A Race for Talent:

Insights from Canadian Cybersecurity Employers

Future Skills Centre

Blueprint

Contents

Executive summary

As cyber threats increase in volume and sophistication, Canadian corporations, both large and small, see cybersecurity as one of the top risks to organizational growth. Cyber talent demand in Canada continues to increase, amidst an acute shortage of trained cybersecurity professionals.

While Canada is not alone in facing this shortage of talent, it does have a unique opportunity to tap into its growing pool of skilled newcomers, many of whom are women and racialized populations that are underrepresented in the cybersecurity sector. Employers must figure out how best to find, attract, recruit and retain this talent to meet the growing needs of the cybersecurity sector.

To make the sector more accessible to Canadians from diverse backgrounds, the Rogers Cybersecure Catalyst (the Catalyst) launched the Accelerated Cybersecurity Training Program (ACTP) in 2020. This program is specifically designed to give women, new Canadians, and displaced workers the skills they need to launch a career in the cybersecurity sector. With funding from the Future Skills Centre (FSC), the Catalyst and Blueprint have collaborated to lead research with cybersecurity employers in Canada to determine demand for cybersecurity professionals at the entry level, understand hiring practices of employers and identify their skills needs and the challenges they face in meeting their demand for cyber talent.

For this employer research, the Blueprint and Catalyst teams reached out to 49 mid-to-senior professionals in 23 medium-to-large organizations with whom the ACTP team had close relationships and invited them to complete the ACTP Employment Partners Survey. Of these 23 employers, 17 completed or partially completed the survey, for a response rate of 74%.

The purpose of the main report is to share findings from what we learned from these employers. In this summary, we share the key questions addressed by this research, the high-level findings that speak to these questions and recommendations for programs like the ACTP and for cybersecurity employers to effectively address the growing gap between demand and supply of cybersecurity talent in Canada.

Key Findings

Employer strategies: How do employers recruit and retain cyber talent?

- Most employment partners find employee referrals to be the most effective recruitment channel, and some also favour hiring candidates through certification training programs not linked to university or college degree programs.
- Employment partners believe that non-monetary aspects of a job such as a flexible work schedule and professional development opportunities may be as attractive to candidates in their job search as the compensation.

Skills needs: Which roles and skills are in-demand?

- Employment partners expect to need anywhere between two to 100 cybersecurity professionals per organization over the next year, and this demand could double in the medium-to-long term, with the highest current and future demand in the category of Protect and Defend roles.
- Incident Response, Cloud and Cyber Risk Management will continue to see high demand from employment partners, Data Security appears to be re-emerging and Security Data Analytics may see dwindling demand in the future.

- Employment partners currently highly value technical skills, such as intrusion detection and response techniques, troubleshooting, and network defense and protection systems operations, though this is likely to change in the next three to five years.
- Verbal communication, problem-solving, critical thinking, and attention to detail are currently the most valued non-technical skills for employment partners. These skills are expected to sustain this demand over the next three to five years.

Employer challenges: What are the biggest pain points for employers?

- Top industry-wide challenges include a shortage of skilled cybersecurity talent, and a mismatch between compensation and benefits offered and candidate expectations.
- Employment partners identified three barriers to creating accurate job descriptions for entry level cybersecurity roles: a mismatch between the organization and the applicants' expectations; lack of understanding by HR managers; and the rapid pace at which the industry is evolving.

Diversifying the sector: What challenges and opportunities lie ahead?

- 35% of employment partners reported challenges in recruiting BIPOC and/or women cybersecurity professionals and suggested three strategies to remedy this: partner with relevant networks and events; offer targeted opportunities for education and training; and have an open mind to hiring from underrepresented groups.
- While most employment partners have programs in place to recruit diverse candidates for cybersecurity roles and offer general workplace inclusion training, only some have invested in ensuring diversity in leadership, providing targeted development opportunities and offering in-depth DEI-related training.

Recommendations

Programs like the ACTP

- In addition to equipping participants with technical skills and certifications, programs like the ACTP should also build non-technical skills through practical exercises in the context of cybersecurity.
- Programs like the ACTP can promote cybersecurity as a career within relevant BIPOC and women's communities and help address misperceptions of the industry.

Canadian Cybersecurity Employers

- While employers perceive employee referral as an effective recruitment channel, they should work to address its limitations, particularly in how it may exacerbate the current underrepresentation of certain groups in cybersecurity.
- To hire candidates from traditionally underrepresented groups, employers need to partner with relevant networks and participate in events/panels that can connect them to this under-utilized talent pool and be more open-minded to new perspectives
- Technical experts, HR and hiring managers at cybersecurity organizations should work together to draft accurate job descriptions for entry-level cybersecurity roles with clearly defined skills and expectations.

1 Introduction

Canadian corporations, both large and small, see cybersecurity as one of the top three risks to organizational growth. While these enterprises have doubled down on cybersecurity, data protection and privacy, 36% of small- to medium-sized businesses and 27% of CEOs say they are unprepared to handle a cyber attack (KPMG, 2021).[1] It is not surprising then that cyber talent demand in Canada continues to increase: one study estimated the cybersecurity workforce gap in Canada in 2021 at 25,000 professionals ((ISC)², 2021). At the same time, there is an acute shortage of trained cybersecurity professionals (Posadzki, 2019).[2]

While Canada is not alone in facing this shortage of talent,[3] it does have a unique opportunity to tap into its growing pool of skilled newcomers, many of whom are women and racialized populations that are underrepresented in the cybersecurity sector. Employers must figure out how best to find, attract, recruit, and retain this talent to meet the growing needs of the cybersecurity sector.

To make the sector more accessible to Canadians from diverse backgrounds, the Rogers Cybersecure Catalyst (the Catalyst) — Toronto Metropolitan University's national centre for training, innovation and collaboration in cybersecurity — launched the Accelerated Cybersecurity Training Program (ACTP) in 2020. This seven-month skills training program is specifically designed to give women, new Canadians and displaced workers the skills they need to launch a career in the cybersecurity sector.

One reason for the cybersecurity talent shortage is the lack of professionals with the credentials necessary to get hired (Lake, 2022). By offering a program that provides industry-recognized certifications and helping women and individuals from diverse backgrounds to enter the sector, the Catalyst aims to address the skills shortage while also fostering more diversity and inclusion in the cybersecurity ecosystem.

In October 2021, the Catalyst received funding from the Future Skills Centre (FSC) to launch the Cyber Talent Transformation Initiative (CTTI) to expand the reach of the ACTP program to individuals who identify as Black, Indigenous and People of Color (BIPOC), and to lead in-depth research that offers perspectives and actionable recommendations on diversity and inclusion in cybersecurity.

Blueprint, as an evidence generation partner of the FSC, is collaborating with the Catalyst to lead research with (a) participants of the ACTP program and (b) Canadian cybersecurity employers. The participant research aims to understand program experience and outcomes, with a focus on the unique challenges facing BIPOC and/or women participants in accessing cybersecurity skills training and employment opportunities. Findings from this research will be shared in a report next year (2023). The employer engagement aims to determine demand for cybersecurity professionals at the entry level, understand hiring practices of employers and identify their skills needs, and the challenges they face in meeting their demand for cyber talent.

Employer Research: Approach and Key Questions

In the first part of our research, we reached out to 23 employers with whom the ACTP team had close relationships.[4] Within these medium-to-large organizations, the ACTP team identified 49 cybersecurity leaders or human resources (HR) professionals who were invited to complete an in-depth survey in April 2022. The purpose of this report is to share findings from what we learned from these employers.[5]

To probe deeper into the survey findings, we interviewed respondents who agreed to share their hiring experiences and insights with us. We drew upon two such semi-structured interviews with cybersecurity professionals with hiring and management responsibilities to provide more context around the survey findings.[6]

An ongoing part of this research (May–November 2022) centres on understanding the broader needs of the Canadian cybersecurity sector. For this, we are exploring the ACTP team's emerging employer relationships with cybersecurity leaders or HR professionals who are familiar with the program, but whose engagement with the ACTP and its graduates is still nascent. We present some preliminary findings from this research in Section 3, and an upcoming report will feature in-depth analysis and comparison between the views of employers with close versus emerging relationships with the ACTP.

The findings in the report speak to four key questions:

Employer strategies
How do employers recruit and retain cyber talent?

Skills needs
Which roles and skills are in-demand?

Employer challenges
What are the biggest pain points for employers?

Diversifying the sector
What challenges and opportunities lie ahead?

ACTP Employment Partners Survey

The ACTP Employment Partners Survey was sent to 49 mid-to-senior professionals in 23 medium-to-large organizations in financial services, IT and Telecommunications and sectors with an industry focus on hiring cybersecurity talent. Nearly 40% of employers we reached out to were large businesses, employing more than 10,000 people.

Blueprint and the Catalyst team iterated on the themes and questions to include in the survey, which was then finalized and fielded by the Blueprint team.[7] Of the 23 employers we reached out to, 17 completed or partially completed the survey,[8] for a response rate of 74%. The individual response rate was 51%.[9]

Readers should keep in mind two considerations while interpreting the results presented in this report. The first is the sample size and survey response rates. Surveys of senior professionals and/or executives typically have lower response rates, and while we achieved reasonably high response rates given the close relationship these professionals share with the ACTP program staff, it is still important to note that findings are based on responses by 25 professionals in 17 organizations.

The second is that this survey was only sent to employers belonging to the ACTP network at the time of fielding the survey. As such, the findings reflect their specific needs and preferences and may not be representative of the broader Canadian cybersecurity sector.

The remainder of this report is structured as follows: Section 2 shares key findings from the ACTP employment partner survey and Section 3 outlines a few preliminary findings from the broader ongoing employment survey. Section 4 presents six recommendations based on these findings for organizations that offer programs similar to the ACTP and for cybersecurity employers.

About Blueprint

Blueprint was founded on the simple idea that evidence is a powerful tool for change. We work with policymakers and practitioners to create and use evidence to solve complex policy and program challenges. Our vision is a social policy ecosystem where evidence is used to improve lives, build better systems and policies, and drive social change. Our team brings together a multidisciplinary group of professionals with diverse capabilities in policy research, data analysis, design, evaluation, implementation, and knowledge mobilization. As a consortium partner of the Future Skills Centre, Blueprint works with partners and stakeholders to collaboratively generate and use evidence to help solve pressing future skills challenges.

About Future Skills Centre

The Future Skills Centre (FSC) is a forward-thinking centre for research and collaboration dedicated to preparing Canadians for employment success. We believe Canadians should feel confident about the skills they have to succeed in a changing workforce. As a pan-Canadian community, we are collaborating to rigorously identify, test, measure, and share innovative approaches to assessing and developing the skills Canadians need to thrive in the days and years ahead. The Future Skills Centre was founded by a consortium whose members are Toronto Metropolitan University, Blueprint, and The Conference Board of Canada, and is funded by the **Government of Canada's Future Skills Program**.

2 Key Survey Findings

In this section, we present findings that speak to the four questions outlined in the Introduction.

Employer Strategies: How Do Employers Recruit and Retain Cyber Talent?

Targeting the right avenues to find talent is a big part of a successful hiring strategy. We asked survey recipients to share the recruitment channels they find most effective, as well as factors they think candidates prioritize during their job search.

Finding 1
Most employment partners find employee referrals to be the most effective recruitment channel, and some also favour hiring candidates through certification training programs not linked to university or college degree programs.

Employment partner respondents largely agree on the most effective recruitment channel to hire cybersecurity talent — employee referrals (58%) (Figure 1). Interviews with two cybersecurity professionals indicated that employee referrals are attractive because they allow candidates to be vetted by individuals with a deep understanding of the nature of the role and the company, and who can more effectively assess the suitability of the candidate for the job. In addition to informal referrals, the interviewees' organization has had formal referral programs for several years, and bonuses to incentivize existing employees to reach out to their networks are calibrated according to the level of demand for skills.

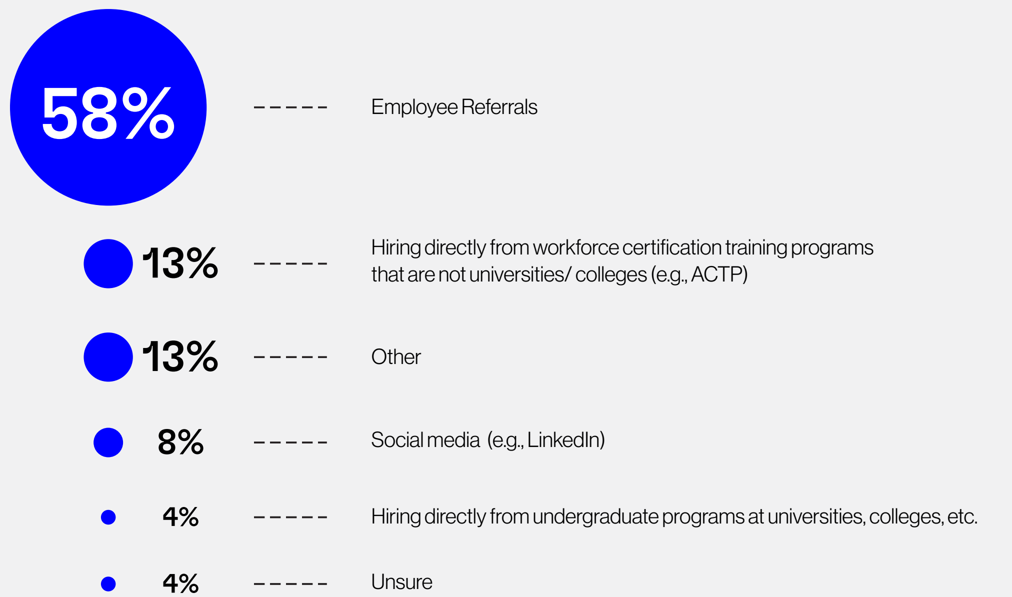
A few respondents viewed hiring directly out of workforce certification training programs that are not linked to university or college degree programs (e.g., the ACTP) as an effective recruitment channel (13%). One interviewee suggested that while they tend to prefer employee referrals, their organization would need to tap into different resources in times of strong demand.

Finding 2
Employment partners believe that non-monetary aspects of a job such as a flexible work schedule and professional development opportunities may be as attractive to candidates in their job search as the compensation.

A majority of employment partner respondents believe that compensation (88%), a flexible work schedule/remote work (88%) and professional development opportunities (76%) are the most important factors for candidates looking for a job in cybersecurity (Figure 2).[10] This implies that to attract the best candidates, these partners might highlight non-monetary aspects of a job such as flexible working hours or learning opportunities (certifications, microcredentials) in the job description and hiring process. Additionally, only 12% believed that sign-on incentives (e.g., retention bonus) are among the most important considerations for candidates during the job search.

Many respondents encourage professional development opportunities.[11] When asked about specific ways in which organizations support employees to pursue cybersecurity certifications, most reported providing monetary incentives or covering course fees (83%), collaborating with employees to help them pursue the right courses (65%) and providing time off to take training and attend courses (43%). As Kvochko (2021) also argues, reskilling current employees who show an interest in security can be a rewarding strategy for companies who are struggling to hire.

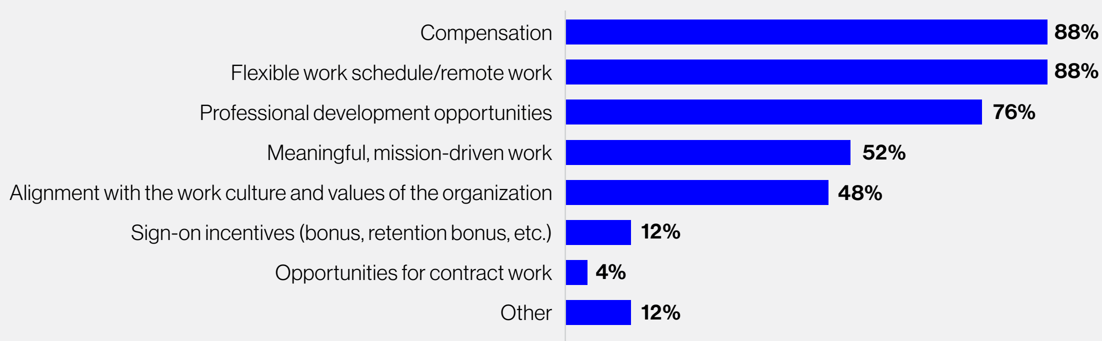
Figure 1 | Most effective recruitment channels



Notes: These percentages are based on responses by 24 individuals.

Three other response options that were not selected by anyone include: specialized external recruiters, advertising on job boards, and Capture the Flag Competitions or Bug Bounty Programs.

Figure 2 | Employment partner perceptions of most important factors for cybersecurity job seekers



Note: These percentages are based on responses by 25 individuals.

Skills Needs: Which Roles and Skills Are In-Demand?

The breakneck speed at which the cybersecurity sector is evolving compels us to understand the recruitment needs of employment partners so programs like the ACTP can ensure they are aligning with industry needs. To do so we asked respondents about their organization's recruitment needs, and whether and how they think these might change in the next three to five years.

Finding 3

While employment partners expect to need anywhere between two to 100 cybersecurity professionals over the next year, this demand could double in the medium-to-long term, with the highest current and future demand in the category of Protect and Defend roles.

Recruitment needs can vary by firm size, nature of business and expected growth. Employment partner respondents expect to need between two to 100 cybersecurity professionals in their organization over the next 12–18 months, though most felt that their organization would need fewer than 10 (40%) (Figure 3). Both interviewees shared that in the next three to five years, their current need for cyber professionals is likely to double.

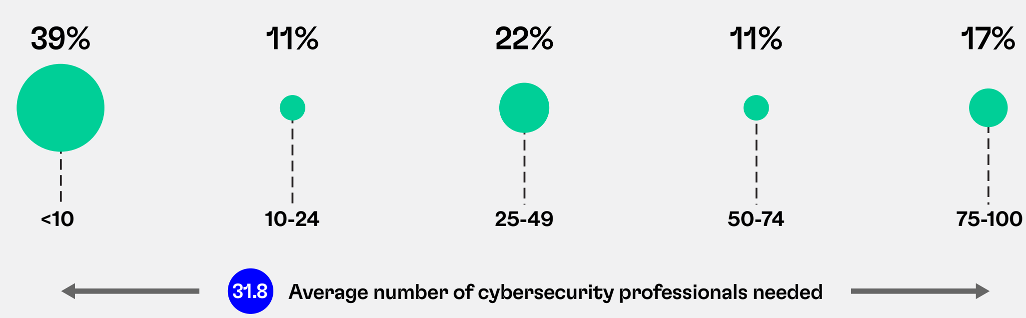
Following the Canadian Cybersecurity Skills Framework (TECHNATION 2022), we considered four categories of business-oriented cybersecurity roles where this demand is likely to show up: Protect and Defend, Design and Develop, Oversee and Govern and Operate and Maintain. The category with the highest current and future demand for cybersecurity professionals is Protect and Defend, which includes roles such as cybersecurity analysts, penetration testers, cybersecurity incident responders and digital forensic analysts. (Figure 4A) [12] This high demand is expected to sustain over three to five years (78%).[13] In general, the ACTP's employment partners believe that all categories will see a similar demand pattern three to five years from now.

Finding 4

Incident Response, Cloud, and Cyber Risk Management will continue to see high demand from employment partners, while Data Security appears to be re-emerging and Security Data Analytics may see dwindling demand in the near future.

The three specializations with the most demand for talent from the ACTP employment partners are Incident Response (54%), Cloud (46%) and Cyber Risk Management (38%) and this demand is likely to increase. 65% of respondents indicated that Incident Response and Cloud will be the most in-demand over the next three to five years (Figure 4B). This may be because the ACTP team has intentionally worked with organizations that need these roles, for which the ACTP graduates are well-suited.

Figure 3 | **Estimated number of cybersecurity professionals needed in 12–18 months**



Note: These percentages are based on responses by 18 individuals.

One specialization that will likely be required by employment partners is Data Security (21% now vs. 35% over the next three to five years). As the volume of data organizations own and manage is expected to increase, so is the demand for talent within this specialization, as companies look to protect their organizational data from loss, compromise, and unauthorized use.

The only specialization that is expected to see a reduced demand is Security Data Analytics. While 29% think that this is currently among the most in-demand groups, only 13% think this will be the case three to five years from now (Figure 4B). This is likely because the adoption of artificial intelligence/machine learning tools is on the rise. These shifting demand expectations can inform programs like the ACTP that are looking to tailor their curricula to meet employer and sectoral needs.

Figure 4A | In-demand cybersecurity categories

	Current	Future
Protect and Defend	75%	78%
Design and Development	38%	43%
Oversight and Governance	29%	26%
Operations and Maintenance	17%	26%
Other	25%	0%
Unsure	0%	13%

Note: Percentages are based on responses by 24 individuals (current) and 23 individuals (future).

Figure 4B | In-demand cybersecurity specializations[14]

	Current	Future
Incident Response	54%	65%
Cloud	46%	65%
Cyber Risk Management	38%	52%
Identity Access Management	38%	N/A
Security Automation Processes	38%	39%
Threat Intelligence Collection Analysis	38%	39%
Security Data Analytics	29%	13%
Security Engineering	25%	26%
Automated Security Processes	25%	17%
Data Security	21%	35%

Percentages are based on responses by 24 individuals (current) and 23 individuals (future).

Finding 5

Employment partners currently highly value technical skills such as intrusion detection and response techniques, troubleshooting, and network defense and protection systems operations, though this is likely to change in the next three to five years.

In hiring for entry-level cybersecurity roles, the three technical skills most valued by employment partner respondents are intrusion detection and response techniques (50%), troubleshooting (42%) and network defense and protection systems operations (38%). A third of respondents also pointed to vulnerability assessment and identity and authentication management as technical skills they look for in candidates (Table A1 in Appendix).

More than 60% of respondents believed that the most valued technical skills in their organization are likely to change in the next three to five years (Figure 5).[15] When it comes to programming or scripting languages, employment partners most value Python for entry-level positions. Languages with relatively low demand include Shell (42%), JavaScript (33%), LINUX (33%) and Java (29%) (Table A4 in Appendix). When addressing microcredentials and certifications, employment partners most value GIAC Security Essentials Certifications (GSEC) (54%), GIAC Certified Incident Handlers (GCIH) (46%), CompTIA Security+ (46%) (Table A3).

Finding 6

Verbal communication, problem solving and critical thinking, and attention to detail are currently the most valued non-technical skills for employment partners. These skills are expected to sustain this demand over the next three to five years.

The three non-technical skills most valued by the ACTP employment partner respondents for entry-level cybersecurity roles were verbal communication (88%), problem-solving and critical thinking (88%) and attention to detail (83%) (Table A2 in Appendix).[16] Respondents also highlighted adaptability and the ability to perform under stress as valuable non-technical skills. This finding is in line with a recent report by (ISC)² (2021) which found that globally, strong problem-solving abilities, curiosity and eagerness to learn, and communication skills were equally if not more important than cybersecurity certifications and relevant cybersecurity experience.

In contrast to technical skills, which appear to have a shorter shelf-life, these non-technical skills are likely to continue to be in demand over the next three to five years: 70% of respondents indicated so (Figure 5). One interviewee shared that while their organization values technical skills, they would likely prefer candidates that are passionate about the work and have good problem solving skills, even if they do not have the exact technical skills background they seek. For programs like the ACTP, this means highlighting the importance of these skills to program participants so they can cultivate these in parallel to technical skills.

Figure 5 | **Changing demand for technical and non-technical skills**

61% — **61%** said that technical skills their organizations looks for in cybersecurity professionals will change in 3–5 years

70% — **70%** said that non-technical skills their organizations looks for in cybersecurity professionals will **not** change in 3–5 years

Over 35% valued these technical skills:

- Intrusion detection and response techniques
- Troubleshooting
- Network defense and protection systems operations

Over 80% valued these non-technical skills:

- Verbal communication
- Problem solving and critical thinking
- Attention to detail

Over 46% valued these certifications:

- GIAC Security Essentials Certifications
- GIAC Certified Incident Handlers (GCIH)
- CompTIA Security +

Note: These percentages are based on responses by 24 individuals

Employer Challenges: What Are the Biggest Pain Points for Employers?

We wanted to know about the biggest pain points for employment partners when it comes to recruiting cyber talent. We asked respondents questions about the types of challenges their organization and the overall cybersecurity sector face in recruiting cyber professionals.

Finding 7

Top industry-wide challenges include a shortage of skilled cybersecurity talent and a mismatch between compensation and benefits offered and candidate expectations.

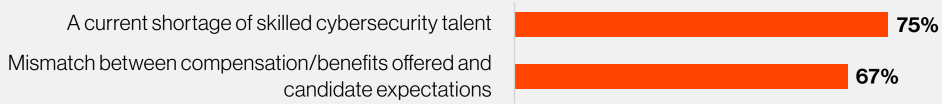
Employment partner respondents confirmed an industry-wide challenge — a shortage of skilled cybersecurity talent in Canada — which prevents organizations from meeting their recruitment needs (Figure 6). This sentiment is also reflected in responses to organization-specific recruitment challenges such as the candidate pool not being adequately qualified (58%), candidates lacking the relevant competencies (50%) and high levels of competition for the right talent (58%). Related, a third of respondents felt that the pool of applicants for open positions is small (33%). Elaborating on some of these challenges, one interviewee highlighted that at the entry level, everyone wants to "do the most sexy job" (e.g., be a hacker or a penetration tester), but these roles require a lot of knowledge and cannot be done by someone entering the sector.

At the industry level, respondents perceived a mismatch between compensation and benefits offered and candidate expectations (67%). A study by Deloitte (n.d.) also finds that "compensation and incentive plans are not keeping pace with market rates — which are continually inflated due to the lack of supply to meet demand." Interviewees confirmed that even for entry level roles, candidates expect to earn 20–40% more than what employers are typically willing to offer.

When asked about specific cybersecurity roles their organization had the most difficulty filling in the past three months, 29% of respondents identified cybersecurity incident responder and cybersecurity operations analyst as the two most-difficult-to-fill cybersecurity roles (Table A5 in Appendix).

> "There needs to be distinct roles and responsibilities within the Cybersecurity space because it is currently very blurred. The landscape is very reactionary [sic], and it lacks planning and investment."
>
> Survey respondent

Figure 6 | **Most common recruitment challenges facing the cybersecurity industry**



Less than 30% selected these recruitment challenges:

- Too many certifications in the market and lack of clarity around the learning outcomes of each
- Perception that cybersecurity roles are high stress, have a heavy workload and irregular hours
- Lack of flexibility for remote working
- Job descriptions/postings that require more experience than necessary
- Applicants' limited understanding of cybersecurity as a distinct IT domain when applying for cyber positions
- Lack of clear, direct career pathways in/into cybersecurity
- Employers' limited understanding of cybersecurity as a distinct IT domain when hiring cyber talent
- Lack of clarity among applicants regarding the education, training and/or prior experience requirements for cybersecurity roles
- Lack of clarity among employers regarding the education, training and/or prior experience requirements for cybersecurity roles
- Lack of training options (e.g. microcredentials, hackathons) to close skills gap
- Other

Note: These percentages are based on responses by 24 individuals.

Finding 8

Employment partners identified three barriers to creating accurate job descriptions for entry level cybersecurity roles: a mismatch between the organization and the applicants' expectations, lack of understanding by HR managers, and the rapid pace at which the industry is evolving.

While inaccurate job descriptions were not among the top recruitment challenges identified by the employment partners in the survey, 70% did describe barriers that might prevent organizations from creating accurate job descriptions for entry-level cybersecurity roles.[17] Our analysis of the open-ended responses reveals three broad barriers.

Discrepancy between applicants' expectations of a job and what the employer wants and can offer. This includes:

- Over-selling the position to applicants
- Misalignment between the organization's business model and applicant's personal goals
- Employers asking too much from candidates applying to entry-level positions
- Some entry level roles requiring more experience than the job postings suggest

> "Despite being entry level, a Level 1 Security Operations role requires profound knowledge of cybersecurity concepts and how to manage working under pressure."

Survey respondent

Lack of understanding on the part of hiring managers or HR professionals. Respondents felt that hiring managers or HR professionals lacked sufficient understanding about the industry, the work requirements of roles within cybersecurity and how to package those requirements into a job description. For instance, a respondent highlighted that HR may overcomplicate the skills needed for the job by making the role sound like it requires in-depth knowledge of certain cybersecurity topics when only general knowledge may be needed.

Fast-paced industry with rapidly evolving requirements. The constantly changing needs of the cybersecurity industry may make it difficult for job descriptions to keep pace (Rashotte, 2019). For instance, rapid expansion of cyber teams can lead to changes in tasks and responsibilities that are not reflected in job descriptions. Cybersecurity also includes multiple areas, which makes it difficult to cover all tasks in a single job description. Finally, partners also identified the lack of an overall cybersecurity strategy.

"Over-complication by HR, some teams require one person with good knowledge or advanced skills in one area and several people with more general knowledge or skills in that given area. However, the same role gets described to fit every individual on the entire team [regardless of how much knowledge they actually need], thereby making it sound like everyone needs to be super-human [i.e., have expert knowledge or skills in a given area]."

Survey respondent

Diversifying the Sector: What Challenges and Opportunities Lie Ahead?

While the underrepresentation of women in STEM fields has been a long-standing challenge, the last few years have seen some progress in diversification of several traditionally-male dominated fields. Globally, women now make up 25% of the cybersecurity workforce ((ISC)², 2021). But while many employers agree to the need for diversification of the sector, they have different formal and informal approaches to ensuring diversity, such as prescribing quotas.[18]

We looked at whether employers face challenges in recruiting BIPOC and/or women cybersecurity professionals, what programs or initiatives exist to promote greater diversity in the sector, and what strategies might improve the status quo.

Finding 9

35% of employment partners reported challenges in recruiting BIPOC and/or women cybersecurity professionals and suggested three strategies to remedy this: partner with relevant networks and events; offer targeted opportunities for education and training; and have an open mind to hiring from underrepresented groups.

"Just be more open-minded. If everyone is given the same opportunities, it is more than likely we will always find the gems."

Survey respondent

Nearly half of employment partner respondents reported that their organization has not faced any challenges in recruiting BIPOC and/or women cybersecurity professionals to date (48%). However, 35% did perceive this to be a challenge.[19] One interviewee revealed an interest on the part of their organization to expand recruitment efforts to under-served populations, specifically Indigenous individuals, but reported that current programs have not been very successful. Similarly, the second interviewee highlighted that while their organization actively looks to recruit BIPOC and/or women professionals, it is not easy to find applicants that belong to these groups due to the current composition of the cybersecurity population within the universities and colleges that they hire from.

To remedy this challenge, we asked respondents to suggest actions that can be taken to promote the recruitment and hiring of more BIPOC and/or women cybersecurity professionals. Nearly 70% shared ideas, which we summarize in the three broad areas below:

Partner with relevant networks

Employers can partner with networks that can connect them to the talent pool they are looking for. Respondents suggested partnering with specific BIPOC and/or women-in-cyber networks, non-profit organizations and/or trusted cybersecurity training programs (such as the ACTP) that have a diverse pool of candidates to hire from. Additionally, employers can participate in panels and events targeted toward underrepresented groups, where they could meet potential hires. These venues can also offer good opportunities for BIPOC and/or women cybersecurity professionals to inspire others to join the sector.

Create more education and upskilling opportunities for underrepresented groups

Employers can create more education and upskilling opportunities for BIPOC and/or women aspirants. Specific suggestions included giving them "the right skills at the right time," providing opportunities and support around security-based education, creating opportunities to train people from these groups if recruiters fail to attract diverse candidates, and promoting cybersecurity as a career within relevant BIPOC and/or women's communities to help address misperceptions of the industry.

Create a cultural shift to being more open to diverse backgrounds

Employers can work to be more open-minded when it comes to hiring candidates and retaining them. Respondents suggested to not focus only on credentials and the technical aspects of cybersecurity, but also to listen with an open mind to perspectives that individuals from diverse backgrounds bring to the table.

In addition to these three strategies, another suggestion was to have flexible work locations, which would allow employers to hire from a broader pool, and therefore attract underrepresented groups that may be based in different locations.

> **The key is to get the right person for the job irrespective of their demographic.**
>
> Interviewee

Finding 10

While most employment partners have programs in place to recruit diverse candidates for cybersecurity roles and offer general workplace inclusion training, only some have invested in ensuring diversity in leadership, providing targeted development opportunities, and offering in-depth DEI-related training.

Most employment partner respondents reported having programs in place within their organization to recruit diverse candidates for cybersecurity roles (74%). This likely reflects the connections that employers have with the Catalyst team to recruit cyber talent from the ACTP, which provides a steady stream of diverse and qualified talent. However, fewer respondents indicated that their organization had programs to develop a pipeline of diverse cybersecurity leaders (39%), and only 26% of respondents' organizations have programs that provide targeted development opportunities for BIPOC and/or women employees (Figure 7).

One interviewee highlighted that as part of their efforts to build a more inclusive workforce, their organization provides training to employees to educate them about diversity. Their approach is to "change the mentality [around DEI] rather than the process." This suggests that rather than have programs targeted at BIPOC/women employees, some employers offer programs to all employees to increase overall awareness about diversity-related issues as a strategy to build a more inclusive workforce within their organization.

While training is only a small part of embracing diversity, equity, and inclusion in the workplace, it does signal the level of commitment or priority that organizations assign to this. Most respondents reported that their organizations offered general workplace inclusion training (65%),[20] however, fewer offered ongoing training on overcoming unconscious bias (43%), embracing differences in the workplace (43%) and embedding inclusive behaviours into everyday job activities and responsibilities (39%). Very few offered training on managing employees from diverse populations (13%) and some do not offer any DEI-related training at all (Figure 7).

The findings presented in this section were based on responses from employers with close relationships with the ACTP. However, these insights have broader relevance for training programs that aim to equip individuals interested in the cybersecurity sector with industry-relevant skills. The next section offers a glimpse into the ongoing employer research, which goes beyond the ACTP's current employment partners, and shares a few preliminary findings from the same.

Figure 7 | DEI Recruitment Practices

Note: These percentages are based on responses by 23 individuals.

3 Broader Industry Survey: Initial Findings

For this ongoing research, the ACTP team developed a list of professionals in organizations with currently limited experience engaging with the ACTP as well as leveraged social media to reach a wide range of employers. The questions asked in this survey are very similar to those in the ACTP Employment Partners Survey. This allows us to compare recruitment needs of these two different employer groups. We believe that these insights can help the ACTP team identify needs and support talent requirements of the broader cybersecurity sector.

The survey has been sent to around 150 mid-to-senior professionals in 85 organizations.[21] As of July 2022, we had received 29 responses, and the survey will remain open for a few more weeks. In a follow-up report in 2023, we will present in-depth survey insights on the current and future cybersecurity talent needs and skills gaps, existing practices to recruit more diverse candidates, and the challenges therein. This short section features two preliminary findings as an example of what industry partners can expect in the upcoming report.

Cybersecurity employers also find employee referrals to be the most effective recruitment channel, but compared to the ACTP employment partners, some also favour recruiting candidates through social media and from undergraduate programs.

We find that employee referrals continue to be perceived as the most effective way to hire in the Canadian cybersecurity sector (48%). Using social media such as LinkedIn comes second, though by a wide margin (21%). This could suggest that employers may reduce their reliance on online job postings to find the cyber talent they are looking for. The emphasis on employee referrals also raises implications for diversifying the cyber workforce: the sector is largely dominated by men and those with an IT background (Deloitte, n.d.), with little representation from women and racialized groups, and future hiring based on referrals might reinforce this composition.

Cybersecurity employers and the ACTP employment partners are aligned on the top industry-wide challenges, but diverge on other challenges facing the sector.

Canada seems to be no different to other countries when it comes to the most acute challenge facing the cybersecurity sector: a current shortage of skilled talent.[22] Similar to ACTP employment partners, respondents from the broader industry highlighted this as the most common recruitment challenge (62%), followed by a mismatch between compensation and benefits offered and candidate expectations (54%).

However, there are two ways in which respondents diverge from their ACTP employment partner counterparts. The first is that a significant number highlighted the lack of clear and direct career pathways into cybersecurity (42%). This does not seem to be unique to Canada. In a recent survey, the Enterprise Security Group found that 66% of cybersecurity professionals globally do not have a clearly defined career path for taking their careers to the next level (Deloitte, n.d.).

The second relates to employers' limited understanding of cybersecurity as a distinct IT domain (42%). These challenges were not necessarily top-of-mind for the ACTP employment partners, suggesting that the broader sector might have a different set of priorities. Employers will need to build their own understanding of the unique needs and distinct nature of cybersecurity within IT, and organizations offering cybersecurity training will need to articulate clear pathways to entry into the sector.

A similar share of cybersecurity employers expressed facing challenges in recruiting diverse talent as the ACTP partners did: 36% said that their organization encountered challenges in recruiting and hiring BIPOC and/or women cybersecurity professionals.

Engaging with Employers: The Catalyst's Industry Advisory Council

Comprised of eight senior executives in leading cyber roles from some of Canada's top companies in the sector, the ACTP Advisory Council aims to inform CTTI research and provide a two-way, open line of communication between the Catalyst team and organizations who are employing graduates from the ACTP. The Council held its first meeting in March 2022 and meets on a quarterly basis. This collaborative approach allows the Catalyst team to share relevant research updates and seek feedback on the implementation of the ACTP program.

In particular, the Advisory Council:

- Advises on potential impacts of the CTTI project research findings on industry
- Advises on ways to improve knowledge mobilization, communication and engagement with the industry
- Identifies opportunities where the ACTP program can most effectively meet cybersecurity talent needs
- Considers research, best practices and actions taken by other institutions on advancing skills development and diversity initiatives in the cybersecurity ecosystem
- Discusses creative ideas and new approaches to reducing existing barriers, including both short-term and long-term measures
- Advises on matters related to accreditation and microcredentials
- Assists in the identification of student placements and employment opportunities
- Makes recommendations on areas of cybersecurity skills development

Following discussions around the growing Canadian cybersecurity talent gap, the ACTP team is working to develop a Cyber Talent Management Playbook to integrate best practices in talent management drawn from HR, organizational development and cybersecurity disciplines. Building upon these best practices, the Playbook will also flip the script on national talent generation by taking a needs-based approach to identifying cybersecurity talent requirements in Canada and engaging the broader cybersecurity ecosystem in creating a talent pipeline that is more responsive to national, regional and sectoral talent requirements.

4 Recommendations

Our findings have reiterated a global challenge facing the cybersecurity sector: an acute shortage of skilled cyber talent which prevents organizations from meeting their recruitment needs. At the same time, the COVID-19 pandemic has increased demand for remote work, thereby increasing the demand for cybersecurity talent.

In this section, we focus on two sets of stakeholders in the cybersecurity ecosystem: program leadership in organizations aiming to build a talent pipeline with a focus on underrepresented groups, and Canadian cybersecurity employers.

Based on findings shared in Section 2, we present three key recommendations each for these groups to effectively address the growing gap between demand and supply of cybersecurity talent in Canada.

Programs like the ACTP

Recommendation 1: Programs like the ACTP should focus on equipping participants with skills for Protect and Defend roles.

Employment partner respondents view the Protect and Defend category of roles as the most in-demand in their organizations and expect to see continued demand in this category over the next three to five years (over 75%). Programs like the ACTP should design their curricula in a way that can effectively meet this demand.

The ACTP prepares its participants for entry-level roles, and many of the roles within the Protect and Defend category are natural extensions of those entry level roles (e.g., penetration testers and digital forensic analysts). If the ACTP can respond to this high demand in Protect and Defend, it will be setting up a pathway for candidates to advance in their cybersecurity careers. Additionally, within the high-demand categories and specializations, the technical skills that employers will look for are likely to change (60%), so programs need to stay flexible to adapt to changing needs.

Recommendation 2: In addition to equipping participants with technical skills and certifications, programs like the ACTP should also build non-technical skills through practical exercises in the context of cybersecurity.

Our findings revealed that even as the technical skills that employers look for in candidates may change three to five years from now, certain non-technical skills that are currently in demand will continue to matter in the future. Moreover, employers often value these skills more than technical ones, which are relatively easier to impart.

Programs like the ACTP that want to ensure that their participants can effectively function as cyber professionals should emphasize non-technical skills that employers perceive to be valuable, such as verbal communication, problem solving and critical thinking as well attention to detail.

Recommendation 3: Programs like the ACTP can promote cybersecurity as a career within relevant BIPOC and/or women's communities and help address misperceptions of the industry.

To bring more women and racialized people into the cybersecurity sector, employers suggested promoting cybersecurity as a career within relevant BIPOC and/or women's communities. To advance this strategy, different stakeholders in the ecosystem have a role to play. For example, schools and universities should pay attention to how they present cybersecurity as a career option and dispel existing gender stereotypes that have contributed to an underrepresentation of women in the sector.

Programs like the ACTP can collaborate with universities to increase awareness about what it means to have a career in cybersecurity, highlight the role of BIPOC and women in the sector and encourage young adults to pursue the relevant education and credentials. They can also involve their program alumni at forums or venues targeted toward BIPOC and/or women professionals to highlight successes to inspire the next generation of cybersecurity leaders.

Canadian Cybersecurity Employers

Recommendation 1: While employers perceive employee referral as an effective recruitment channel, they should work to address its limitations, particularly in how it may exacerbate the current underrepresentation of certain groups in cybersecurity.

Employee referrals are attractive to employers for various reasons, and while this can often be the least risky option when it comes to finding talent, it does not come without a cost. Relying on employee referrals means largely tapping into similar kinds of networks and people with similar socio-demographic and professional backgrounds. This method may perpetuate the underrepresentation of BIPOC and/or women in the sector.

To address some of the potential challenges that may come with relying heavily on employee referrals, employers should actively reach out to online communities such as women's networks or newcomers to Canada to build strong connections that can help them access the talent they need from within those communities. Posting job descriptions that are accurate and clear can also make social media (e.g., LinkedIn) a more effective channel than it currently is.

Recommendation 2: To hire candidates from traditionally underrepresented groups, employers need to partner with relevant networks and participate in events/panels that can connect them to this underrepresented talent pool and be more open-minded to new perspectives.

To recruit more talent from underrepresented groups, employment partner respondents suggested partnering with specific BIPOC and women-in-cyber networks, non-profit organizations and/or trusted cybersecurity training programs (such as the ACTP) that have a diverse pool of candidates to hire from.

Employers can encourage their employees — particularly BIPOC and/or women leaders — to participate in events and panel discussions to share their stories and experiences. Hearing directly from these leaders can be a strong source of motivation and inspiration for professionals considering joining the sector and staying in it.

Respondents also suggested that employers need to be "more open-minded" in terms of hiring from diverse backgrounds and take a more fulsome view of what a candidate can offer, rather than focusing solely on their credentials and technical skills. Employers can expand their pool of candidates significantly if they start emphasizing non-technical skills and attributes and create the right training and upskilling opportunities for these individuals.[23] In the short-term, while the industry continues to use recognized credentials, employers should work with training organizations (such as the Catalyst) to ensure that those from diverse groups get appropriate opportunities to become credentialed.

Recommendation 3: Technical experts, HR and hiring managers at cybersecurity organizations should work together to draft accurate job descriptions for entry-level cybersecurity roles with clearly defined skills and expectations.

Employers indicated that a mismatch between applicant expectations of a job and what the organization wants and/or can offer, along with a perceived lack of understanding by HR managers, makes it difficult to draft accurate job descriptions for entry-level cybersecurity roles. To remedy this, technical experts, HR and hiring managers need to work together to ensure that the job descriptions are accurate and focus on what is needed without overcomplicating the set of requirements.

While employers may have different requirements depending on their organization, team size, and nature of their business (ie. professional services), a good starting point is for employers to discuss roles and responsibilities for common cybersecurity roles and positions, and agree on required versus desirable credentials and qualifications. With some basic standards in place, employers could then meet on a regular basis to revisit these requirements to ensure that they are keeping up with the changing needs of the industry.

Next Steps

This report shared the views and perspectives of one group of employers who hire cybersecurity professionals. The report examined recruitment strategies to hire and retain cybersecurity talent, the demand for cyber specific skills, and the challenges faced in hiring BIPOC and/or women.

In an upcoming report in 2023, we will share insights from an ongoing survey of employers that are part of the larger Canadian cybersecurity ecosystem, as well as from the research with the ACTP program participants. We will bring together the participant and employer perspectives to share actionable insights on how programs like the ACTP and cybersecurity employers can better close the demand-supply gap for cyber talent in Canada.

References

Deloitte. (n.d). The changing faces of cybersecurity: Closing the cyber risk gap. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF

(ISC)². (2021). A resilient cybersecurity profession charts the path forward. https://www.isc2.org//-/media/ISC²/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

(ISC)². (2022). (ISC)² Cybersecurity hiring managers guide: Best practices for hiring and developing entry- and junior-level cybersecurity practitioners. https://www.isc2.org//-/media/ISC2/Research/2022/ISC2-Cybersecurity-Hiring-Managers-Guide.ash

KPMG. (2021). CEO outlook — Canadian insights. https://home.kpmg/ca/en/home/insights/2021/09/kpmg-2021-ceo-outlook-canadian-insights.html

Kvochko, E. (2021, October 19). How to attract cybersecurity talent. Forbes. https://www.forbes.com/sites/sap/2021/10/19/how-to-attract-cybersecurity-talent-and-build-a-culture-of-security/?sh=7f1a116a6b5f

Lake, S. (2022, June 30). Companies are desperate for cybersecurity workers — more than 700K positions need to be filled. Fortune. https://fortune.com/education/business/articles/2022/06/30/companies-are-desperate-for-cybersecurity-workers-more-than-700k-positions-need-to-be-filled/

Posadzki, A. (2019). Hackers wanted: Canada faces a troubling shortage of cybersecurity talent. Globe and Mail. https://www.theglobeandmail.com/business/article-canada-faces-a-troubling-shortage-of-cybersecurity-workers/

PwC. (2022, March 15). Using upskilling to solve the cybersecurity talent shortage. https://proedge.pwc.com/blog/using-upskilling-to-solve-the-cybersecurity-talent-shortage

Rashotte, R. (2019, July 4). The critical shortage of cybersecurity expertise. Policy Options. https://policyoptions.irpp.org/fr/magazines/july-2019/the-critical-shortage-of-cybersecurity-expertise/

TECHNATION (2022). Canadian Cybersecurity Skills Framework. Retrieved September 21, 2022, from https://technationcanada.ca/en/future-workforce-development/cybersecurity/cybersecurity-skills-framework/

Appendix

Table A1

Most Valued Technical Skills	% of Respondents
Intrusion detection and response techniques	50%
Troubleshooting	42%
Network defense and protection systems operations	38%
Vulnerability assessment	33%
Identity and authentication management	33%
Penetration testing	29%
Application of cloud security technologies and methodologies	29%
Security analytics	29%
Security testing and evaluation	25%
Digital forensics	25%
Security-related programming and scripting languages (secure coding)	21%
Security engineering	21%
Data management protection	21%
Malware analysis and reverse engineering	21%
Security appliances troubleshooting	17%
Installation, integration and testing of security appliances	17%
Application security development	17%
Audit and compliance	13%
Cryptography, encryption and key management	8%
Other	25%

Note: These percentages are based on responses by 24 individuals

Table A2

Most Valued Non-Technical Skills	% of Respondents
Verbal communication skills	88%
Problem-solving and critical thinking	88%
Attention to detail	83%
Written communication skills (including technical and non-technical report writing)	67%
Adaptability	63%
Performing while under stress	63%
Teamwork and leadership skills	58%
Customer service skills	54%
Risk analysis	25%
Data analysis or data science	25%
Project management	25%
Threat modelling	13%
Other	13%

Note: These percentages are based on responses by 24 individuals

Table A3

Most valued cybersecurity certifications for entry-level roles	% of Respondents
GIAC Security Essentials Certification (GSEC)	54%
GIAC Certified Incident Handler (GCIH)	46%
CompTIA Security +	46%
GIAC Certified Intrusion Analyst (GCIA)	25%
CompTIA CyberSecurity Analyst+ (CSA+)	25%
Certified Information Systems Security Professional (CISSP)	8%
EC-Council Certified Network Defender	0%
EC-Council Certified Security Operations Center Analyst	8%
EC-Council Certified Ethical Hacker (CEH)	17%
GIAC Security Expert (GSE)	8%
GIAC Security Leadership Certification (GSLC)	0%
CompTIA Advanced Security Practitioner (CASP)	8%
Certified Information Systems Auditor (CISA)	4%
Certified Information Security Manager (CISM)	0%
Cybersecurity Practitioner (CSX-P)	0%
SSCP Security Administrator	8%
Offensive Security Certified Professional (OSCP)	17%
Other	4%

Note: These percentages are based on responses by 24 individuals

Table A4

Most Valued Programming and Scripting Languages at Present	% of Respondents
Python	63%
Shell	42%
JavaScript	33%
LINUX	33%
Java	29%
C++	13%
Ruby	13%
C	8%
PHP	8%
Perl	8%
Pascal	0%
Other	13%
Don't know / Not sure	33%

Note: These percentages are based on responses by 24 individuals

Table A5

Cyber Talent Recruitment Challenges	% of Respondents
Cybersecurity incident responder	29%
Cybersecurity operations analyst	29%
Cybersecurity or information systems security manager	21%
Penetration tester/analyst	21%
Identity management and authentication specialist	17%
Cyber architect	17%
Cyber engineer	17%
Cyber threat intelligence specialist	17%
Secure software engineer or developer	17%
Security automation engineer or analyst	13%
Vulnerability assessment analyst	13%
Cybersecurity operations technician	13%
Data privacy specialist	8%
Digital forensics analyst	8%
Operations technology security analyst (e.g., ICS, SCADA, etc.)	8%
Cybersecurity sales specialist	8%
Senior Level roles, including Chief Information Security Officer, Chief Information Systems Security Officer and others	8%
My organization has not had any difficulty hiring for any cybersecurity roles	8%
Cryptographer/Cryptanalyst	4%
Security testing and evaluation specialist	4%
Security administrator	4%
Cybersecurity customer service representative	0%
Network security operator	0%
Information security auditor	0%
Other	29%

Note: These percentages are based on responses by 24 individuals

Endnotes

1 The 2021 KPMG report also states: “while 73% say they are well prepared for a future cyber attack, 59% of businesses surveyed say they are only ‘somewhat confident’ in their ability to detect and respond to a cyber attack.”

2 This is defined in the (ISC)² study (2021) as the number of additional professionals that organizations need to adequately defend their critical assets.

3 According to a report by Cybersecurity Ventures, the number of unfilled cybersecurity jobs worldwide grew 350% between 2013 and 2021, from 1 million to 3.5 million, and researchers predict the same number of openings in 2025 (Lake, 2022).

4 These cybersecurity leaders or HR professionals were in regular contact with the ACTP team for more than six months at the time of the survey, and their organization had made at least one hire from the ACTP.

5 All figures in this report are based on this research unless otherwise noted.

6 Four out of 23 employers agreed to be contacted for an interview, and we spoke with two individuals that belonged to the same organization.

7 The invitation to respond to the survey was sent out by the ACTP program team, and the survey was in the field for around four weeks, during which time the team sent out three reminders.

8 Most of the questions in this survey were multiple choice where respondents could select multiple response options. Therefore, the percentages in the figures presented in this report do not add up to 100%, but rather represent the proportion of respondents that selected a given response.

9 Out of 49 individuals who received the survey, 47% (23/49) completed it and 4% (2/49) partially completed it.

10 To assess the degree of alignment between employer and candidate perceptions of candidates’ top factors when looking for a job, Blueprint will ask participants of the ACTP a similar question. We will share these findings in the final report to be published next year.

11 A 2021 survey of hiring managers in Canada revealed that 93% say they allow entry- and junior-level cybersecurity team members career development time during work hours ((ISC)², 2022)).

12 The Catalyst’s key employment partners are security services organizations. Therefore, it was always likely that most organizations who completed this survey would need Protect and Defend roles. As such, these findings may not represent the broader needs of the cybersecurity sector more generally.

13 While still far from the high demand seen for Protect and Defend, the category of Design and Development is currently in demand (38%) and will continue to see demand over the next three to five years (43%). This category includes roles such as secure software developers, security architects, security engineers and systems analysts. (TECHNATION, 2022)

14 Due to a programming error, “Identity Access Management” was accidentally excluded as a response option for this question.

15 Respondents that answered "yes" to whether technical skills their organization looks for will change in the next three to five years could write in their responses to indicate the skills: the most common responses were Cloud (36%) and DevSecOps and SecOps (29%).

16 While relatively less valuable, written communication skills (including technical and non-technical report writing) can also help employers distinguish among strong candidates (67%).

17 The Catalyst team, in engaging with employers in the Industry Advisory Council (See Page 19), had previously identified a lack of accurate job descriptions as one of the challenges facing the cybersecurity industry. The Blueprint team added an open-ended question for employers: "Based on your experience, what barriers might prevent organizations from creating accurate job descriptions for entry-level cybersecurity roles?"

18 Both interviewees we spoke to indicated that while there are no specific quotas for hiring BIPOC and/or women and BIPOC cybersecurity professionals, their organization monitors the percentage of individuals in their cybersecurity workforce belonging to each of these groups. Based on these percentages, their organization develops diversity targets that aim to achieve parity within their teams, such as having a 50/50 ratio of men to women.

19 About 17% selected Unsure when asked: "To date, has your organization encountered challenges in recruiting and hiring BIPOC and/or women?"

20 This option included people management standards and regulations, including Human Rights Code and Anti-Harassment/Discrimination legislation.

21 We used a two-pronged simultaneous approach to target the widest range of employers possible. First, we obtained access to a database created by CyberDB (a research platform), where we targeted 95 organizations that provide cybersecurity services and consulting. Over 50% of employers we reached out to were small businesses employing between 1–50 people and the 95 individual contacts were senior-level executives such as CEOs and presidents. While the aim was to get a broader representation of employers in Canada, this cold calling approach was not successful in obtaining responses. Second, the ACTP team created a list of individual contacts in 85 organizations with whom they have emerging relationships (these are a combination of their personal and professional contacts). The ACTP team sent out email invitations to these contacts, posted the survey link on social media (LinkedIn and Facebook) and encouraged their contacts to further forward the link to others that met the eligibility criteria. In this report, we present preliminary findings based on responses up until July 19, 2022.

22 Globally, it was estimated that 3.5 million cybersecurity jobs went unfulfilled in 2021. In the US, 50% fewer candidates are available than are needed in the cyber field (PwC, 2022).

23 To help fill certain high-demand roles, Deloitte Cyber developed a train-to-hire program that trains candidates in cybersecurity topics to fill jobs they wouldn't traditionally be qualified for (Lake, 2022).

Future Skills Centre

Blueprint