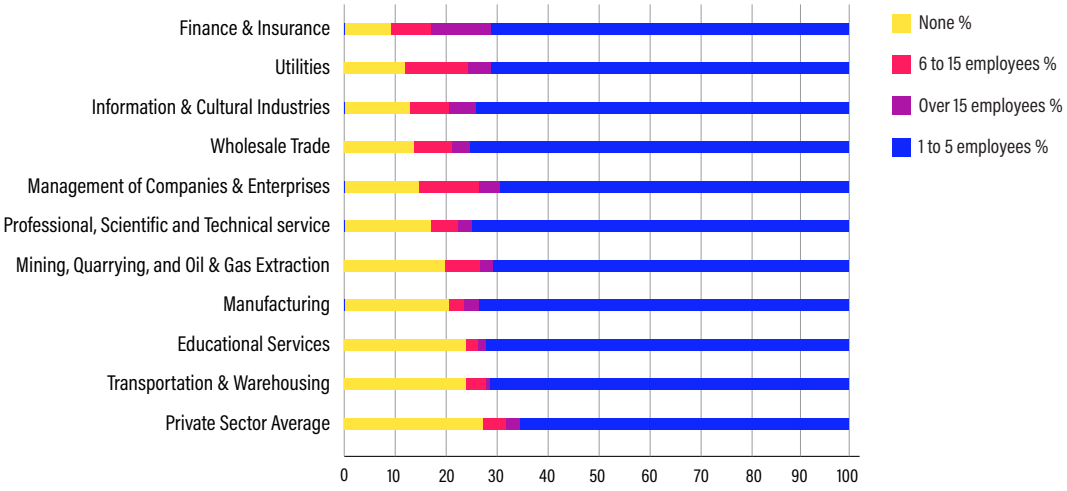


Figure 8: Percentage of businesses indicating the number of employees primarily responsible for overall cybersecurity, including the top 10 industries that are the most likely to have at least one employee responsible for cybersecurity, as well as the private sector average. Source: Statistics Canada 2017 Survey of Cybersecurity and Cyber crime.

Unemployment

Cybersecurity is a highly competitive field with a sharp talent deficit. As such, it is of little surprise that the unemployment rate in the cybersecurity field is very low, even by the standards of the ICT sector. Some international reports on the cybersecurity labour gap tout global unemployment rates as low as 0%.[45] However, these reports are unrealistic as a certain level of frictional unemployment will always occur due to delays between workers switching jobs.

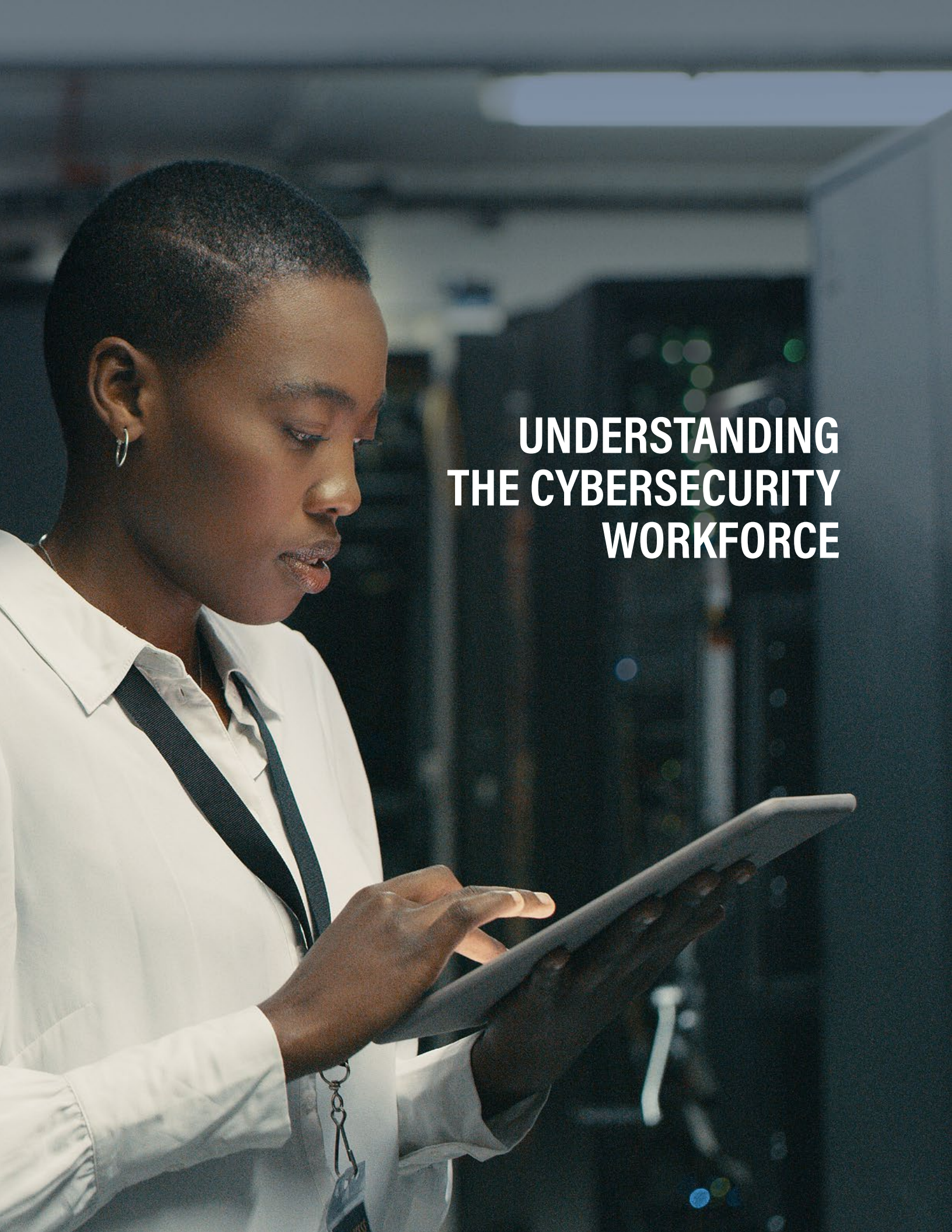
Work Conditions

With the cybersecurity field experiencing a substantial talent shortage amid rapid growth in cyber crime, it is little wonder that cybersecurity is a field with substantial levels of stress and burnout. Per a 2022 study, over half (57%) of U.S. cybersecurity professionals reported that they had experienced increased stress from staff turnover in the last six months and one in five were considering leaving their jobs.[46] An earlier American study from 2021 found that half (51%) of cybersecurity professionals had experienced "extreme stress or burnout," and two-thirds (65%) had considered leaving their job because of stress.[47] Some interviewees from previous ICTC studies have attested to a sort of "vicious circle" in cybersecurity recruitment; talent shortages help drive up salaries but also result in high levels of stress and burnout, which blemish the image of the profession and thus help reinforce the original talent shortage.

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

[46] "Cybersecurity staff turnover and burnout: How worried should organizations be?," Helpnet Security, 2022: https://www.helpnetsecurity.com/2022/01/31/cybersecurity-teams-retention-issues/

[47] Pollard, J. "Predictions 2022: Cybersecurity, Risk, And Privacy," Forrester, 2021: https://www.forrester.com/report/predictions-2022-cybersecurity-risk-and-privacy/RES176406



UNDERSTANDING THE CYBERSECURITY WORKFORCE

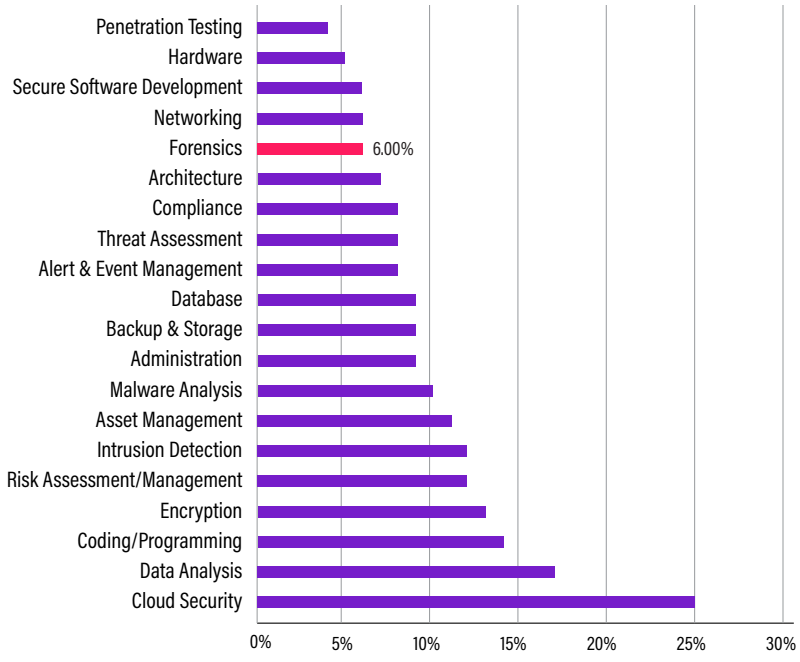
Cybersecurity professionals vary widely in their responsibilities, educational backgrounds, skills, experience levels, and certifications. Finding the right mix of qualifications can be difficult. In a 2018 study by Deloitte on the cybersecurity ecosystem in Canada, the vast majority (76%) of Chief Information Security Officers noted that finding the right mix of technical, analytical, and soft skills was a significant challenge when recruiting cybersecurity staff.[48] At the same time, cybersecurity professionals are highly skilled and certified. In a 2019 study that sampled over 3,000 cybersecurity professionals worldwide, the average respondent had four years of experience in their current position, five years of experience in a cybersecurity role, six years of experience at their current organization, nine years of experience in IT roles, four security organization certifications, and three security organization memberships.[49]

Technical Skills and Soft Skills

Job titles and descriptions in the cybersecurity ecosystem are not always easy to categorize due to the idiosyncratic needs of different organizations, as well as general unfamiliarity that many have with terminology related to the field. Employers frequently write very broad job descriptions to attract a diverse array of applicants and, consequently, job descriptions will often resemble organizational "wish lists."[50]

MOST IMPORTANT TECHNICAL SKILLS - 2021 SURVEY

Figure 9: Cybersecurity roles Technical Skill Importance Comparison 2021 Survey[51]



[48] Ibid.

[49] "Strategies for Building and Growing Strong Cybersecurity Teams," 2019, ISC2, https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

[50] Herron, C., et al., "Searching for Hidden Talent," June 2020, ICTC, https://medium.com/digitalthinktankictc/searching-for-hidden-talent-2fa7b44becaa?source=

[51] "The Cybersecurity Career Pursuers Study: Build Resilient Cybersecurity Teams" *(ISC)²*, 2021, https://www.isc2.org/Research/CareerPursuers?utm_source=isc2&utm_medium=pressrelease&utm_campaign=GBL-careerpursuersreport&utm_content=report

The precise hard skills required for different types of cybersecurity professionals will vary depending on their level of experience, area of focus or specialization, and the employer's specific technology. Ensuring the security of a database, for example, demands a slightly different skill set than securing a web application. The following figure identifies top technical skills in cybersecurity.

Cybersecurity professionals also require soft skills to perform their jobs well. Some of these skills, such as problem solving and effective communication, can be learned in an educational context, while others are more suited to "on-the-job" learning. These skills often apply to many different types of roles. Examples of soft skills needed in cybersecurity include attention to detail, visualization, risk awareness, effective communication, problem solving,[52] logical reasoning,[53] adaptability, passion, curiosity, and teamwork.[54]

Training and Education for a Cybersecurity Career

Cybersecurity is a fast-evolving field that attracts self-motivated, ambitious professionals who enjoy learning new skills. It is also a field in which the education and career pathways are not clear cut; a 2019 study by (ISC)^2 found that nearly half of cybersecurity professionals did not begin their career intending to pursue cybersecurity.[55]

The pathways into the cybersecurity field can be broadly divided into three categories: certification, college diploma or graduate certificates, and bachelor's or graduate degrees.[56] These paths can differ depending on stage of career and intended specialization in cybersecurity roles.

TRADITIONAL POST-SECONDARY PATHWAYS

The Canadian Institute for Cybersecurity, based at the University of New Brunswick, offers classes in cybersecurity and advanced certifications.[57] Numerous Canadian universities and post-secondary institutions provide instruction in cybersecurity, although bachelor's and master's programs focused on cybersecurity are rare.[58]

---

[52] Kassner, M., "Don't forget to evaluate soft skills when hiring for cybersecurity positions," TechRepublic, 2021: https://www.techrepublic.com/article/dont-forget-to-evaluate-soft-skills-when-hiring-for-cybersecurity-positions/

[53] Fund. B., "16 Soft Skills You Need to Succeed in Cyber Security," Flatiron School, 2021: https://flatironschool.com/blog/soft-skills-cyber-security/

[54] "Soft Skills in Cybersecurity: Communication and Training Are Key," Maryville University, accessed 2022: https://online.maryville.edu/online-masters-degrees/cyber-security/careers/skills-in-cybersecurity/

[55] Ibid.

[56] "Cyber Security Career Pathways," Canadian Centre for Cyber Security, 2022: https://cyber.gc.ca/en/guidance/career-pathways

[57] "Canadian Institute for Cybersecurity" *University of New Brunswick*, 2021: https://www.unb.ca/cic/

[58] "Forensic Investigation (Digital Forensics and Cybersecurity Option)" *British Columbia Institute of Technology*, 2021: https://www.bcit.ca/programs/forensic-investigation-digital-forensics-and-cybersecurity-option-advanced-certificate-part-time-526jadcert/

EMERGING EDUCATION PATHWAYS

Coding bootcamps, Massive Open Online Courses (MOOCs), and other forms of emerging education provide an alternative or complementary approach to traditional education in universities or colleges. They can also be easier to scale than traditional programs, offering a more accessible form of technical training to some students. However, while coding bootcamps and MOOCs have been highly disruptive and successful in areas such as software development, uptake in the cybersecurity field has been comparatively low.

No formal study has focused on this discrepancy for a couple of reasons. First, cybersecurity is a small field with a high degree of specialization, which makes it difficult to design a generalist curriculum that would transition quickly to the workplace. Second, the fact that cybersecurity roles are so high paying and have such low unemployment may paradoxically hinder the growth of education opportunities: experts in the field may opt for high-wage cybersecurity jobs rather than invest their time in contributing to educational programs.

CERTIFICATIONS

Certifications are a major feature in the cybersecurity ecosystem. A 2019 study found that 59% of cybersecurity professionals either planned to obtain at least one certification that year or were already pursuing one.[59] Cybersecurity-specific training can include training obtained from former work experience in cybersecurity, or through a cybersecurity-specific credential such as a professional certificate. Microsoft Solutions Architect (MCSA) Certifications allow cybersecurity employees to customize their skill set while providing a reliable framework for communicating skills across national and industry borders. However, while helpful for the cybersecurity industry, certifications can be expensive, and the price of many of the certifications has been criticized as deterring potential entrants to the field. A 2019 (ISC)^2 study found that only 37% of cybersecurity professionals had their certifications paid for completely by their organization, while 35% were entirely responsible for paying for their own certification.[60]

[59] "Strategies for Building and Growing Strong Cybersecurity Teams," 2019, ISC2, https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

[60] "Strategies for Building and Growing Strong Cybersecurity Teams," 2019, ISC2, https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

Examples of relevant certifications in the cybersecurity field include:

Cyber Security Fundamentals

GIAC Security Essentials

CompTIA Security+

CompTIA Advanced Security Practitioner

Certified Information Systems Security Professional

Certified Information Security Manager

Certified in Risk and Information Systems Control

Systems Security Certified Practitioner

Certified Chief Information Security Officer

CyberSec First Responder

Certified Secure Computer User

Certified Secure Software Lifecycle Professional

Certified Wireless Security Professional

CertNexus CyberSAFE®

Certified Ethical Hacker

Certified Information Systems Auditor

Certified Cloud Security Professional

Cyber Security Nexus Practitioner

Offensive Security Certified Professional

GIAC Information Security Professional

GIAC Security Leadership Certification

GIAC Information Security Fundamentals

GIAC Certified Perimeter Protection Analyst

GIAC Certified Intrusion Analyst

GIAC Certified Incident Handler

GIAC Certified UNIX Security Administrator

GIAC Certified Windows Security Administrator

GIAC Certified Enterprise Defender

GIAC Certified Web Application Penetration Tester

GIAC Assessing Wireless Networks

Global Industrial Cybersecurity Professional

GIAC Critical Controls Certification

GIAC Penetration Tester

GIAC Security Expert[61]

[61] "Cyber Security Career Pathways," Canadian Centre for Cyber Security, 2022: https://cyber.gc.ca/en/guidance/career-pathways

The in-house Student Survey portion of this study builds on findings from previous studies. On a certification-by-certification basis, there was no one certification that more than 15% of students were planning to pursue, presumably because of the wide variety of certifications available. In addition, close to a quarter of respondents said they were not pursuing certifications because they were "too expensive." Close to a third said that they were not pursuing certificates because the prerequisites for achieving them were too demanding.

MICRO-CREDENTIALS

In addition to traditional certifications for cybersecurity skills, there are also more micro-credential options. Micro-credentials are certifications of assessed competencies that are "additional, alternate, complementary to, or a component of a formal qualification."[62]

Examples of cybersecurity micro-credentials include:

- Cybersecurity – Intrusion Detection[63]
- Cyber Security Operations (Cisco)[64]
- Digital Forensics[65]
- General Cyber-Security Micro-redential[66]
- Cybersecurity – Offensive[67]

Salary

High salaries are a recurring theme in both previous ICTC research and external studies. A third of Canadian CISOs felt that cybersecurity compensation packages had been inflated by demand,[68] and when extended to North America, this impression is held by 41% of respondents.[69] In Canada, 27% of companies polled by the Canadian Internet Registration Authority (CIRA) reported that they lacked the resources to employ a cybersecurity professional, and businesses that were hiring external cybersecurity consultants were devoting 19% of their total IT budgets on average to cybersecurity.[70]

[62] "National Framework for Microcredentials," Colleges and Institutes Canada, 2022: https://www.collegesinstitutes.ca/policyfocus/micro-credentials/

[63] "ACS Microcredentials," Australian Computer Society (ACS), 2022: "Cyber Security Operations (Cisco) https://www.acs.org.au/professionalrecognition/microcredentials-home.html

[64] "Cyber Security Operations (Cisco)," Futurelearn, 2022: https://www.futurelearn.com/microcredentials/cybersecurity-operations

[65] Combs, V., "Micro-credentials are a quicker and cheaper way to improve your resume," TechRepublic, 2020: https://www.techrepublic.com/article/micro-credentials-are-a-quicker-and-cheaper-way-to-improve-your-resume/

[66] "Cyber-Security Micro-credential," BMCC, 2022: https://www.bmcc.cuny.edu/cyber-security-micro-credential/

[67] "Microcredential Cybersecurity Offensive," Sheridan College, 2022: https://caps.sheridancollege.ca/products/cybersecurity-offensive.aspx

[68] Deloitte and the Toronto Financial Services Alliance, The changing faces of cybersecurity: Closing the cyber risk gap, 2018, pp. 12-14

[69] 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.

[70] "Fall 2018 Cybersecurity Survey Report," CIRA, 2018, p. 10.

Cybersecurity salaries are influenced by the same factors as most other jobs: seniority, experience, formal education. The (ISC)[2] Cybersecurity Workforce Study in 2019 found that certified cybersecurity employees in North America had an average salary of $93,000 USD, while uncertified made only $76,500.[71] However, it was not possible to determine whether this effect was causal, as certification might have been correlated with factors such as experience.

Salaries can also vary widely according to role. Based on data from Hays Canada, the lowest salaries are in Administrative, Analysis, or Consultant roles. Salaries in those roles range from under $50,000 CAD to just under $100,000. Engineering and Architect roles range from $80,000 to $160,000. The highest salaries in cybersecurity go to executives, such as Chief Information Security Officers, and VPs or Directors of Information Security. Salaries at this level start at six-figures and can exceed $200,000.

ROLE	AVERAGE SALARY RANGE
Chief Information Security Officer (CISO)	180,000 to 230,000
VP, Information Security	130,000 to 200,000
Enterprise Security Architect	130,000 to 160,000
Director, Information Security	100,000 to 150,000
Network Security Architect	105,000 to 135,000
Cloud Security Architect	90,000 to 130,000
Application Security Engineer	80,000 to 110,000
Digital Forensics Analyst	65,000 TO 95,000
Senior Penetration Tester	60,000 TO 90,000
Data Security Consultant	60,000 TO 90,000
Malware Analyst	60,000 TO 90,000
Security Administrator	45,000 TO 75,000

Figure 10: National Salary Range for Cybersecurity Roles. Source: Hays Canada.[72]

[71] "Strategies for Building and Growing Strong Cybersecurity Teams," 2019, ISC2, https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

[72] "Salaries are expressed in Canadian dollars and do not reflect any benefits packages, bonuses, or any other arrangements between employers and candidates." Ibid.

Looking at cybersecurity-related NOC codes sacrifices precision but allows for access to more data. While there are some discrepancies based on whether one uses job posting data from labour market data company EMSI (which has considerably fewer observations) or Labour Force Survey Data from Statistics Canada, all data broadly harmonizes and shows that across Canada, roles corresponding with Computer and Information Systems Managers (NOC 0213) are paid the most, while Information Systems Testing Technicians (NOC 2283) and Computer Network Technicians (2281) are paid the least.

MEDIAN SALARIES IN CYBERSECURITY-RELATED NOC CODES, DATA FROM EMSI AND STATISTICS CANADA

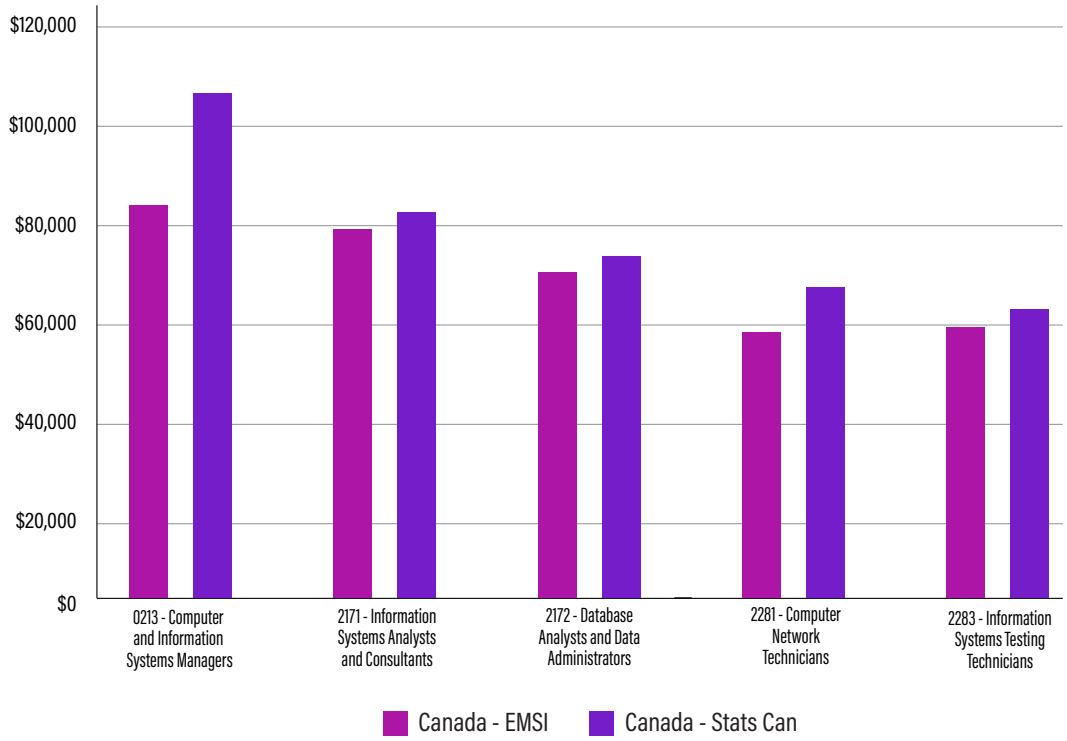


Figure 11: Median salary (base pay) by data source and region for ICT National Occupation Codes related to Cybersecurity. ICTC, Analysis, EMSI and Statistics Canada Data, 2020.

EQUITY, DIVERSITY, AND INCLUSION IN CYBERSECURITY

EQUITY, DIVERSITY, AND INCLUSION IN CYBERSECURITY

The 2021 (ISC)² Cybersecurity Workforce Study estimated that there was a shortage of 25,000 cybersecurity professionals in Canada.[73] However, this figure may to be substantially higher given the attested presence of a substantial hidden job market in cybersecurity.[74]

A lack of diversity among cybersecurity talent pools may prolong the talent shortage. For example, Canadian CISOs have noted that the underrepresentation of women contributes to the low number of experienced cybersecurity professionals.[75] A 2021 report by (ISC)² also found that people of colour and women were underrepresented in cybersecurity. Canadian research found that only 20% of cybersecurity workers in Canada identify as women and only 25% identify as Black, Indigenous, or as a Person of Colour (BIPOC).[76]

Gender disparities occur at all levels of experience. ICTC's in-house student survey found that women drop out of cybersecurity at a 50% higher rate than men. While 30% of male respondents to the survey reported that they had left the field, over 50% of women did so. On the other end of the experience spectrum, research on the North American cybersecurity industry found that men are four times more likely to hold executive positions and are nine times more likely to hold management positions.[77] Globally, in 2016, women in cybersecurity earned less than men at every level of employment,[78] even though women typically enter cybersecurity with higher levels of education than men.[79] Women in cybersecurity are aware of the difficulties they face. 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 (versus 79% of male respondents).[80]

There is some evidence that diversity is being taken more seriously as an objective in the cybersecurity field. The Accelerated Cybersecurity Training Program (ACTP) at Ryerson University is designed to help individuals from diverse backgrounds that include education, experiences, cultural differences, and age (in addition to gender, race, and sexual orientation). To bolster diversity, the program targets women, mid-career individuals, career-changers, and newcomers to Canada that can bring new ideas and viewpoints to cybersecurity.[81]

---

[73] "A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)² Cybersecurity Workforce Study, 2021," (ISC)², 2021, https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[74] Hasham, R., "Fostering innovation in cybersecurity through diversity and inclusion," Future Skills Centre, 2022: https://fsc-ccf.ca/fostering-innovation-in-cybersecurity-edi/

[75] Deloitte and the Toronto Financial Services Alliance, The changing faces of cybersecurity: Closing the cyber risk gap, 2018, pp. 12-14.

[76] https://fsc-ccf.ca/fostering-innovation-in-cybersecurity-edi/

[77] "The 2017 Global Information Security Workforce Study: Women in Cybersecurity," Frost & Sullivan, 2017: https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2019/01/women-cybersecurity-11-percent.pdf

[78] 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.

[79] Ibid. p. 10.

[80] "State of cybersecurity 2019: Current trends in workforce development," ISACA, 2019, p. 14.

[81] Hasham, R., "Fostering innovation in cybersecurity through diversity and inclusion," Future Skills Centre, 2022: https://fsc-ccf.ca/fostering-innovation-in-cybersecurity-edi/

One of the issues identified related to diversity is a lack of mentorship and opportunities to develop relevant skills in traditional university programs.[82] If there are significant prerequisites (real or perceived) of first completing an engineering or computer science degree, individuals who face barriers to achieving traditional university degrees are heavily discouraged from pursuing further education through cybersecurity courses.[83]

The ICTC Student Cybersecurity pathway survey shows mixed perceptions of diversity barriers. A plurality of respondents neither agreed nor disagreed on diversity barriers in the field. While more students who completely disagreed than completely agreed that there were barriers in the field, more students somewhat agreed on the presence of diversity barriers than somewhat disagreed.

STUDENT CYBERSECURITY CAREER PERCEPTIONS

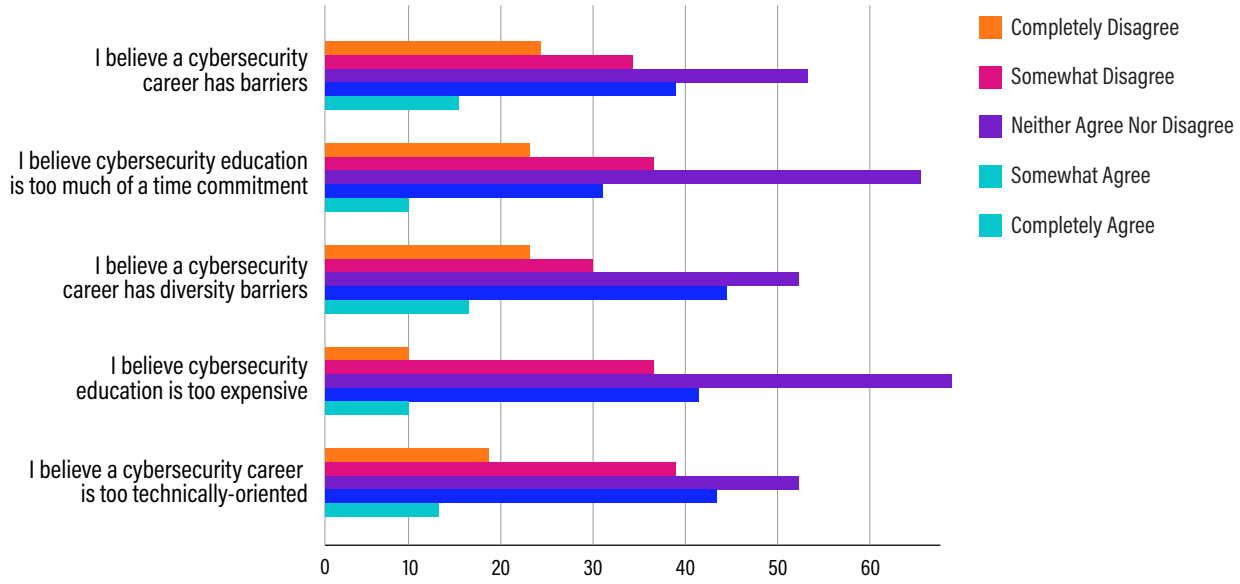
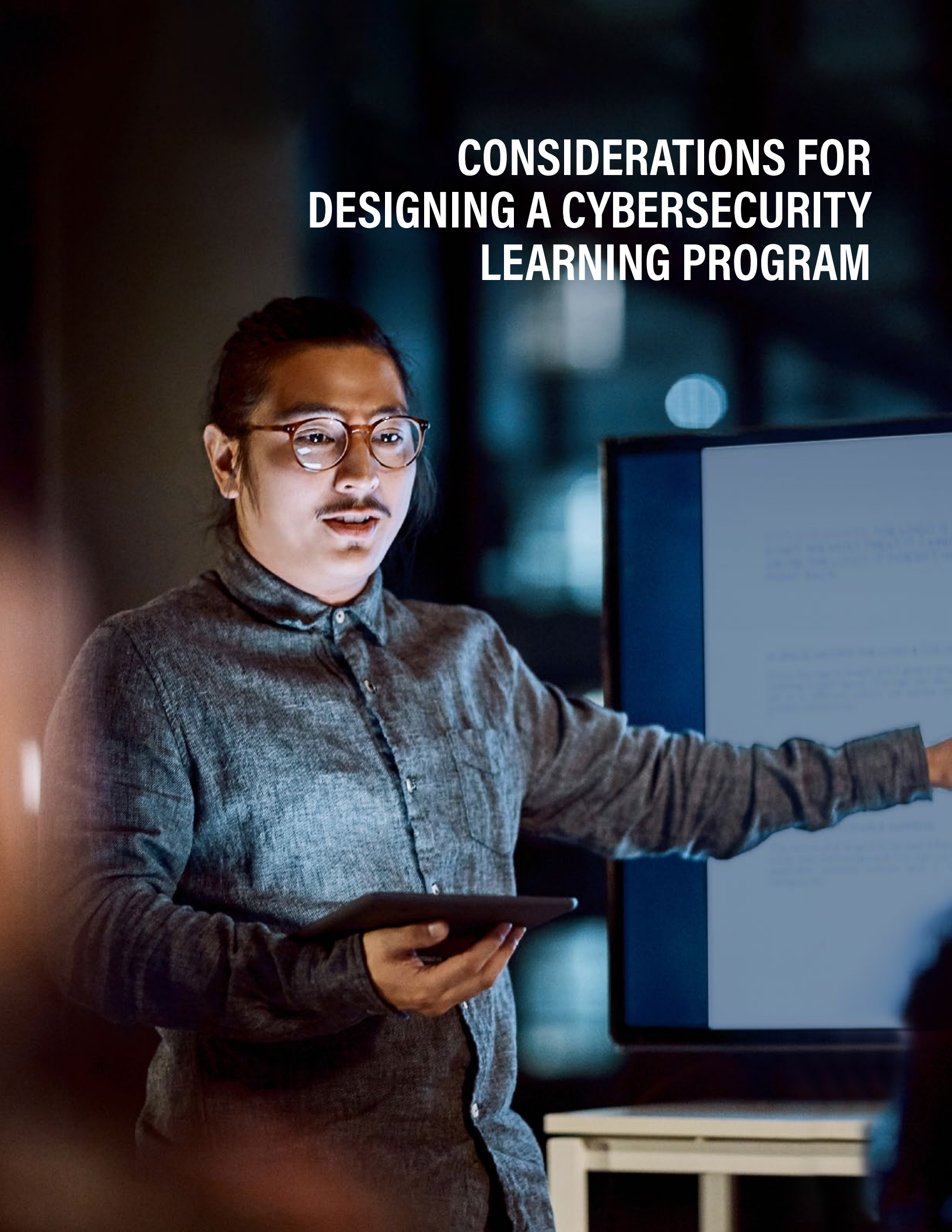


Figure 12: Student perceptions of barriers to a career in Cybersecurity. ICTC Cybersecurity Student Survey, 2022.

[82] Palios, S., "To Become More Diverse, Cybersecurity Experts say Industry Needs More Mentors and Problem Solvers," BetaKit, 2021: https://betakit.com/to-become-more-diverse-cybersecurity-experts-say-industry-needs-more-mentors-and-problem-solvers/

[83] Palios, S., "To Become More Diverse, Cybersecurity Experts say Industry Needs More Mentors and Problem Solvers," BetaKit, 2021: https://betakit.com/to-become-more-diverse-cybersecurity-experts-say-industry-needs-more-mentors-and-problem-solvers/

CONSIDERATIONS FOR DESIGNING A CYBERSECURITY LEARNING PROGRAM



Those capable of succeeding in the cybersecurity sector are "elite" in terms of both skills and temperament and would likely be highly capable of succeeding in other well-compensated technical fields such as software engineering or data science. Ensuring a robust talent pipeline, then, does not only consist of providing training programs in cybersecurity that serve the needs of industry; it also consists of attracting highly skilled talent to the cybersecurity field, retaining their interest, and allowing them to develop a strong sense of connection to the cybersecurity field.

Given the large role that student decisions and perceptions will play in the growth of the cybersecurity field, it is essential for ICTC to analyze student experiences in cybersecurity to understand what draws them to the field, what skills they hold, and what challenges they face. The following section details findings from this recent survey ICTC conducted among students pursuing cybersecurity qualifications in Canada.

The purpose of this research is to design a program to supplement the cybersecurity pipeline. Designing such a program should consider the needs of both students and employers when designing a curriculum.

There is a substantial value proposition in a work-integrated learning (WIL) program. A majority of former cybersecurity students said that their decision might have been changed by providing WIL or micro-credentials. Fewer (less than 10%) were sure that their decision would not have been affected by these. The remainder were unsure.

Top Roles

According to the student survey completed for this research, the most frequently sought jobs by students are cybersecurity engineer, cybersecurity analyst, and network analyst. The roles generating the least interest are intrusion detection, incident response, and red and blue team specialist roles.

CYBERSECURITY JOBS INTERESTED IN

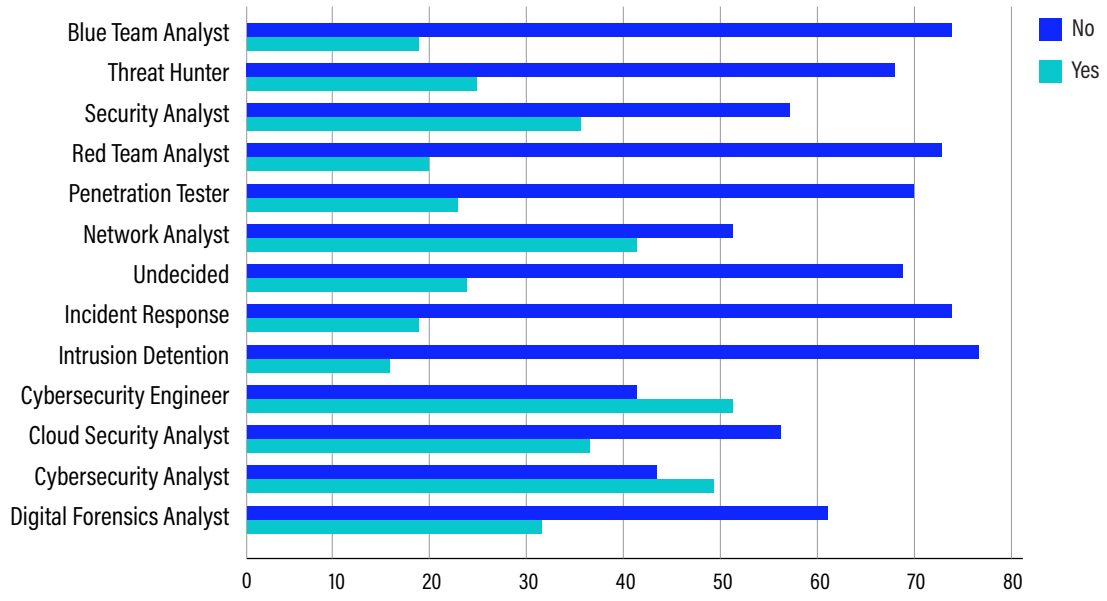


Figure 13: Cybersecurity job types of interest to students. ICTC Cybersecurity Student Survey, 2022.

The top roles that employers are looking for are cybersecurity analysts, cybersecurity engineer, security analyst. The roles of least interest are threat hunter, digital forensics analyst, and red and blue team analysts.

All in all, the top roles sought by students line up well with the top roles sought by employers. This is a fortunate finding indeed for the purposes of designing a program that both appeals to students and satisfies the needs of industry.

CYBERSECURITY ROLES IN HIGH DEMAND

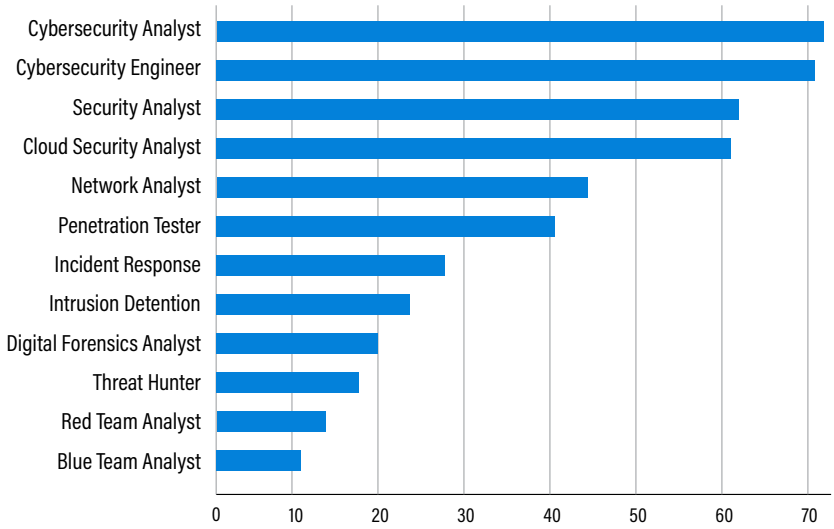


Figure 14: Cybersecurity jobs in high demand. ICTC Cybersecurity Employer Survey, 2022.

Technical Skills

The student survey found that students rated their skills in Operating Systems, internet protocols, and networks the highest. In these categories, a plurality rated themselves as "somewhat comfortable." For cloud security, digital forensics, and incident response, a plurality of respondents rated their comfort as "neutral." But students in general seemed somewhat hesitant in their skills—far fewer rated themselves as "very comfortable."

STUDENT COMFORT WITH TECH SKILLS

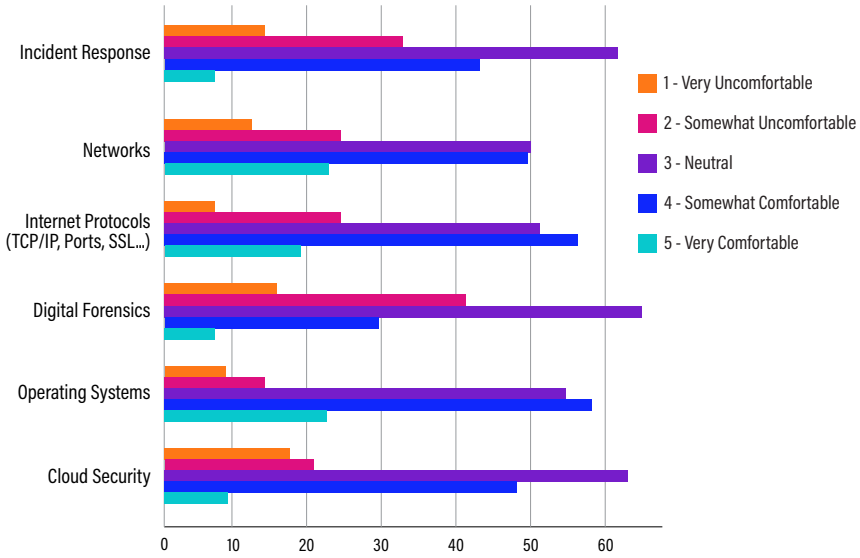


Figure 15: Cybersecurity student comfort levels with various technical skills. ICTC Cybersecurity Student Survey, 2022.

In the Employer Survey, cryptography is ranked as relatively less crucial than other technical skills. Security operations, network security, and cloud security are identified as the most essential for cybersecurity roles. Notably network security has the highest vote for "essential to the role" and "a requirement for hiring."

The Employer Survey also invited participants to identify the skills they believe were most lacking among cybersecurity program graduates. The most common response was cloud security, which is one of the highly essential technical skills, as seen in the previous table. For cloud security, more employers indicated that this was a necessary requirement for hiring rather than a capability that can be developed on the job. As such, it is important for education institutions and students to ensure that they can learn these cloud security skills before they enter the workforce. Other important skill gaps are incident response and digital forensics, although employers report considerably less demand for these skills overall than cloud security.

IMPORTANCE OF TECH SKILLS

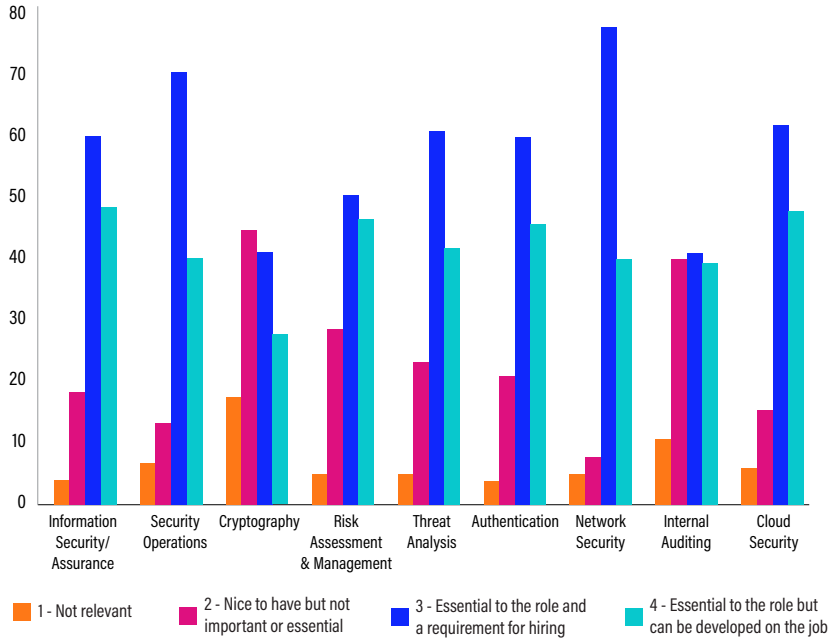


Figure 16: Importance of various technical skills for cybersecurity employers. ICTC Cybersecurity Employer Survey, 2022.

CYBERSECURITY SKILLS GRADUATES MOST LACKING

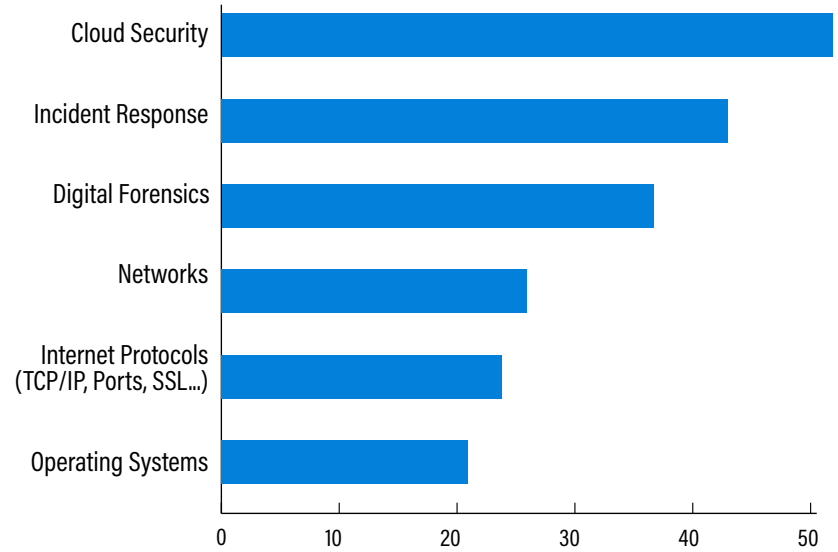


Figure 17: Most lacking skill areas among cybersecurity program graduates, according to cybersecurity employers. ICTC Cybersecurity Employer Survey, 2022.

Soft Skills

The student survey found that cybersecurity students are quite confident in their "general" or "soft" skills. For eight of the nine skill areas profiled, a plurality of respondents indicated that they are very comfortable in their abilities. The responses were skewed toward the positive side. For all nine skill areas, only a very small percentage (less than 10%) indicated they are either very uncomfortable or somewhat uncomfortable. The skill areas with the highest levels of confidences are "Reading and Writing," "Communication," and "Adaptability."

"Work under pressure" has the lowest levels of self-reported confidence, and the only skill area in which a plurality reported they were only "Somewhat Comfortable." As such, future programs may wish to add further opportunities for students to work under high-pressure environments (time-limited assignments, for example). However, further research may also need to investigate if these self-assessed levels of confidence correspond with evaluations by cybersecurity employers.

STUDENT COMPORT WITH SOFT SKILLS

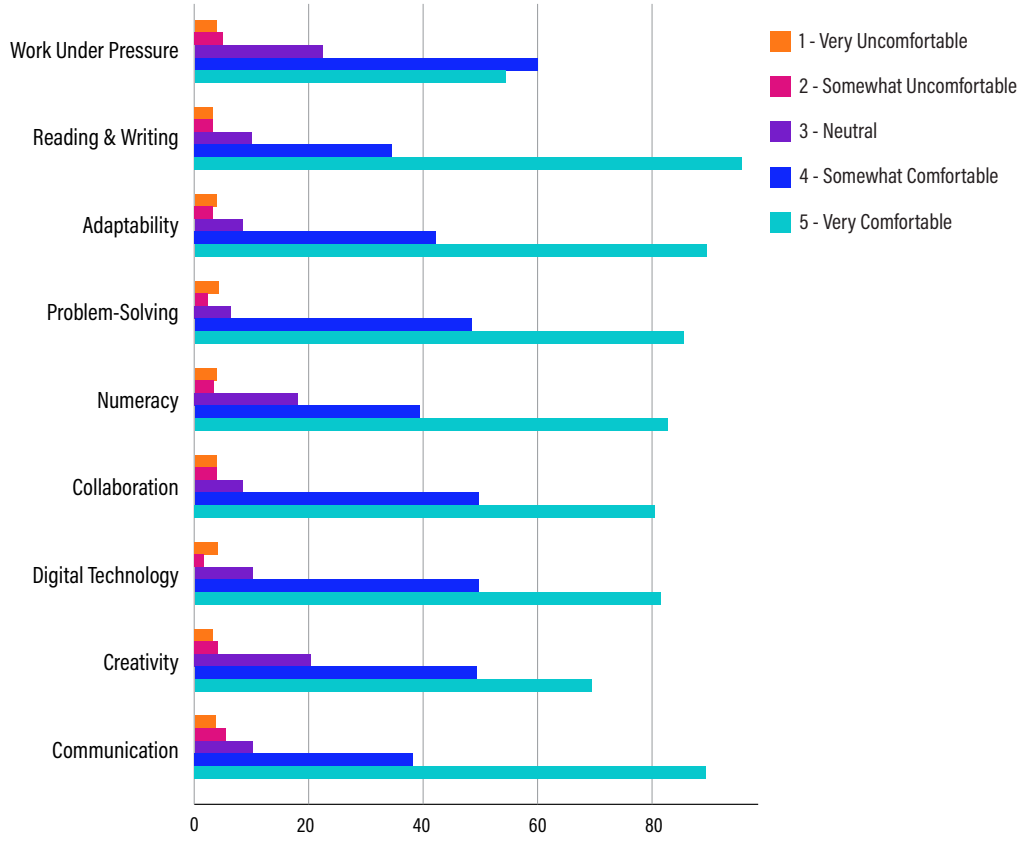


Figure 18: Self-reported comfort level with various "soft skills" among cybersecurity program participants. ICTC Cybersecurity Student Survey, 2022.

Employers view most soft skills as "essential to the role and a requirement for hiring" (especially dependability) or "essential to the role but can be developed on the job." Compared to other soft skills, leadership and creativity are different. Leadership is mostly considered as "nice to have" but not important or essential; it received the highest "not relevant" vote of all the soft skills as well. Creativity gets very few "not relevant" responses, but it has a similar share of responses for "nice to have," "essential and a requirement for hiring," and "essential but can be developed on the job." The highly essential skills are critical/analytical thinking and problem solving and reasoning.

IMPORTANCE OF SOFT SKILLS

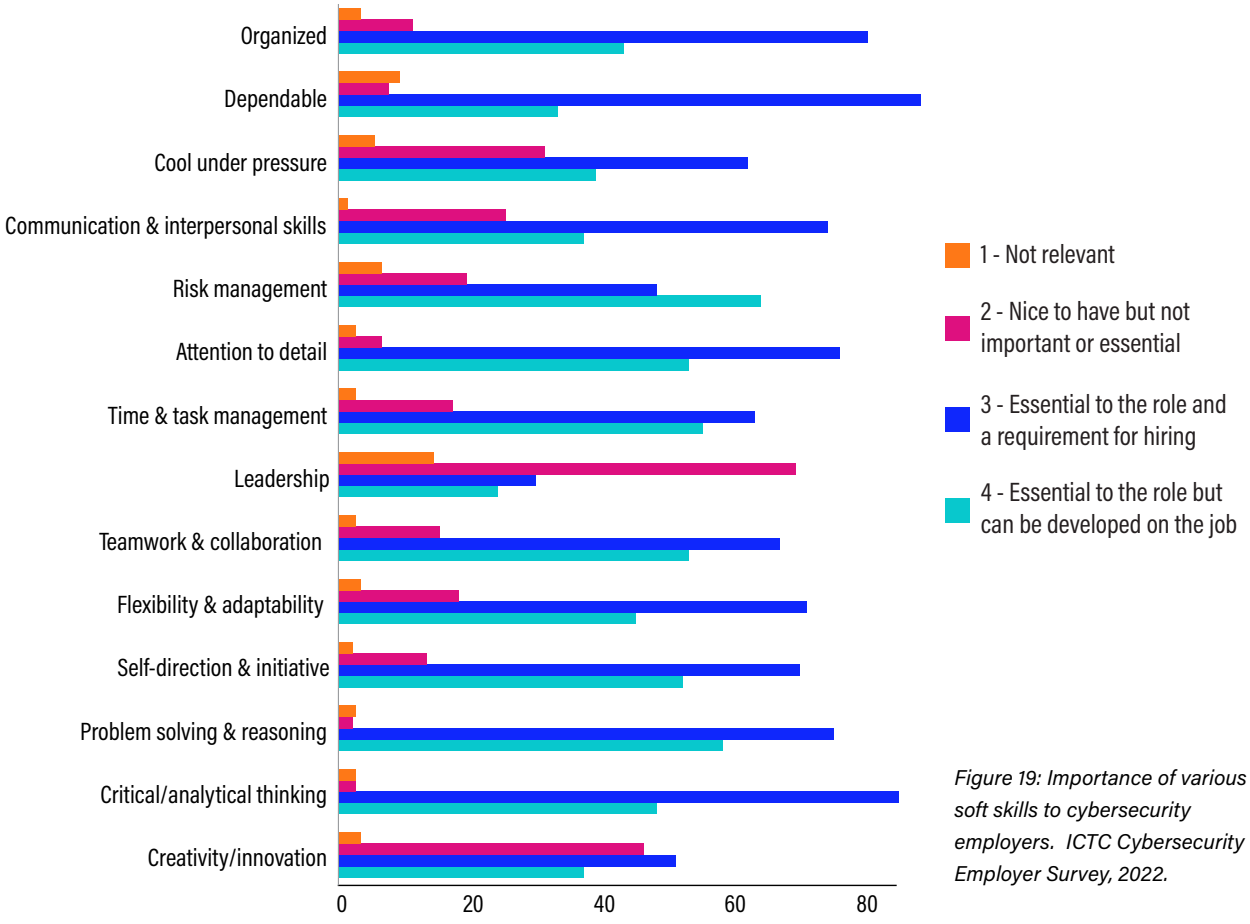


Figure 19: Importance of various soft skills to cybersecurity employers. ICTC Cybersecurity Employer Survey, 2022.

Frameworks

The following frameworks were also ranked in the Employer Survey, which found that some are more relevant than others. Among these cybersecurity frameworks, NIST Cybersecurity Framework receives the highest vote as "very important" and "mandatory." More responses consider it as "very important" than "somewhat important." Other frameworks have more votes on "somewhat important" than "very important."

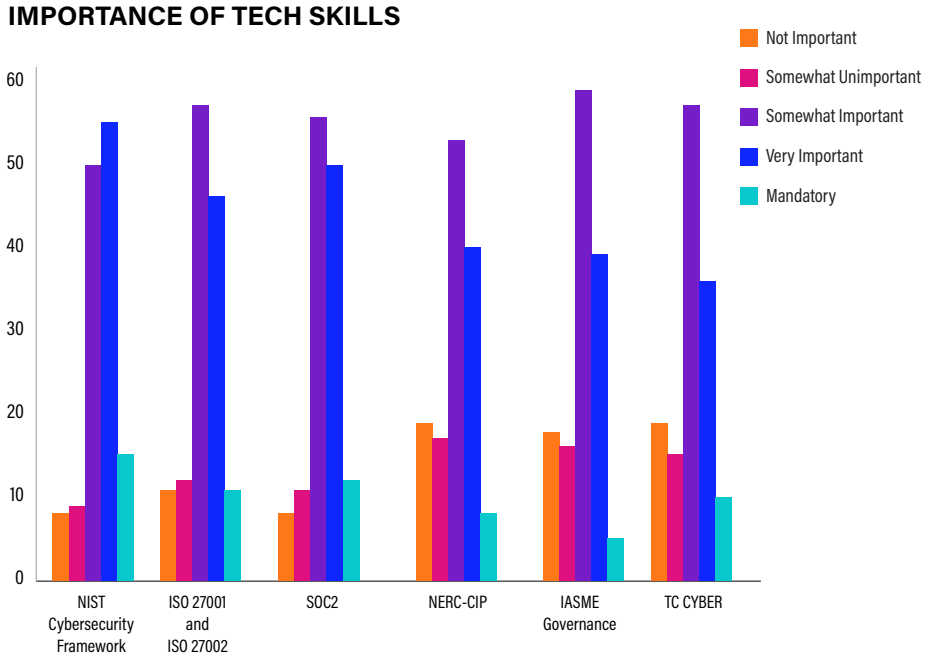


Figure 20: Importance of various cybersecurity frameworks to cybersecurity employers. ICTC Cybersecurity Employer Survey, 2022.

Certifications

Industry certification is generally viewed as less important than the graduates' knowledge of cybersecurity frameworks. CISSP (Certified Information Systems Security Professional) has the most aggregated votes for somewhat "important," "very important," and "mandatory."

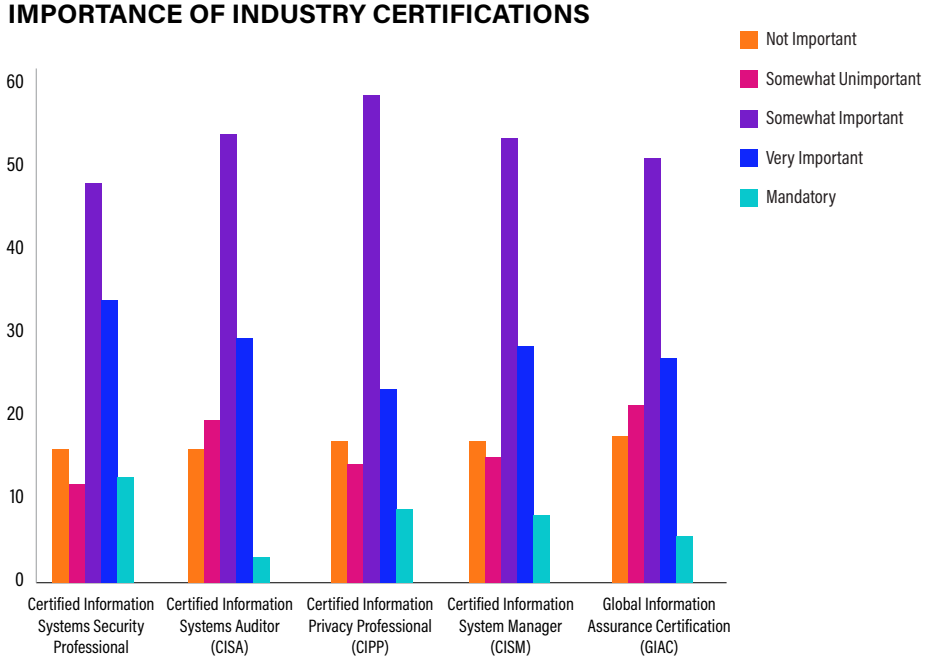


Figure 21: Importance of various cybersecurity certifications to cybersecurity employers. ICTC Cybersecurity Employer Survey, 2022.

Applications Skills

An effective workforce preparation program will also consider the application process specifically. ICTC's in-house Employer Survey found that companies look for talent by a variety of methods ranging from job boards to word of mouth. Organizations identified the job interview as the most important aspect of candidates' application. The applicant's CV or resume was considered the second most important consideration when hiring. Note that assignment/tests can be considered as part of the technical interview. Unsurprisingly, referrals, word of mouth, or industry connections was also commonly identified as a hiring consideration. In the cybersecurity field, cover letters were identified as less crucial when reviewing potential job candidates.

As such, Canadian cybersecurity educators should ensure that applicants are well-prepared to make a positive impression with their CV and interviewing skills.

IMPORTANCE OF ASPECTS OF CANDIDATE'S APPLICATION

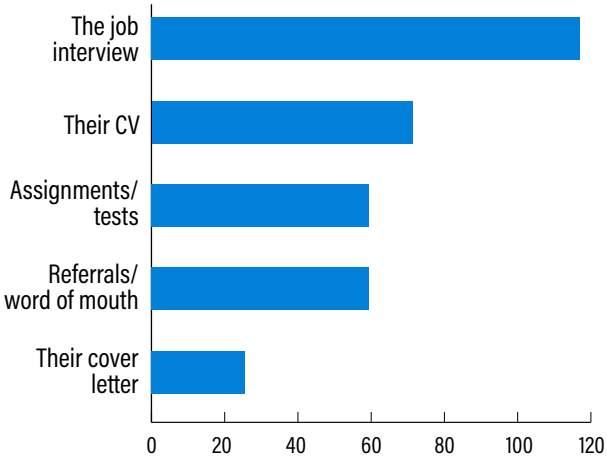


Figure 22: Importance of various aspects of candidates' applications to cybersecurity employers. ICTC Cybersecurity Employer Survey, 2022.

Addressing Barriers and Attrition

A high degree of attrition in cybersecurity programs is a major challenge facing the cybersecurity industry, as it delays the closure of the talent gap. Attrition is also gender-imbalanced, meaning that even if more women become interested in the field, ultimate gains in the workforce may be limited; ICTC's student survey found that over 50% of women who began a career in cybersecurity dropped out of the field, compared to 30% of men.

When both male and female former students were asked why they had left their cybersecurity education, the three top reasons were better opportunities elsewhere, finding cybersecurity too technical, or experiencing a loss of interest in the field. Some interesting cohort effects were seen among students with different backgrounds. Engineers, for example, tended to leave the field for what they saw as better opportunities elsewhere. Engineers and business majors were more likely to find the field too technical. Computer science students were most likely to report that the field was too stressful or they lost interest.

For the students who abandoned cybersecurity as a career path, the majority of survey respondents indicated that the availability of work integrated learning programs and/or micro-credential offerings would have influenced their decision to self select out of cybersecurity.

The student survey found that high levels of stress, time commitment, and technical requirements were the three top factors negatively impacting student enjoyment of cybersecurity learning programs. By contrast, student interest was minimally affected by diversity and culture considerations or affordability.

However, the ability of a cybersecurity learning program to allay these concerns in the long term may be limited. Cybersecurity is a field that demands high time commitment and high technical certification, and frequently subjects its workers to high stress. While designing a highly flexible cybersecurity program may encourage more people to study cybersecurity, as well as provide an alternative for those uninspired by a rigorous university or college-based approach, the long-term impacts of such a program might be less beneficial than expected. Such a program might simply delay the exit of unsuitable workers, rather than eliminating it.

Assessing the Expectation Gap Between Post-Secondary Institutions and Employers

Although post-secondary institutions (PSIs) were not included in the surveys due to limited time and project resources, there were clear differences between student self-assessments related to technical skills and soft skills, and employer assessments and expectations. This is of particular importance for those skills employers have identified as "must have pre-hiring" skills versus those that can be developed on the job.

A lack of communication between PSIs and cybersecurity job employers has been identified by the ICTC National Advisory Committee on Cybersecurity Training (INACCT) and is reflected in the differences between student and employer survey responses. Future research could include more in-depth understanding of how essential pre-hire skills, both technical and soft, can be developed. This is acutely important for students who may not be able to develop and accurately assess these pre-hire skills before attempting entry into the cybersecurity workforce.

CONCLUSION

Existing research has noted the significance of the cybersecurity field in Canada and abroad. Given the increasing digitalization of work, which has been accelerated by the growth of remote work due to COVID-19, cybersecurity is a priority for both the public and private sector. There are multiple pathways into cybersecurity roles such as directly from a relevant college or university program, or as part of a mid-career transition through upskilling. It is also worth considering the role of work integrated learning (WIL) programs and micro-credentials as alternative routes to upgrading capabilities in this area. However, there are challenges to recruitment and retention for these in-demand cybersecurity roles. The scope of challenges has increased, and it remains a demanding industry. Research indicates that there are high levels of burnout with many employees considering leaving in the next year. As seen in other fields, the "Great Resignation" and the changing balance of labour supply and labour demand give greater leverage to jobseekers and pose challenges for company recruitment.

ICTC's ongoing research and recent survey provides new data on a variety of different dimensions for cybersecurity employers, such as the relative ranking of importance of industry certifications, frameworks, key hiring considerations, and employee skill requirements. This is supplemented with survey data that focuses on the perspectives of cybersecurity students (such as their impressions of the negative aspects of field or their self-assessment of skill level) to better understand the future supply pipeline for cybersecurity. Ultimately, this data can be used to compare the needs and expectations of both employees and employers, and address the talent needs of the cybersecurity field in Canada.

To validate and implement the findings of this report, it is recommended that INACCT and ICTC explore options to design and implement a pilot project, in partnership with a Canadian college(s) offering cybersecurity training, to address the key skill deficiencies (both hard/tech and soft skills) of graduating cybersecurity talent and include at least one micro-credential and a WIL program.

CYBERSECURITY TALENT PROJECT METHODOLOGY

The methodology of this cybersecurity talent project was comprised of a literature review and primary research consisting of an employer survey and a student survey.

The literature review was a meta study, consolidating current and relevant cybersecurity and WIL research, articles, existing cybersecurity skill frameworks, and sector employment trends. The literature review helped inform the design of the surveys.

The goal of the project is to create a research brief that will inform the design of a WIL-driven cybersecurity pilot project to address the most pressing issues in cybersecurity hiring of post-secondary institution graduates and validate/fine-tune the assumptions of the ICTC National Advisory Committee on Cybersecurity Training (INACCT).

Primary Research:

The primary research had two components, starting with an Employer Survey to better understand:

- How employers assess the necessary skills when hiring for cybersecurity roles
- What skill gaps are employers finding among post-secondary graduates looking for cybersecurity roles
- What understanding of security checks/ clearances is necessary for hiring cybersecurity roles

The final component of the primary research was a Post-Secondary Institution Student Survey. The survey targets students from:

- Tradition program sources of cybersecurity talent (computer science, networking, IT)
- Non-traditional program sources of cybersecurity talent (business, liberal arts)

The survey sought to understand:

- If students have self-selected to not pursue a career in cybersecurity
  - Why they left the cybersecurity career path
  - What the perceived barriers were
  - What course offerings (i.e., micro-credential, certification…) and/or career path mitigations might have changed their mind
- How the availability of WIL programs influences their career path choices
- How students self-assess their readiness for cybersecurity careers

APPENDIX

In-Demand Cybersecurity Skills (Taken from New Brunswick Labour Market Research and Analysis [LMRA] Study)[84]

As several key informants noted, job titles and descriptions in the cybersecurity ecosystem are not always easy to categorize, as employers will, with some regularity, write very broad job descriptions to attract a diverse array of applicants. It was also noted that industry representatives intentionally oversaturate the skills (both human and technical) requirements for postings because limited or narrow qualifications requirements often discourage suitable candidates. Skill sets are therefore both specific to particular roles and, frequently, cross-sectional and applicable across a wide array of job titles. The analysis below inverts skill sets from least to most specific, first examining the human and transferable skills emphasized by employers in two ways: through key informant interviews and job posting descriptions. The skill sets are roughly ranked using the order of importance assigned by respondents to ICTC'S New Brunswick Employer Survey. While skill sets 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 web scraping 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.

[84] From the report *Searching for Hidden Talent: Experience and Expertise in New Brunswick's Cybersecurity Community*, https://www.digitalthinktankictc.com/reports/searching-for-hidden-talent.

APPENDIX

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 skill sets 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 skill sets are reinforced across the board and useful in a number of applications, including Communications and Network Security; Security Engineering; Network Architecture, Security, Tools and 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.

SKILLS RANKED IN ORDER OF IMPORTANCE FROM ICTC'S NEW BRUNSWICK EMPLOYER SURVEY[85]	SKILLS DIRECTLY MENTIONED IN INTERVIEWS OR SPECIFIC TO QUALIFICATIONS MENTIONED IN INTERVIEWS	SKILLS SCRAPED FROM JOB POSTINGS IN NEW BRUNSWICK (AGGREGATED WHEN SIMILAR)
HUMAN AND TRANSFERRABLE SKILLS		
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

[85] *Respondents were asked: "When hiring cybersecurity personnel in New Brunswick, which of the following [human or technical] skill sets 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.*

APPENDIX

SKILLS RANKED IN ORDER OF IMPORTANCE FROM ICTC'S NEW BRUNSWICK EMPLOYER SURVEY[85]	SKILLS DIRECTLY MENTIONED IN INTERVIEWS OR SPECIFIC TO QUALIFICATIONS MENTIONED IN INTERVIEWS	SKILLS SCRAPED FROM JOB POSTINGS IN NEW BRUNSWICK (AGGREGATED WHEN SIMILAR)
3. Courtesy/Empathy	• Emotional Intelligence (Empathy) • Customer service skills	• Emotional intelligence • Situational awareness • Client and customer service
Leadership	• Leadership skills • Volunteer/Internship experience	• Leadership, managerial, supervisory skills
CYBERSECURITY-SPECIFIC TECHNICAL SKILLS		
Group one (highest-ranked in survey)		
• Network Security	• Security Engineering • Communications and Network Security	• Network Architecture, Security, Tools, & Protocols • Protection Concepts • Firewall Management
• Knowledge of Cloud Computing Security	• Communications and Network Security • Cloud Security	• Protection Concepts
Group two: (second-highest)		
• Systems and Network Engineering	• Security Engineering • Communications and Network Security • Identity and Access Management • Information Systems Operations	• Network Architecture, Security, Tools, & Protocols • Protection Concepts
• Integrating Technologies, Systems, and Services	• Security Engineering • Communications and network security • Identity and Access Management • Software development security	• Network Architecture, Security, Tools, & Protocols • Data Protection and Encryption
• Information Security & Knowledge of Best Practices for Systems Architecture	• Security Engineering • Communications and network security • Identity and Access Management	• Network Architecture, Security, Tools, & Protocols • Data Protection and Encryption • Protection Concepts • Automation (Configuration, Management, Security Systems) • SOC Processes and Concepts • Managing Enterprise-Level Security Systems

APPENDIX

SKILLS RANKED IN ORDER OF IMPORTANCE FROM ICTC'S NEW BRUNSWICK EMPLOYER SURVEY[85]	SKILLS DIRECTLY MENTIONED IN INTERVIEWS OR SPECIFIC TO QUALIFICATIONS MENTIONED IN INTERVIEWS	SKILLS SCRAPED FROM JOB POSTINGS IN NEW BRUNSWICK (AGGREGATED WHEN SIMILAR)
• Governance and Compliance	• Security Analysis • Risk Management • Asset Security • Security Operations • Auditing Information Systems • Information Systems Acquisitions • Management Responsibility • Information Security Governance • Risk Management	• Governance and Compliance • Protection Concepts • Risk Mitigation and Management • Security Metrics and Reporting
• Penetration and Vulnerability Testing	• Security Analysis • Communications and Network Security • Identity and Access Management • Security Assessment and Testing • Software Development Security • Auditing Information Systems	• Vulnerability Evaluation & Management • Threat Evaluation Analysis Network Architecture, Security, Tools & Protocols • Knowledge of Attack Methods • Protection Concepts • Penetration Testing
• Incident Investigation & Response	• Security Analysis • Risk Management • Communications and network security • Identity and Access Management • Security Operations • Auditing Information Systems • Information Systems Operations • Incident Management • Cloud Security • Threat Hunting	• Event Monitoring • Data Protection and Encryption • Vulnerability Evaluation & Management • Digital Forensics • Threat Evaluation Analysis • Firewall Management • Network Architecture, Security, Tools, & Protocols • SOC Processes and Concepts • Incident Response • Handling Compromised Systems • Protection Concepts • Managing Enterprise-level Security Systems • Detecting Complex and Advanced Breaches • Developing Hunting and Detection Routines • Risk Mitigation and Management • Running SIEM & Data Loss Prevention (DLP) Systems • Automation (Configuration, Management, Security Systems)

APPENDIX

SKILLS RANKED IN ORDER OF IMPORTANCE FROM ICTC'S NEW BRUNSWICK EMPLOYER SURVEY[85]	SKILLS DIRECTLY MENTIONED IN INTERVIEWS OR SPECIFIC TO QUALIFICATIONS MENTIONED IN INTERVIEWS	SKILLS SCRAPED FROM JOB POSTINGS IN NEW BRUNSWICK (AGGREGATED WHEN SIMILAR)
Group three:		
• Risk Assessment & Management	• Security Analysis • Risk Management • Security Assessment and Testing • Auditing Information Systems • Risk Management • Security Management	• Vulnerability Evaluation & Management • Threat Evaluation Analysis • Protection Concepts • Risk Mitigation and Management • Security Metrics and Reporting
• Knowledge of IoT Security	• Security Analysis • Risk Management • Security Engineering • Communications and Network Security • Identity and Access Management • Cloud Security	• Vulnerability Evaluation and Management • Threat Evaluation Analysis • Network Architecture, Security, Tools, & Protocols • Protection Concepts
• Encryption and Cryptography, Quantum-safe Cryptography	• Security Engineering • Communications & Network Security	• Data Protection & Encryption • Knowledge of Attack Methods
OTHER TECHNICAL SKILLS [RESPONSES GIVEN TO OPEN-ENDED ALTERNATIVE, "ANOTHER IMPORTANT SKILL SET (PLEASE SPECIFY)"]		
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

Figure 16