MAY 2025

CyberTowns Report

PREPARED BY
Canadian Cybersecurity Network

ccn

IRON SPEAR

Contents & Contributors

Contents & Contributors

Introduction

by François Guay

CyberTowns 2025–Building Canada's Cyber Future, One Community at a Time

In 2024, the Canadian Cybersecurity Network launched the inaugural CyberTowns report, a data-driven ranking of the top places in Canada to live and work in cybersecurity. That edition drew on Statistics Canada data and a nationwide CCN survey, using factors like affordability, job availability, education, and quality of life to spotlight emerging cybersecurity hubs across the country.

This year's edition, CyberTowns 2025 takes the project to the next level.

Rather than focusing solely on where to live and work, this year's research asks why certain communities are succeeding and how they are doing it. We explore what Canada's top cybersecurity cities are doing on the ground to attract, retain, and grow talent and businesses. The report examines the ecosystems that support innovation from workforce training and startup support to government collaboration, research infrastructure, and inclusive economic development strategies.

What makes this project especially powerful is that it is rooted in the communities themselves. Each city profile is developed in partnership with local cybersecurity leaders, who serve as researchers, writers, and community ambassadors. This ensures the report reflects not just statistics but real-world insight from the people shaping Canada's cyber future.

Why This Matters Now

As cybersecurity becomes a defining issue for global competitiveness, national security, and digital resilience, Canada must ensure its communities are equipped to lead. Cybersecurity talent is increasingly mobile, and companies are choosing where to invest based on the strength of local ecosystems. In this context, the CyberTowns project is more than a research report; it is a roadmap for building the environments where people, innovation, and opportunity converge.

To protect our national way of life, we must ensure Canada remains a magnet for cybersecurity professionals, students, entrepreneurs, and companies. That will not happen by accident, it will happen through intentional investment in communities. Cities are where innovation is tested, talent is developed, and cross-sector partnerships take shape.

Each city profile is developed in partnership with local cybersecurity leaders, who serve as researchers, writers, and community ambassadors.

Equally important is the need for national collaboration. Cybersecurity success requires education providers, local governments, provinces, the federal government, and industry to work together. When post-secondary institutions align with employer needs, when public funding supports innovation, and when industry shares insight with policymakers, the entire ecosystem accelerates. CyberTowns showcases what's possible when that alignment is done right.

What's Next

Going forward, CyberTowns will become a biennial project, blending the strengths of both approaches: the quantitative rankings from 2024 and the qualitative community ecosystem analysis featured in 2025. This new hybrid model will allow us to both benchmark progress and inspire action.

Final Thought

This report comes at a critical time. The world is in a cybersecurity arms race, and nations that cultivate local excellence will shape the global landscape. Canada does not need to pay the most or be the biggest to become the home of the world's best cybersecurity talent. It just needs to create the best communities where people, technology, and families thrive together. CyberTowns is our contribution to that vision.

Executive Summary

The Blueprint for a Cyber-Secure Canada

Canada's cybersecurity future isn't just being written in boardrooms or classrooms; it's being built in its cities. Across 12 CyberTowns from coast to coast, this report uncovers a vibrant and distinctively Canadian model for cyber innovation: one grounded in world-class education, a deep talent pool, urban livability, and a collaborative national spirit.

Canada's City-Driven Cyber Advantage

Each city profiled, Calgary, Edmonton, Fredericton/Moncton/Saint John, Halifax, Montreal, Ottawa-Gatineau, Quebec City, Toronto, Vancouver, Victoria, Waterloo, and Winnipeg brings its own flavor to the national cyber ecosystem. Yet common threads emerge:

- **Talent-Powered Ecosystems:** From Fredericton's early bet on cyber education to Waterloo's academic-corporate integration and Ottawa's/Gatineau's huge tech workforce, talent is the lifeblood of Canada's cyber strength.
- **Education That Delivers:** Institutions like SAIT, Concordia, UVic, NAIT, and the University of Waterloo lead programs with near-immediate job placement, while cities like Halifax and Winnipeg emphasize work-integrated learning and co-op pipelines.
- **Quality of Life That Retains Talent:** Canada's livability is a strategic asset. Victoria offers "the best of both worlds" with nature and tech; Calgary and Edmonton win on affordability and family-friendliness; Vancouver and Montreal deliver urban vibrancy; and smaller cities like Fredericton and Halifax provide community without compromise.
- **Inclusive, Diverse Workforces:** Cities emphasize representation and access Toronto's ElleHacks, Calgary's newcomer pathways, and Halifax's bilingual workforce show how diversity fuels innovation. In Montreal, leading voices like Olivier Bilodeau (NorthSec & MontreHack) have built a globally respected hacker culture: "Events like MontreHack, NorthSec, and OWASP Montreal aren't just conferences. They're talent incubators." This community has helped launch cyber careers and positioned Montreal as one of Canada's premier technical talent hubs." Quebec City combines cutting-edge research with French-language educational leadership. While close ties between Université Laval and the provincial government drive cyber innovation in public sector systems, making it a model for local cyber-government collaboration in Canada.
- **Strong Community Fabric:** Cybersecurity isn't siloed. Each city hosts thriving ecosystems of meetups, CTFs, accelerators, and innovation zones, where government, industry, and academia intersect daily.

Emerging Challenges

Despite momentum, challenges persist:

- **Talent Gaps at the Mid-Senior Level:** Cities like Winnipeg and Calgary are flush with junior talent but struggle to retain or attract seasoned professionals.
- **Housing & Affordability:** Vancouver and Toronto risk losing talent to U.S. hubs due to cost of living and housing shortages.
- **Capital Flight & Startup Pressures:** Many founders cite limited Canadian investment appetite as a barrier to scale, pushing them south for funding.
- **Credentialing Barriers for Newcomers:** Immigrants in multiple cities report systemic delays in having cyber-related qualifications recognized.
- **AI Disruption:** Automation and generative AI are changing the hiring landscape squeezing entry-level roles and increasing demand for niche expertise.

The Opportunity Ahead

The CyberTowns report makes one thing clear: Canada's cyber strength is local and national. Its future lies in doubling down on this unique city-powered model supporting community-based growth, investing in applied learning and micro-credentials, and creating seamless pathways from classroom to SOC. Done right, this approach can position Canada not just as a player but a global leader in cybersecurity.

Calgary: A Proud Local's Perspective

by Tim McCreight

Why I'm here

I moved to Calgary over a decade ago, to grow my career and experience what this city has to offer. I'd come to Calgary many times over the years to visit friends and family, and occasionally for work or conferences. I was always fascinated by the beauty and strength of this city. The allure and draw of Calgary finally convinced me to head south down Highway 2 and make it my home.

I can see the Rockies to the west of me when I go for a run, beckoning me to get in my car and drive the hour into the mountains. I feel the purpose and pride of our business community when I journey through the pedways of downtown Calgary. And I feel the sense of community when my wife and I walk the dogs every day, see kids playing in our parks, and watch families bring out lawn chairs to join their neighbors on driveways and front yards.

It was one of the best decisions I've ever made in my personal and professional life, moving to Calgary. I'm proud to write about our city and why I feel Calgary is the place to grow your career, help others through their cybersecurity journey, and give back to an amazing community.

My hometown

With a population of over 1.3 million,[1] the city thrives as the energy capital of Canada. The technology sector is evolving quickly as well, surpassing expectations according to recent data from Calgary Economic Development.[2]

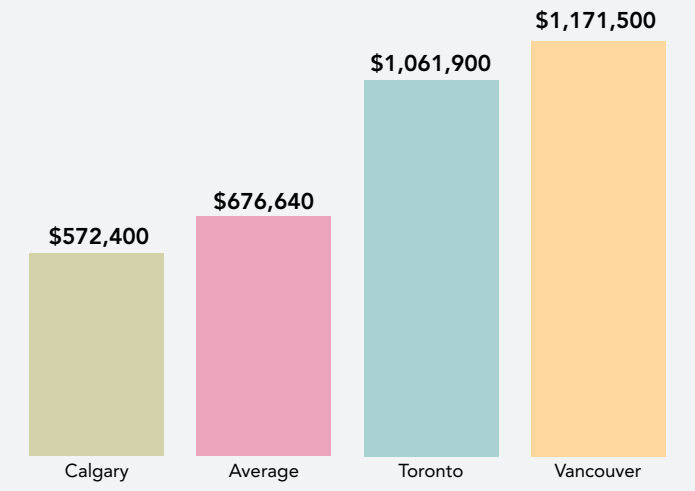
As Calgary continues its journey to become the prominent technology hub in Canada, cybersecurity plays an integral role in the overall success of an organization, which is evident across all industry sectors. A recent report published by the Coldwell Banker Richard Ellis (CBRE) consulting division highlighted Calgary as the only Canadian city in its regional spotlight of global cybersecurity markets.[3] We're showing the world that our city is a place where you can grow your career and become part of a thriving and supportive cybersecurity community!

According to the CBRE report, Calgary's cybersecurity community boasts over 4,400 professionals and has grown more than 44% since the previous report. The energy sector is recognized as a major employer of cybersecurity talent, with a particular emphasis on critical asset and operational technology security.

Calgary's population profile highlights its diversity. The city has experienced an incredible population growth with a 25.1% increase over the past 10 years.[4] Calgary is home to 165 languages, over 240 cultural origins and permanent residents from more than 100 countries, the city is proud to be one of Canada's most diverse metropolitan centres.[5]

Calgary's economic indicators reflect the growth of the city and the resilience of its economy. Calgary's inflation rate for December 2024[6] was 2.4%, lower than the national average and down from November 2023. The average residential home price was $572,400 in Calgary as of December 2024, a slight increase from the prior year. The average Canadian home (all regions) was listed as $676,640 – positioning Calgary as more affordable compared to other metropolitan regions like Toronto ($1,061,900) and Vancouver ($1,171,500).

How Calgary's Housing Prices Compare Nationally



Source: The Canadian Real Estate Association (CREA)

Celebrating Our City

Every year, Calgary hosts a diverse array of annual festivals and events that celebrate our rich cultural heritage. We pride ourselves on showcasing artistic expression, community spirit, and appreciating our historical roots.

Since 1912, "The Greatest Show on Earth," the Calgary Stampede, has taken place every July and reflects the spirit and community of the city. The Stampede has become a symbol of Calgary's resilience and is one of the city's largest economic drivers. In 2024, Calgary celebrated a major milestone by welcoming nearly 1.5 million visitors to the Stampede Park,[7] breaking all attendance records.

We're not just about cowboys and horses! Calgary's Folk Music Festival draws musicians from across the world to Prince's Island in late July, showcasing an eclectic mix of music genres, workshops, and family events.[8] A new venue for the city's professional hockey team[9] along with plans for the revitalization of its Arts Common[10] district, will ensure the vibrancy of Calgary's downtown and its arts community for years to come.

We also celebrate science, film, and education. The Calgary International Film Festival (CIFF)[11] brings together artists and films from over 40 countries every October, showcasing an incredible array of talented filmmakers, production companies, and the artists bringing the films to life. Beakerhead[12] is a multi-day festival fusing art, science, and engineering with exhibits, entertainment, and workshops to promote science education in unique ways. Sponsored by TELUS Spark Science Centre, Beakerhead is an opportunity to bring STEAM (science, technology, engineering, art, mathematics) to everyone in Calgary.

Calgary cares about diversity, equity, and inclusion. We celebrate Calgary Pride every October and promote our collective journey to "create spaces that ensure 2SLGBTQ+ belonging and celebration."[13] Our GlobalFest cultural celebration is another way we embrace the diversity of our city. Since 2003, GlobalFest[14] has promoted Calgary's cultural diversity by showcasing different cultures, ethnicities, and artistic expression. The fireworks competition is one of the highlights of GlobalFest, along with creating safe spaces for collaborative discussions around racism, discrimination, and global justice.

Where We Work

The growth of cybersecurity roles in our city continues to increase, demonstrated by the number of cybersecurity positions posted in 2024. As reported by the Canadian Cybersecurity Network[15] in August 2024, Calgary had 298 postings related to cybersecurity roles across both public and private sectors. The growth of the city's technology innovation hubs and the influence of the energy sector are driving the demand for cybersecurity professionals.

Throughout 2024, several Calgary businesses posted for cybersecurity expertise, ranging from entry level analysts to Chief Information Security Officers (CISOs). A partial list of organizations focused on building their cybersecurity teams includes:

- UFA Co-Operative Ltd.
- iON United
- Canadian Natural
- Neo Financial
- Enerflex Ltd.
- WBM Technologies
- Precision Drilling Corporation
- Trans Mountain
- The Calgary Airport Authority
- Pason Systems Corp
- The City of Calgary
- Wolf Midstream
- TransAlta Corporation
- Enbridge
- Mobia Technology Innovations

Troy Davidson, CISO for the Southern Alberta Institute of Technology (SAIT) has seen exponential growth with SAIT's cybersecurity team over the past 18 months. "We've doubled our team size and are spending more time identifying risks and communicating across the organization." Troy has taken the time to focus his attention on developing a risk-based approach to cybersecurity. The benefits of this management philosophy are clear in the growth of his team and their ability to select a managed security service provider to bring their protection program into a 24/7 operation.

Ashif Samnani, the Cyber Security Practice Lead at Mobia Technology Innovations notes that his team "has grown from 3 to 15 people in less than two years." That amazing growth can be attributed to the changes in the regulatory environment impacting Calgary-based organizations and a greater understanding of the marketplace in Calgary and Western Canada.

Cara Wolf is an industry expert in cybersecurity and is the CEO of Ammolite Security,[16] an award-winning Calgary-based cybersecurity firm. Cara's firm specializes in Cybersecurity Maturity Model Certification (CMMC) assessments, Canada's Cyber Protection and Certification for Secure Contractors (CPCSC) compliance, and zero-trust encryption. "The future of cybersecurity in Calgary is set for rapid growth as industries adopt AI-driven security solutions, zero-trust frameworks, and quantum-resistant encryption" states Cara. "With increasing cyber threats targeting critical infrastructure and supply chains, businesses must prioritize proactive defense strategies, regulatory compliance, and next-generation technologies. Calgary is poised to be a key player in strengthening national and global cyber resilience."

Where We Learn

Calgary's post-secondary institutions are providing much-needed education

programs focused on cybersecurity. Every post-secondary institution in Calgary offers education in cybersecurity, from cybersecurity specialist certificates to master's degrees in privacy and cybersecurity, and everything in between! The variety and depth of programs offered by post-secondary institutions in cybersecurity highlights the importance of continuing cybersecurity education.

SAIT has invested time and resources to provide a diverse array of security training at the degree, diploma, and certification levels. Carla Marioni, SAIT's chair of Cyber Security in the School for Advanced Digital Technology was quoted as saying "…the role of cybersecurity has never been more essential to empower progress and safeguard the future of business and technology."[17] SAIT's programs include a Bachelor of Technology in Cybersecurity; an Information Systems Security diploma program; an information security analyst certificate; a cybersecurity for control systems certification, and a certification program for cyber security analysts.

Bow Valley College's (BVC) Cybersecurity Post-Diploma Certificate program[18] has seen success in the Calgary market. One area of growth is within the financial services sector, which is atypical for Calgary. Tony Wigglesworth, Associate Dean with the School of Technology at BVC states that "financial services in Calgary is growing its reputation, and Bow Valley's work (in) integrated learning program(s) is a real plus for local organizations." Financial institutions in Calgary have benefited from the work of BVC graduates, helping organizations with specialized programs like Identify and Access Management.

The University of Calgary's Master of Information Security and Privacy (MISP)[19] is the first in Canada to be designated as an International Academic Partner (IAP) by the International Information Systems Security Certification Consortium (ISC2). This master's level program allows students to complete two certificate education programs before advancing to the Master's classes, preparing them to tackle the prestigious CISSP designation sponsored by ISC2.

Michael Primeau, an instructor for MISP at the University of Calgary, has seen increasing demand for the program. "Our enrollment has increased from one cohort of 20 students to two cohorts. There is an opportunity to grow to three cohorts by 2027." As a past guest lecturer at this program, I can attest to the calibre of the students, and their desire to begin giving back to the community. I always feel re-energized after I spend time with Michael and his students!

There are other institutions offering cybersecurity programs at educational institutions across Calgary. These include the Cybersecurity Specialist program at CDI College, Mount Royal University's Cybersecurity Fundamentals Certificate and Advanced Cybersecurity Certificate, and ABM College's Cybersecurity Diploma.

Other organizations provide tailored or specialized training programs to facilitate continuing professional education opportunities, supporting existing cybersecurity certifications. These include courses offered locally through ISC2, ISACA, and SANS Calgary chapters.

Innovation is Key

Calgary's innovation community is driving demand for cybersecurity professionals. A recent announcement from Fortinet regarding its $30 million investment in a cybersecurity technology hub[20] demonstrated the recognition of Calgary as a leading player in the global cybersecurity space. Fortinet's investment will bring 165 new cybersecurity jobs to Calgary, adding to the city's reputation as a nexus for cybersecurity innovation and services.

A recent announcement from Fortinet regarding its **$30 MILLION** investment in a cybersecurity technology hub demonstrated the recognition of Calgary as a leading player in the global cybersecurity space.

The city's cybersecurity is steadily expanding, thanks in part to the expanding business community and increased investment in technology startups. Innovators and incubators are actively involved, from identifying opportunities for further investment in local firms, to attracting prospective life-science companies, ensuring Calgary remain a top destination.[21]

The Opportunity Calgary Investment Fund (OCIF) was established in 2018 and focuses on diversifying Calgary's economy, developing opportunities to train entrants to new

technologies and markets, and generating national and global interest in Calgary's growing economy.

Platform Calgary[22] is concentrating on growing relationships within Calgary's technology ecosystem. This organization serves as a foundation for innovation, offering programs and services to companies in various stages of their startup journey. In June 2022, Platform Calgary celebrated the opening of its 50,000-square-foot facility in downtown Calgary. Since then, it has increased its program uptake and local business support.

M-Tech Innovations[23] is another technology incubator headquartered in Calgary that helps software startups sell their products to enterprise clients. The incubator helps new companies seek out and obtain federal funding for their products, as well as gain access to marketplaces in Canada and North America. M-Tech has also partnered with venture capital firms to provide access to different rounds of funding to new technology startups.

Key industry partners are increasing their presence in the Calgary marketplace.

Techterra, a Calgary-based not-for-profit geomatics support centre, recently announced a significant investment in post-secondary geomatic technology programs.[24] Two of the four educational institutions are in Calgary – the University of Calgary, and SAIT.

Key industry partners are increasing their presence in the Calgary marketplace. Calgary has become a hub for autonomous systems, ranging from autonomous vehicles as a service (AVaaS) to systems integration and component manufacturing.[25]

Partnerships in innovation has also grown, a perfect example is the Canadian Cyber Assessment, Training, and Experimentation Centre (CATE), which is managed by ENFOCOM Cyber organization.[26] ENFOCOM, a Calgary-based training centre for law enforcement agencies, operates through a public-private partnership between the Calgary Police Service, the University of Calgary, and ENFOCOM itself. This partnership led to the creation of CATE and a state-of-the-art training facility that includes a cybersecurity range. The "range" offers realistic scenarios for law enforcement members to practice hands-on cyber security skills. The range gives participants an opportunity to understand how cyber intrusions are launched and detected, attack patterns and methodologies, as well as intelligence collection relating to tactics and capabilities of cyber threat actors.

The CATE Centre offers a strong curriculum in cybersecurity, developed in concert with members of the Calgary Police Service and other law enforcement agencies from across Canada. The Centre creates opportunities for University of Calgary students in the cybersecurity program to participate in training exercises and "range" activities, providing a one-of-a-kind experience for university students.

The team at ENFOCOM and Cate Centre, in partnership with CyberAlberta, has recently expanded their educational offerings to high schools across Alberta, including a Capture the Flag event in April 2025, over 50 high schools are expected to participate. There will be ten 5-member teams participating in the event, giving high school students a chance to experience what cybersecurity professionals focus on everyday. "We want to involve as many high school students as possible, getting them ready for the workforce" states Herbert Fensury, founder and CEO of ENFOCOM. "We want to create a better way for law enforcement agencies and industry to work together during an incident." This progressive approach to collaboration across industry, academia, and law enforcement demonstrates how complex problems in the Calgary cybersecurity community are solved.

Growing cybersecurity in Calgary

Calgary's economy features several dominant industries, and these drive much of our cybersecurity workforce requirements. The energy sector, particularly oil and gas, is a cornerstone of Calgary's demand for security talent. The oil & gas industry is critical to the economy and faces constant cyber threats as high-value targets, from state-sponsored espionage to ransomware attacks. As a result, large energy corporations based in Calgary have built robust cybersecurity teams to safeguard operations and data.

Protecting industrial control systems, pipelines, and supply

chain data requires specialists in operational technology (OT) security and risk management. This has led to increased hiring of cybersecurity professionals with knowledge of industrial systems and critical infrastructure protection. Energy companies often seek experts in areas like network segmentation, incident response for ICS/SCADA systems, and threat intelligence focused on nation-state actors. Given high-profile cyber incidents (for example, the 2023 Suncor breach in Canada's oil sector), security investment in Calgary's energy industry has only increased.

I can attest to the growth of cybersecurity teams across Calgary these past 10 years, having been a security executive in oil and gas, transportation, and the public sector. The ongoing investment in cybersecurity programs is necessary because the threats to critical infrastructure, public services, and transportation continue to grow.

Calgary boasts an enviable lineup of cybersecurity conferences.

The financial services industry is another key driver of cybersecurity jobs in Calgary. While Toronto is Canada's financial hub, Calgary hosts significant financial operations (regional bank offices, investment firms, fintech startups, and headquarters of Alberta's financial institutions). The financial sector faces a surge in cybercrime and fraud attacks. In 2022, digital fraud attempts in financial services were up 20%.[27]

Canadian banks are among the top global targets for cyber-attacks. To strengthen its cybersecurity teams, these organizations seek analysts to combat fraud, security architects to secure online banking platforms, and compliance specialists to meet strict regulations (like PCI-DSS for payments or OSFI cyber guidelines for banks). In response to the increasing threat of fraud, the financial sector has maintained strong cybersecurity hiring to project data and assets.

Many financial firms also require talent in identity and access management, security monitoring, and encryption to safeguard transactions – these specialized roles are in demand locally. As noted earlier, we learned how Tony Wigglesworth and the team at BVC identified this need and collaborated with local financial institutions to create specialized training and learning programs.

Beyond energy and finance, other industries in Calgary contributing to cybersecurity employment include healthcare, telecommunications, and government. Calgary's healthcare sector (hospitals, health authorities, biotech companies) manages sensitive personal health information and has been investing in security to protect patient data – this drives demand for cybersecurity analysts and compliance officers who are familiar with health data privacy. In fact, Calgary's overall job postings reflect the presence of major enterprises in natural resources and healthcare fields.[28]

On compensation and total salary of cybersecurity professionals, Calgary ranks in the top ten for overall cybersecurity salaries based on data from GetGIS.org[29] with a median annual income of $88,278. Mid-career cybersecurity professionals can often earn between $80,000 and $100,000 annually, while senior leadership roles can exceed $200,000 in annual compensation for seasoned cybersecurity professionals.[30]

Some of the most sought-after skills include cloud security, forensics, blockchain security, AI and IoT security skills. Calgary's strong oil and gas infrastructure reflects these skills as energy companies continue to face ongoing threats against their operational technology infrastructure. Local tech hubs are focusing on blockchain and AI to help new startups gain market share.

Our strength – The Calgary Cybersecurity Community

Calgary boasts an enviable lineup of cybersecurity conferences, meetings and in-person meet ups throughout the year, from major multi-day conferences, to local cybersecurity meet-ups and chapter events. If you're looking for an opportunity to network with fellow security professionals and gain a greater understanding of cyber risks, Calgary is a great place to be!

In June 2024, Calgary hosted the second annual Cyber Security for Critical Assets (CS4CA) security summit.[31] This event united senior security leaders from energy, utilities, oil & gas, mining, health, and transportation sectors. Over 45 expert speakers presented, including the CISOs from BHP, NAV Canada, the Government of Alberta, Edmonton

International Airport, and the Canadian Centre for Cyber Security. The conference was sponsored and supported by industry vendors like Fortinet (official lead sponsor), IBM Security, and a roster of OT security companies. This strong sponsorship underscored the focus on protecting industrial and critical systems from evolving threats.

Sponsored by Evanta,[32] the Calgary CISO Executive Summit, held June 18th, 2024, was a one-day, invitation only conference. This in-person summit convened Calgary's top CISOs and CIOs to discuss strategic cybersecurity challenges in an interactive forum. Discussions focused on high-level themes like improving operational cyber efficiency, enabling data-driven security decisions, and leveraging AI securely. All topics were chosen by a local governing body of senior IT executives (including the City of Calgary CIO and CISOs from energy and retail companies). This summit highlighted leadership priorities and allowed security executives from industry and government to share insights in a private setting.

2024 marked a strong return to face-to-face conferences and meetups.

BSides Calgary,[33] in addition to being one of the city's flagship events, is also a community effort. BSides Calgary describes itself as a "high caliber gathering for information security professionals, hackers, coders, students and the greater tech community." The 2023 event (the data most currently available) highlighted over 40 speakers, 700 onsite attendees and 800 registrants. The organization created a not-for-profit foundation, manages several online social media groups, and offers an online job board for local security roles.

Given Calgary's strong oil & gas and utilities sector, there's a vibrant community around industrial control systems (ICS) security. The Calgary Cyber Security for Control Systems meetup (part of the global (CS)²AI association) connects professionals responsible for SCADA/OT and critical infrastructure security.[34] Over the last 18 months, this group has hosted numerous sessions focused on operational technology threats. Some events are local roundtables, including a March 2025 in-person meetup that discussed product lifecycle security & certification for industrial systems.

The Calgary Security Professionals Information Exchange (SPIE)[35] began in 1988, when a group of information security professionals began meeting every second month to share issues, concerns, and potential solutions to the nascent field of information (now cyber) security. In 2003, SPIE registered to become a not-for-profit society in Alberta, the first board of directors' elections followed in 2004.

Other events are virtual, such as (CS)²AI symposiums featuring international experts. The Calgary chapter recently hosted a symposium in March 2025 on electric-sector cybersecurity with participants from across Canada. The ICS group enjoys sponsorship from specialized OT security companies (Fortinet, Waterfall Security, etc.) and an organizer network of global experts (the chapter is co-run by Derek Harp, founder of (CS)²AI). These meetups provide a forum for sharing best practices in securing energy infrastructure, and often include presentations, panel Q&As, and even happy hour networking for the OT security crowd.

Calgary's homegrown cybersecurity companies have stepped up as well. iON United, a cybersecurity services firm based in Calgary, has been a prominent sponsor of the Calgary Cyber Summit (managed by the Calgary Police Service). As part of their sponsorship, they hosted a reception and contributed panelists, showcasing local expertise. Other local firms like Sable Lion (a Calgary cybersecurity startup) and Subnet Solutions (industrial network security) have supported events targeting the energy sector. And SecuredNet,[36] a local security company founded in 2006, continues its ongoing relationship with BSides Calgary as a Gold Sponsor for this year's event.

Having local sponsors is crucial, they bring a regional perspective and often recruit local talent through these forums. This period also saw Calgary's tech incubators and innovation organizations (Platform Calgary, for example) partner in small cybersecurity boot camps and competitions, further bolstering the ecosystem.

2024 marked a strong return to face-to-face conferences and meetups. We saw how BSides Calgary adapted during the pandemic, sold out its first fully in-person conference in 2023, and grew yet again for its 2024 event. This trend was echoed across other events – the Calgary Cyber

Summit, CS4CA, and iTech were all on-site, and each saw lively attendance and networking buzz that simply can't be replicated online.

The benefits of in-person format are clear: networking during coffee breaks, live demos from socials vendors, and serendipitous knowledge exchange. Calgary's social meet-ups also flourished with in-person formats – after moving online in 2020–21, groups like YYC Local resumed physical gatherings at breweries and offices, which dramatically increased participation.

Longtime professionals have noted that these face-to-face interactions build trust and camaraderie, strengthening the community's cohesion (as evidenced by feedback after BSides 2023, which was praised as "engaging" and community-building).

Challenges We Face

With all the positivity we experience in Calgary, we still face obstacles and issues that are familiar across Canada and the world. The lack of more senior security resources, coupled with the need to strengthen soft skills, creates gaps that organizations are trying to fill.

Terry Ingoldsby, founder of Amenaza Technologies Limited,[38] highlights the need for a greater focus on strategic issues, "we need to be able to look at the bigger picture and understand how business(es) and systems are being attacked, and…the business impact." Cybersecurity is becoming a regular topic of discussion at the C-suite level in organizations, and there needs to be a greater understanding of the IT industry as well as stronger collaboration between post-secondary institutions, cybersecurity teams, and local businesses.

While there are many entrants to the cybersecurity field in Calgary, finding the right resource that will fit an organization's culture and work ethic has been difficult for some. James Cairns, one of the volunteer leaders behind BSides Calgary and the Associate Director of IT Security at BVC described how their latest Governance/Risk/Compliance role "was difficult to fill." While technical knowledge and certifications are evident from applicants, Cairns wanted to ensure that the new team member would be a cultural fit as well. This demonstrates a maturing of the hiring process, a welcome change for many but a new element that must be considered by applicants for roles in Calgary.

Burnout continues to be an ongoing challenge for cybersecurity professionals in Calgary and across the globe. Fortune magazine recently published an article describing the impacts of the stress facing cybersecurity professionals.[39] Changes to recent Alberta Legislation (Regulation 84/2024[40]) and the requirement to ensure critical infrastructure organizations have a holistic Security Management Plan (SMP) are driving additional stress across the Calgary ecosystem. The economic growth attached to the energy sector is now forcing cybersecurity professionals to ensure they can assess risks and adapt their SMP to address them.

At a recent security conference hosted by NKST,[41] this topic filled the entire agenda. I was honoured to be a speaker at the conference and realized how much work this new legislation will bring to the teams managing our energy and critical infrastructure organizations over the next few years. While the goal of the legislation is important, it will have an impact on the work and efforts of cybersecurity teams across Calgary.

A more recent international development – the on again/off again implementation of tariffs on Canadian goods is having an impact on potential hires to cybersecurity teams in Calgary. One interviewee for this report identified that, while new hires for their cybersecurity team were approved, they were going to wait to see what impacts tariffs will have on Calgary's economy. Calgary has been identified as the second most impacted city in Canada by the threat of tariffs from the Trump Administration.[42] While it is still too early to see what direct impacts these tariffs will have on the city's economy, any drop in demand from the energy sector has historically impacted energy companies across Calgary. This decrease creates a negative knock-on effect to other businesses and service providers across the city.

The Journey Forward

Where does Calgary's cybersecurity journey go from here? What do the next five years look like for Calgary and its growing cybersecurity community?

Legislative and regulatory changes to critical infrastructure and energy mean these organizations must ensure they have security programs that can protect the sector from cyber threats. We're going to see greater focus on the development and implementation of security management plans across the energy sector, in turn requiring a well-trained cybersecurity community capable of delivering these programs.

Over the past five years, post-secondary institutions have purposefully developed an array of cybersecurity programs that are focused on different levels of training

while attempting to address industry demands. It has taken time to develop these programs, but Calgary has responded to the challenge, as evidenced by the diverse education and training programs offered across the city. These next five years will hopefully showcase smaller, more targeted "micro" certification programs focused on specific skills as well as addressing legislative and regulatory requirements.

Many organizations now recognize the value of implementing a cybersecurity program or updating the current program to reflect a risk-based approach to security. This awareness as a critical component of success is still new to many organizations, but the impacts of this approach are being felt across the city. One of the services my company provides is developing risk-based programs for organizations. Companies in Calgary are beginning to see how security can truly support the overall success of the organization.

New technologies like AI, large language models, and quantum computing are being assessed for potential security risks across the globe. Businesses in the city are incorporating these technologies into the workplace, and security teams are being called upon to review the potential risks these innovations bring. We are uniquely positioned to address the risks and will see Calgary's security community take up the challenge to find the right balance between productivity and risk.

Our workforce continues to grow and mature, albeit not at the pace we want it to be. Our journey forward must focus on the variety and maturity of skills sought by businesses while finding ways to upskill our current cadre of cybersecurity professionals. This will be key to the ongoing success of Calgary's cybersecurity community – being resilient to market demands, ready to support our organizations, and ensuring legislative obligations are met.

We have seen the city rebound from financial crisis, recover from a historic flood, and bounce back from a global pandemic. Our journey forward will focus on new training programs, increased acceptance of cybersecurity as a business enabler, and greater involvement between public and private sectors. I see our security conferences and events growing, perhaps even eclipsing some conferences from our neighbour to the south.

We don't sit back and reflect on our success – we keep moving forward. I firmly believe that our cybersecurity community will do just that. And we'll create a cybersecurity community that is inclusive, diverse, and welcoming for all who want to help, give back, and grow.

See end notes for this article's references.

Tim McCreight is a visionary leader in the global security industry, with over four decades of experience spanning physical and cybersecurity. As the CEO and Founder of TaleCraft Security, he is a passionate advocate for Enterprise Security Risk Management (ESRM) and has dedicated his career to empowering organizations to build resilient, business-aligned security programs.

CYBERSECURITY CONSULTING,

Minus the Sales Pitch!

Cybersecurity should be about **protecting what matters,** not pushing products. At Iron Spear, we believe in a **partnership-first approach** — one built on expertise, transparency, and real-world solutions.

Here's how we do things differently:

- **No sales teams.** You work directly with experienced security professionals — not someone trying to meet a quota.
- **No vendor affiliations.** We recommend solutions based on what's right for you, not what earns us a commission.
- **Real-world solutions.** Security isn't just compliance checkboxes — it's about practical defenses that actually work.
- **Community-first mindset.** We don't just consult—we contribute, mentor, and advocate for a stronger cybersecurity industry and give back to the communities we serve.

We're here to help you navigate cybersecurity challenges with honest, actionable guidance — so you can focus on what matters.

Find us online:

WWW.IRONSPEAR.CA

IRON SPEAR

BUSINESS & INDUSTRIAL CYBER SECURITY

Cyber Resilience: Building Strength in the Face of Inevitable Threats

by Drew Carmichael, Presented by Iron Spear Information Security

In today's volatile cyber threat landscape, one thing is certain: cyber incidents are inevitable. No matter how robust your defences are, it's impossible to guard against every threat. Cyber incidents have become so commonplace that a large-scale breach involving millions of records may get little to no visibility. What does still draw the attention of the public are poorly handled cyber breaches. An organization that quickly responds to an incident, restores services and makes amends to those impacted is far more likely to emerge from the event unscathed. For those who delay, deny or deflect, the impacts can be much more long-lasting. Some organizations may never regain lost client trust.

Welcome to the era of Cyber Resilience.

What Is Resilience?

Resilience is crucial for navigating life's challenges. Every day, we are all faced with setbacks and stresses that can sometimes feel insurmountable. Resilience provides us with the skills necessary to bounce back from these setbacks – to improvise, adapt, and overcome.

SO, WHAT ARE THE CHARACTERISTICS OF A RESILIENT PERSON?

- **The ability to positively respond** to adversity, adapt to change and maintain a positive outlook despite challenges.
- **A tenacious refusal** to give up in the face of adversity.
- **Self-regulation and managing** emotions during stressful circumstances, and demonstrating flexible thinking to adapt to challenging circumstances.
- **A proactive approach** to problem solving and a willingness to learn from their experiences.

An important aspect of resilience is that it is a learned behaviour. People are not born resilient; they learn resilience over time through practice and experience.

Cyber Resilience

Much like a resilient individual, a cyber-resilient organization is able to respond to challenges with composure and address issues in a structured manner. When faced with a cyber incident, the resilient organization is agile, pivoting when it encounters challenges and always looking for creative ways to solve problems. All the while, it is able to manage heightened emotions and keep its eye on the prize: a restored system, a functioning business process, and limited long-term damage to the reputation and brand of the organization.

A cyber-resilient organization is also able to reflect on an event and look for opportunities to improve. In the case of a cyber incident, this continuous improvement takes the form of "Lessons Learned" activities. Completed as part of the incident close-out, a lesson learned session provides a retrospective assessment of what worked and what didn't work during the incident, looking for opportunities to adjust procedures to leverage these findings to improve the processes.

Cyber resilience also includes taking accountability for the incident and making amends for any damage caused. This would include being truthful in your dealings with your stakeholders. A truly resilient organization doesn't deflect blame or retreat into denial after an incident. Instead, it takes accountability and communicates transparently, learning from the experience.

Cyber resilience is far more than just good cybersecurity hygiene. It's the organizational ability to detect threats quickly, contain and eradicate them efficiently, and restore operations with minimal disruption.

And just like personal resilience, cyber resilience is learned over time, through planning, training, and above all, practice.

The Asymmetric Nature of Cyber Warfare

The first difficult truth that all cybersecurity professionals must accept on the road to cyber resilience is that the cyber threat actor has the upper hand. A lone hacker or a small group can easily launch a very sophisticated cyber-attack against the operations of a billion-dollar company using freely available tools. The defender, on the other hand, must invest heavily in infrastructure, personnel, and monitoring just to keep up with new cyber hacking modes and strategies. Adversaries can attack repeatedly, using advanced tools and stealthy tactics and then retreat into the shadows only to try again and again. Attackers only need to get lucky once. Meanwhile, the defender's job is much more difficult. Their defences must be perfect, every time, and, given the complex nature of the modern IT infrastructure, there are many potential points of weakness that can be exploited. This imbalance is the reality of today's cyber threat environment.

For an organization to truly embrace the cyber resilience ethos, it must first accept the inevitability of a cyber breach. You must hope for the best and plan for the worst.

Limited Cyber Security Resources

Key to planning for the inevitable cyber incident is having ready access to the skilled resources required to respond and recover effectively. Cybersecurity managers face significant challenges in recruiting and retaining skilled cybersecurity. The scarcity of cybersecurity expertise is particularly pronounced in smaller markets, and some organizations may lack the financial resources to employ dedicated cybersecurity personnel. Given the extensive range of cyber threats, it is imperative for organizations to adopt a risk-based approach to threat management which focuses on threats that are most pertinent to their business model, sector, or geographic region.

CYBER THREAT INTELLIGENCE

Effective cyber threat intelligence (CTI) is essential to this focus. A well-tuned CTI program can provide targeted visibility of an organization's unique threat landscape, including those threat actors who are most likely to target it. This visibility helps organizations to anticipate and mitigate threats by focusing on the tools and techniques favoured by these threat actors. This allows the cybersecurity

team more time to focus on configuring and tuning cyber tools to detect and defend against these threat actors in the environment.

Subscription CTI services can assist the cybersecurity team by issuing alerts for missing security patches in the organization's technology stack, which reduces the need for the team to monitor numerous vendor alerts each week. Additionally, CTI services can provide visibility into dark web forums, marketplaces, and other hidden sources that might contain exposed company data or credentials. Advanced CTI services may also monitor social media for references to the company's VIPs that could indicate potential fraud or other illegal activities.

CHAOS MONKEY GOES CYBER

In a move that redefined IT resilience in 2011, Netflix introduced the "Chaos Monkey"—a tool designed to validate the resilience of its IT systems. Netflix understood the critical importance of its IT systems in delivering services and aimed to ensure that these systems could handle unexpected disruptions, like a spiteful monkey with wire cutters getting into the server room. The Chaos Monkey tool was designed to simulate the unexpected. It randomly shut down processes and systems to test if the infrastructure and systems were architected to continue operating, despite these unpredictable disruptions.

In the context of cyber resilience, organizations should adopt similar "chaos engineering" techniques in their cyber incident response planning. Cyber incident response teams are generally quite effective at handling predictable events, such as employees clicking on malicious links or laptops being stolen. These common incidents can be managed using standard playbooks and automation.

The real challenge lies in dealing with unexpected events, the Cyber Chaos Monkeys. These unpredictable incidents are more likely to cause extended outages, significant data exposure, or system integrity issues. To achieve a heightened state of cyber resilience, organizations must reduce the number of Cyber Chaos Monkeys in their environment. By intentionally disrupting systems and testing their cyber resilience, organizations can better prepare for unexpected cyber threats and ensure they are able to maintain critical business operations even in the face of unforeseen cyber events.

"The unexpected blows of fortune fall heaviest and most painfully."

—Seneca

The Roman philosopher Seneca was fond of saying that the unexpected blow lands hardest. We are most likely to be hurt by events that we don't see coming. A cyber-resilient organization spends a significant amount of time considering various threat scenarios and how the organization would respond if faced with them. Organizations must prepare for the unpredictable, not just the expected. Routine incidents like phishing or lost laptops should already be handled via automation and playbooks. But it's the Black Swan events—the true Cyber Chaos Monkeys—that require innovative planning and continuous scenario testing.

This testing should consider all components: people, processes, and technology. It could include penetration tests and Red Team exercises to identify control weaknesses and ensure that detection tools are functioning correctly. It should also include regular cyber incident tabletop exercises to confirm that all incident responders are well-versed in the cyber incident response plan and understand their roles. These exercises should be based on a diverse range of scenarios, both common and rare (such as 'black swan' events), and involve participants from technical, management, and even executive teams.

How Fast Is Fast Enough?

"Slow is smooth. Smooth is fast."

Once the resources have been secured and the threat environment understood, a metric for evaluating the effectiveness of incident response activities must be established. As indicated at the outset, organizations are now being judged less on whether a breach occurred, but on how swiftly and efficiently they responded. The timeline for "acceptable" recovery is highly contextual. Each organization (and potentially each department within the organization) will have a unique recovery time objective, which is the maximum time it can be without its IT systems before experiencing unacceptable consequences. A medical system outage might require a return to service within minutes, while the cafeteria system can afford a few days of downtime. This is why conducting a Business Impact Assessment (BIA) is so critical.

WHAT IS A BUSINESS IMPACT ASSESSMENT (BIA)?

A BIA evaluates how different systems and processes support critical business functions. It helps identify an

organization's "crown jewels." These are systems that must be prioritized during an incident response. Not all systems are created equal. Scare resources should be directed at restoring those systems that are most critical to business operations. Having a structured and regularly tested disaster recovery plan that lays out those priorities will significantly reduce the impacts to critical services and ensure that recovery activities are aligned with business expectations.

PRACTICE MAKES PREPARED

In crisis situations, muscle memory matters. The ability to respond instinctively—not through last-minute improvisation—can be the difference between chaos and control. Organizations should test their incident response plans as often as they test disaster recovery strategies.

A cyber incident response plan must establish the roles and responsibilities during an incident to limit confusion and streamline decision-making. Prior to an event, the incident response team must know: who is authorized to declare an incident, who approves returning a system to operations, and what is an acceptable level of containment. The answers to these questions should be pre-determined and not made in the 'fog of war'.

KEYS TO ACHIEVING CYBER RESILIENCE

1. Prioritize the Mission

Identify and protect the systems most critical to business objectives. Use your BIA to determine where limited resources should be deployed during a crisis.

2. Anticipate Likely Threats

Understand your threat landscape—who's likely to target you, how, and why. Don't try to defend everything; focus on where the risks are real.

3. Shift from "If" to "When"

Prepare for the inevitability of an attack. Use tabletop exercises to simulate unexpected scenarios and expose blind spots.

TLDR: What Defines a Cyber-Resilient Organization?

A CYBER-RESILIENT ORGANIZATION:

- **Accepts the inevitability** of a cyber breach and prepares diligently to respond effectively when it occurs.
- **Takes a risk-based approach** to cyber and directs scarce resources at those threats that are most impactful to the organization.
- **Regularly tests security controls** and incident response processes to validate they are operating as intended and to establish a strong muscle memory.
- **Measures success not by isolation** of the threat, but by recovery aligned with business expectations.
- **Restores systems rapidly** without sacrificing accountability or transparency and keeps stakeholders informed honestly and consistently.

Final Word: The Resilience Mindset in a Cyber World

Cyber resilience isn't just about technology, it's about preparedness, agility, and accountability. It's about building an organization that not only withstands cyber attacks but emerges stronger each time. Just like resilient people, resilient organizations don't crumble under pressure. They adapt. They learn. And they keep moving forward.

The unpredictable nature of cyber threats demands an unwavering commitment to resilience. It's time to fortify your organization against these inevitable challenges and ensure that when the storm hits, you are not only prepared but well positioned to emerge stronger.

"Cyber Resilience is not just about surviving the storm—it's about learning to dance in the rain."

Drew Carmichael is Vice President, Cyber Security for Iron Spear Information Security where he provides both practical and pragmatic advice to his clients to assist them with fulfilling their commitments around the protection of sensitive data. Drew previously held the role of Chief Information Security Officer for Canada Life. Drew has over 25 years of IT experience in the financial services industry in Canada and Europe with the past 15 years focused exclusively on technology risk management with a specialty in Cyber Security risk.

IT issues?

Solutions at the press of a button.

Hit F12 on your own keyboard and get the smooth, worry-free IT your business deserves—without major distractions slowing you down. Enjoy instant IT support for immediate help solving issues. Advanced cybersecurity that prevents threats before they happen. Clear, transparent costs that bring calm certainty to your budget, with no hidden surprises. And scalable solutions that grow seamlessly alongside your business.

One button does it all. GetInfinite.ca Reach out to us today.

F12.net™

Edmonton: Cyber Gateway of the North

by Curtis L. Blais

Picture this—a city buzzing with opportunity, where students, researchers, and industry leaders converge to tackle some of the most pressing challenges in digital security.

This is Edmonton.

Preface: The Cybersecurity Community

The scene unfolds like the pages of a cherished novel, accompanied by the warmth of a hot cup of coffee on a cool summer's morning. Nestled along the North Saskatchewan River in central Alberta, Edmonton has always been a city of resilience and innovation. Known for its sweeping prairie landscapes and vibrant cultural scene, it is now making waves in a different field: cybersecurity. Over the past decade, Edmonton has quietly transformed into one of Canada's most promising cybersecurity hubs. This is a story of collaboration, growth, and untapped potential—a story that invites newcomers, professionals, and businesses alike to explore what this city has to offer.

A resolute community of cybersecurity professionals committed to innovation and collaboration. As of 2025, job boards like Indeed and Glassdoor reveal a promising snapshot of the city's potential—dozens of openings for cybersecurity roles, from analysts to compliance advisors, speak to a thriving industry.

Every great story has a setting, and in Edmonton, that setting is built on the foundation of education and collaboration. The city's cybersecurity community thrives because of the institutions and individuals who shape it, each playing their part in writing this evolving tale.

Meet a Few of the Characters

Imagine state-of-the-art labs and classrooms filled with some of the brightest minds in computer science and artificial intelligence, working on groundbreaking research in computing science and related engineering disciplines. The University of Alberta (U of A), ranked #1 in Canada and #6 globally in Impact Rankings by Times Higher Education (City of Edmonton, 2025), doesn't just educate students; it equips them to become leaders in a rapidly evolving field. The U of A boasts Canada's oldest and one of the largest computing science departments, renowned globally for its contributions to both the theoretical underpinnings and practical applications of computing (Invest Alberta, 2025). Through partnerships with industry and government, the university ensures its graduates are ready to tackle the world's most complex cybersecurity challenges. "The cybersecurity community in Edmonton has grown exponentially in recent years" says Michael Spaling, Principal Security Architect for the U of A and recipient of the Queen's Platinum Jubilee Medal for his work in cybersecurity. "The community is made up of an incredibly diverse group of people from all walks of life including age, backgrounds, cultures and thoughts. Everyone is always welcome."

Across the city, the Northern Alberta Institute of Technology (NAIT) is a hive of activity, where students dive into hands-on training that prepares them for the realities of the workforce. With a 93% employment rate within 9 months of graduating from full-time programs and 98% employer satisfaction, NAIT is a solid choice for those looking to join the technology workplace (NAIT, 2025). Programs in digital media and IT with a focus on cybersecurity are designed to meet industry needs, producing graduates who are ready to hit the ground running.

You are in Alberta, a province built on innovation, ambition, and digital possibility. That is where Cybera comes in—the gateway to a smarter, faster, more connected future. As Alberta's research and education network facilitator, Cybera drives the connections that create research breakthroughs, lead collaborations that spark change, and power cybersecurity to keep these initiatives moving forward. They do not just enable digital technology—they advocate for better access to digital tools (and stronger services) to help Albertans thrive in an evolving digital economy. "Our vision is for a connected, secure, and equitable digital future for every Albertan," says Barb Cara, President of Cybera. And they are making it happen. (Cybera Inc., 2025)

Artificial Intelligence is increasingly important in robust cybersecurity, and the Alberta Machine Intelligence Institute (Amii) shines as a beacon of innovation in this narrative. Based in Edmonton, Amii is one of Canada's three national AI institutes, advancing the country's leadership in artificial intelligence as part of the Pan-Canadian AI Strategy. They work alongside the Montreal Institute for Learning Algorithms (MILA), the Vector Institute,[1] and the Canadian Institute for Advanced Research to drive world-class research, develop top AI talent, and support the responsible use of AI across industries. The research is so leading edge that the Chief Scientific Advisor for Amii, Richard S. Sutton, was co-awarded the 2024 ACM A.M. Turing Award for developing the conceptual and algorithmic foundations of reinforcement learning. They are positioning Canada as a global leader in AI innovation (Alberta Machine Intelligence Institute , 2025). Joan Hertz, the incoming Chair of the Amii board agrees,"I look forward to continually increasing literacy in AI and showing how Canada can be a leader in responsible Artificial Intelligence."

And then there is CyberAlberta, which is not just another government cybersecurity initiative—it's an award-winning collaborative force. Based in Edmonton, CyberAlberta is championed by the Minister for Technology and Innovation, the Honourable Nate Glubish, and is led by Alberta's highly respected Chief Information Security Officer, Martin Dinel. Their mission—to unite industry, government, and academia in a relentless fight to keep Alberta's digital world safe. The CyberAlberta Community of Interest (COI) has over eight hundred participants; and it is growing every month.

They do not just talk about cyber resilience—they build it, one connection, one innovation, one breakthrough at a time. Training the next generation through groundbreaking programs that bring people with little to no experience into the cyber world through education, mentoring and an apprentice program that is just in the works. Because in the ever-evolving battleground of cybersecurity, CyberAlberta is not just keeping up; they are leading the charge. Equipping businesses. Strengthening defenses.

[1] Located in Toronto, Ontario, Vector is a premier AI research institute focusing on machine learning and its applications in business and healthcare.

And other jurisdictions are taking notice. "Historically people have been looking at Edmonton as being just Government," says Dinel. "But I'm seeing a change. We have a lot of technology organizations that are opening up right now, whether it's game designers, whether it's AI technology with Amii (see above). It is starting to happen here, in Edmonton."

What sets the story of Edmonton apart is not just the talent or the institutions—it's the spirit of collaboration that ties it all together. It is recognized by CBRE, a global commercial real estate services and investment firm, as part of the Top 50 Scoring Tech Talent list for North America in 2024 (CBRE Research, 2024). Picture a room filled with government officials, tech entrepreneurs, and university researchers, all brainstorming solutions to the next big cybersecurity challenge. This collaborative culture has become the city's hallmark, evident in initiatives like the annual Cyber Summit hosted by Cybera. These events foster an environment where ideas flow freely, and partnerships are born.

Edmonton's journey into the cybersecurity space is rooted in its history of educational excellence and economic resilience.

Writing the Future: Attracting Talent and Businesses

Every exceptional story has a beginning. Edmonton's journey into the cybersecurity space is rooted in its history of educational excellence and economic resilience. For decades, the city has prioritized research and innovation, laying the groundwork for its current success. The provincial and federal government's focus on economic diversification has also played a crucial role, steering investments toward technology and digital infrastructure. The federal government describes Edmonton as a "thriving source of economic diversification in Alberta and home to some of Canada's most innovative, high-growth companies responsible for strengthening our national economy," and as a result will see $6.7 million of federal funding split across four small-to-medium firms recognized to be innovating locally through technology (Thomas, 2025).

A key character in this tale is Alberta Innovates, a crown corporation that has consistently provided funding and support for research and technological advancements across Alberta, including Edmonton. Its programs, like the Digital Innovation in Clean Energy initiative, fuel new chapters in Edmonton's technology-driven future (Guay, 2024).

The Provincial Technology and Innovation Strategy (2022) serves as a road map, guiding Edmonton's transformation through strategic investments in digital infrastructure, artificial intelligence, and cybersecurity. This strategy has already reshaped the city's landscape—between 2015 and 2020, Edmonton saw

a 53% surge in technology jobs, outpacing even Toronto, Montreal, Vancouver, and Calgary over the same period (Government of Alberta, 2022). It is a story of momentum, one that continues to unfold with each passing year.

Edmonton Global, a foreign direct investment and international business development agency, plays a crucial role in shaping the city's economic future. Like a skilled narrator positioning Edmonton on the global stage, this agency connects local businesses with key partners, governments, and investors to ensure the story of Edmonton's cybersecurity growth is told far and wide (Edmonton Global, 2025).

Edmonton saw a

53%

surge in technology jobs outpacing even Toronto, Montreal, Vancouver, and Calgary.

One of Edmonton's most storied settings, the Edmonton Research Park, has long been a hub for companies focused on technological research and development. Established in 1979, it has been the backdrop for countless innovations, offering a stage where startups and established firms alike push the boundaries of what's possible. Here, ideas don't just take shape—they take flight, redefining industries and propelling Edmonton forward as a center of technological ingenuity (Edmonton Research Park, 2025).

In this evolving tale, Edmonton's academic institutions stand as pillars of knowledge, supporting the next generation of cybersecurity professionals. The University of Alberta, a globally recognized research powerhouse, has helped lay the foundation for the city's prominence in cybersecurity. Similarly, Concordia University of Edmonton (CUE) continues to develop the city's talent pool through its Master of Science in Information Technology (MSc IT) program, equipping students with the skills needed to navigate an increasingly complex digital world (Concordia University of Edmonton, 2025).

As Edmonton turns the page toward the future, the province is actively writing a new economic narrative—one that moves beyond its historical dependence on oil and gas. Forward-thinking initiatives like the Alberta Government's Innovation Employment Grant (IEG) are fostering growth in emerging sectors such as technology and cybersecurity by offering tax incentives to businesses investing in research and development (Government of Alberta, 2025).

Edmonton Unlimited is another key player in this narrative, supporting the startup ecosystem with critical funding, mentorship, and coaching. With 6,496 one-on-one coaching hours, 1,372 program participants, and over $21 million in startup investments, it is cultivating the next generation of innovators. Alberta Catalyzer, a pre-accelerator program, further nurtures the entrepreneurial spirit, ensuring that Edmonton remains a fertile ground for tech-enabled companies looking to make their mark (Edmonton Unlimited, 2025).

Each new development in Edmonton's tech ecosystem is another line in its unfolding story. Over the past decade, the city has consistently attracted investment to strengthen digital infrastructure and foster innovation. The Smart Cities Alliance in Edmonton, for example, has pioneered secure IoT systems for urban infrastructure, reinforcing the city's commitment to a tech-forward future. In 2020, Edmonton's ingenuity was recognized on an international scale when it received a Smart 50 Award in Digital Transformation from Smart Cities Connect. This accolade celebrated the city's development of advanced AI software that streamlines building inspections, reducing bureaucratic red tape and allowing inspectors to focus on higher-risk projects (The City of Edmonton, 2025).

The investment landscape further cements Edmonton's role as an emerging cybersecurity powerhouse. According to the 2023 Canadian Venture Capital Private Equity Association fourth-quarter report, the Edmonton Region secured the fifth position nationally for venture capital, attracting $188 million across 21 deals—a remarkable 324% increase from the previous year (Boily, 2024). These figures illustrate the confidence investors have in Edmonton's technology sector, affirming that the city is poised for continued growth in fields like artificial intelligence, blockchain, and cloud computing. Local companies are not just following industry

trends; they are setting them, developing cutting-edge solutions that safeguard everything from personal data to national infrastructure.

Retaining Talent: A Story of Growth and Stability

Why Edmonton? The answer lies in its unfolding story—a narrative of opportunity, ambition, and a city committed to those who call it home.

For professionals seeking a place where they can shape their careers while making a lasting impact, Edmonton presents a compelling storyline. It is a city where talent and opportunity converge, where academic institutions collaborate with industry to solve real-world problems, and where innovation is woven into the very fabric of its community.

As this story unfolds, Edmonton has established itself as a cybersecurity hub, not only attracting top talent but ensuring they stay by offering the right mix of quality of life, career growth, and an ever-expanding network of support. With competitive salaries, a thriving tech ecosystem, and continuous upskilling initiatives, cybersecurity professionals have every reason to plant roots here and contribute to the city's evolving digital frontier.

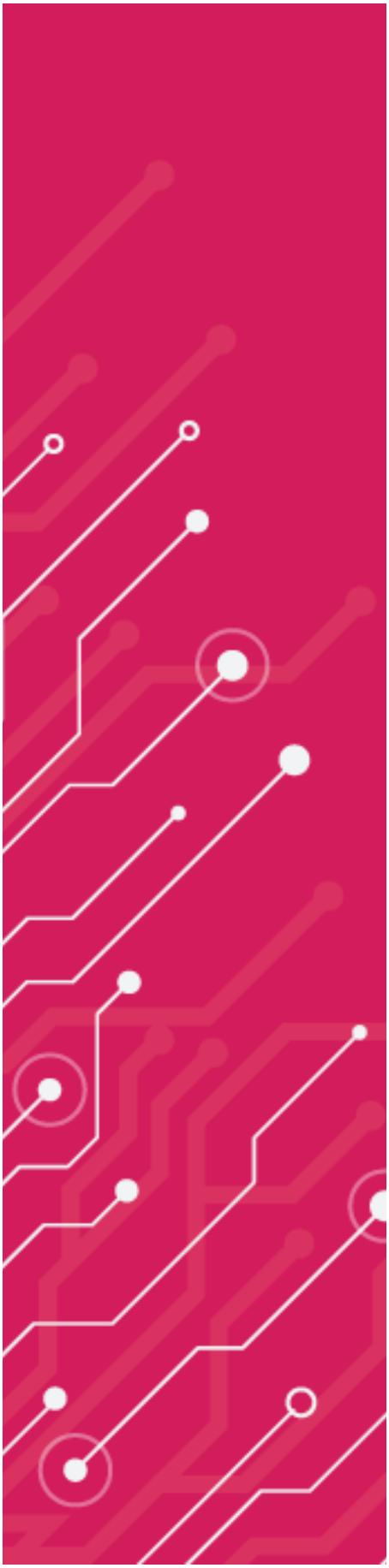
One of Edmonton's strongest story lines is its balance between affordability and opportunity. As of January 2025, the average annual salary for cybersecurity professionals in Edmonton exceeds $110,000 (Zip Recruiter, 2025). Yet, despite its growing prominence, Edmonton remains an accessible city where professionals can thrive. The cost of living, though 7% higher than the national average, is still more affordable than in larger Canadian cities, offering a rare combination of economic stability and a high standard of living (Cost of Living in Edmonton, Alberta | Cost of Living Index | ERI, 2025).

Edmonton's story isn't just about financial incentives; it's about a city that offers an unmatched quality of life.

Consider this: the average monthly cost of living for a single individual in Edmonton is less than $2,650, covering essentials like housing, utilities, groceries, and transportation (Nacario, 2025). This affordability doesn't come at the expense of lifestyle. Instead, it allows professionals to enjoy the city's vast cultural, recreational, and technological offerings—an essential chapter in Edmonton's talent retention success.

The city's diverse industry base—including government, healthcare, energy, and finance—fuels a sustained demand for cybersecurity expertise, offering professionals a wealth of career pathways without the need to relocate. This dynamic job market, paired with Edmonton's lack of provincial sales tax (PST), ensures that residents keep more of their earnings—an advantage that enhances quality of life in both tangible and experiential ways.

But Edmonton's story isn't just about financial incentives; it's about a city that offers an unmatched quality of life. The North Saskatchewan River Valley, the



largest urban parkland in North America, provides an expansive setting for year-round outdoor adventures, from hiking and biking in the summer to cross-country skiing in the winter. Meanwhile, Edmonton's reputation as "Festival City" brings arts and culture to life throughout the year with landmark events like the Edmonton International Fringe Festival and the Folk Music Festival.

Beyond its cultural vibrancy, Edmonton ensures access to world-class healthcare, with top-tier institutions like the University of Alberta Hospital and the Cross Cancer Institute leading the way. Sports enthusiasts find their excitement at Rogers Place, home of the Edmonton Oilers, where the energy of the crowd is as much a part of the city's identity as the game itself. And for art lovers, the Art Gallery of Alberta stands as a beacon of creativity, its striking architecture housing a diverse collection of over 6,000 works from Canadian and international artists (Art Gallery of Alberta, 2025).

Whether drawn by financial advantages, outdoor recreation, or cultural depth, cybersecurity professionals find in Edmonton a story worth staying for—a place where careers flourish alongside a rich and fulfilling lifestyle.

Yet, Edmonton's story is not written by these institutions alone. Employers play a leading role in shaping this chapter, investing in talent retention through upskilling programs, certifications, and mentorship opportunities. Recognizing that growth and engagement go hand in hand, companies offer competitive benefits, flexible work arrangements, and a culture that keeps cybersecurity professionals motivated and committed.

Education remains a vital plot line in Edmonton's cybersecurity narrative. The city has distinguished itself as the only one in Canada offering open registration for the SABSA (Sherwood Applied Business Security Architecture) Foundations course, a globally recognized framework for security architecture. With training budgets often stretched, having access to world-class instruction locally makes it easier and more affordable for professionals to advance their expertise.

For Thomas Wong Matthews, Director of Cybersecurity and Chief Information Security Officer at MacEwan University, this marks a turning point. "This is a significant opportunity to assemble a community of security architects right here in Edmonton," he said. "This cohort will learn together, build together, grow together, and stick together!"

In Edmonton's ongoing cybersecurity story, talent isn't just recruited—it is nurtured, developed, and celebrated. With every investment in innovation, every professional choosing to stay, and every new opportunity created, Edmonton's narrative strengthens. And for those looking for a city where they can not only be part of the story but help write it—Edmonton is waiting.

The Next Chapter: Engagement and Community

Every great story is shaped by the voices within it, and Edmonton's cybersecurity narrative is no different. At its core, this is a story of connection—where professionals, businesses, government entities, and academic institutions come together to build a cybersecurity community that is stronger, smarter, and more resilient. Edmonton is not just participating in the cybersecurity conversation; it is helping to write the next chapter.

Collaboration fuels this ecosystem, and through strategic partnerships, industry events, and knowledge-sharing initiatives, Edmonton continues to reinforce its reputation as a leading cybersecurity hub. These gatherings are more than just events; they are the heartbeat of a growing community, spaces where ideas take shape, where mentorship sparks innovation, and where cybersecurity professionals find their place in the story.

One of the defining moments in Edmonton's cybersecurity journey came with the launch of the CyberAlberta Community of Interest in 2022. Established by the Alberta government and centered in Edmonton, this initiative bridges the public and private sectors to strengthen cybersecurity resilience across the province. Through structured collaboration and shared expertise, CyberAlberta empowers organizations to navigate an increasingly complex digital threat landscape, ensuring that Edmonton remains at the forefront of security innovation.

Every great story needs a stage—and in Edmonton, cybersecurity professionals gather on some of the best.

But every great story needs a stage—and in Edmonton, cybersecurity professionals gather on some of the best. Events like BSides Edmonton act as catalysts for industry engagement, bringing together experts, students, and security enthusiasts to discuss emerging threats and explore the future of cybersecurity. What started as a local initiative supported by the (ISC)² Alberta Chapter has since grown into an independent non-profit, a testament to the demand for cybersecurity dialogue in the region.

For many, Edmonton's cybersecurity story is one of transformation. Harvinder Singh Dhami, who arrived in Canada as an international student in 2014, found a professional home in the city's cybersecurity scene. "The Edmonton Cyber Security community is exceptional because everyone is approachable and supportive," he says. "It is also a place for innovation, learning, and networking for both professionals and students."

Others, like Donald Ashdown, founder of the Open Web Application Security Project (OWASP) Edmonton, see the city's community as more than just a professional network—it is a welcoming space where knowledge and ideas flow freely. "OWASP Edmonton is more than just a meetup—it's a welcoming space where cybersecurity enthusiasts can connect, learn, and grow together," Ashdown said. With over 500 members, OWASP Edmonton plays a key role in fostering collaboration and professional development. "There is such a demand here in Edmonton—it's crazy."

This demand is met by organizations like the ISACA Edmonton Chapter, which provides educational opportunities in information systems auditing, IT governance, security, and internal controls. By equipping professionals with the knowledge and certifications they need, ISACA helps shape the next wave of cybersecurity leaders, ensuring that Edmonton's expertise continues to grow.

But the network doesn't stop there. Edmonton's cybersecurity web extends across multiple platforms and initiatives. The ISC² Alberta Chapter provides another vital link in the community, offering professional development opportunities and a space for security practitioners to exchange knowledge. Meanwhile, YEGSEC, a Slack community launched in 2016, has grown to over 800 participants, reinforcing Edmonton's reputation as a place where professionals don't just work in cybersecurity—they live and breathe it.

From grassroots initiatives like OWASP Edmonton to industry-driven events such as BSides, Edmonton offers an inclusive and collaborative environment that continues to attract talent. With ISACA providing specialized training and the SABSA Foundations course bringing world-class security architecture education to the city, Edmonton isn't just keeping pace with the global cybersecurity industry—it is helping to define its future.

Behind every thriving cybersecurity hub lies a network of partnerships, and Edmonton's story is no exception. Organizations like Cybera, a not-for-profit corporation, operate Alberta's Optical Regional Advanced Network, connecting research universities, colleges, K-12 schools, non-profits, and business incubators. By fostering collaboration between researchers and the private sector, Cybera supports the development of digital technologies, including cloud computing and next-generation networking—essential tools in today's cybersecurity landscape.

Meanwhile, the federal government's Cyber Security Innovation Network (CSIN) plays a role in broadening Edmonton's impact. By facilitating research and development, increasing the commercialization of cybersecurity innovations, and expanding the country's talent pool, CSIN ensures that Edmonton's cybersecurity ecosystem remains vibrant, forward-thinking, and well-connected.

In the grand narrative of cybersecurity, Edmonton is not a passive character. It is an active participant, shaping its destiny through collaboration, education, and innovation. And for those looking to be part of this unfolding story, Edmonton extends an invitation—not just to watch from the sidelines, but to step in and help write the next chapter.

Overcoming Challenges: A Story of Persistence

Every great story faces its share of obstacles, and Edmonton's cybersecurity journey is no exception. The path to becoming a world-class cybersecurity hub is not without its challenges, but true to its spirit, Edmonton meets these hurdles with resilience, adaptability, and a relentless drive to innovate.

One of the most pressing challenges in this evolving narrative is the global shortage of skilled cybersecurity professionals—a gap that Edmonton, like many other regions, continues to grapple with. According to the 2024 ISC² Cybersecurity Workforce Study, organizations must expand opportunities for workforce growth and invest in training entry-level professionals to close the skills gap (ISC2, 2024). Without a steady pipeline of new talent, the industry's rapid expansion risks being slowed.

By acknowledging these barriers, embracing collaboration, and actively implementing solutions, the city is ensuring that its digital security ecosystem remains strong.

But recruitment is only part of the story—retention is just as critical. Cybersecurity professionals face long hours, high-pressure environments, and, in some cases, burnout. A report by CyberSN found that 68% of cybersecurity professionals feel their jobs negatively impact their personal lives, and nearly 75% remain open to changing positions (CyberSN, 2025). If Edmonton is to secure its standing as a cybersecurity leader, it must ensure that professionals who come to the city choose to stay.

For Edmonton businesses, the competition for top-tier cybersecurity talent is fierce. Larger organizations with deeper pockets can offer salaries and benefits that smaller enterprises may struggle to match. This, in turn, creates a talent war where companies must find creative ways to attract, engage, and retain the best minds in the field. Extended vacancies and recruitment struggles pose a real risk to industry growth, making it imperative that Edmonton's cybersecurity ecosystem continues to refine its approach to talent development.

Yet, like any great protagonist, Edmonton refuses to let challenges define its story. The city's cybersecurity community is already acting, implementing targeted strategies to strengthen its workforce and bolster its reputation as a place where cybersecurity professionals can build rewarding careers.

Across Edmonton, businesses, academic institutions, and industry groups are working together to foster inclusive workplace cultures, create career development opportunities, and emphasize work-life balance—all factors proven to enhance job satisfaction and retention. The community is also leveraging the power of networking, mentorship, and ongoing education to ensure that Edmonton's cybersecurity workforce continues to evolve.

Events like BSides Edmonton bring industry professionals together to exchange ideas, discuss best practices, and engage in hands-on learning. Community-driven initiatives such as the CyberAlberta Community of Interest (COI), OWASP Edmonton, and YEGSEC serve as platforms for mentorship and professional growth, connecting individuals with the broader cybersecurity ecosystem. Meanwhile, organizations like ISACA Edmonton and the SABSA Foundations training provide specialized instruction that strengthens local expertise, making professional development more accessible to cybersecurity practitioners in the region.

Edmonton's cybersecurity story is one of perseverance. By acknowledging these barriers, embracing collaboration, and actively implementing solutions, the city is ensuring that its digital security ecosystem remains strong, innovative, and future-ready. The road ahead may not always be easy, but if there's one thing Edmonton's history has proven, it's that this city thrives when faced with a challenge. And in the ever-evolving world of cybersecurity, persistence is the key to success.

The Epilogue? Not Yet—This Story is Ongoing

Every great story leaves room for the next chapter, and Edmonton's cybersecurity journey is far from complete. What began as a city of industry and innovation has evolved into a hub of digital security, resilience, and technological leadership. The foundations have been laid, the characters—its

people, institutions, and businesses — have stepped into their roles, and the plot continues to unfold with every breakthrough, collaboration, and investment in the future.

Edmonton is cementing its reputation as a center for cybersecurity through a growing network of initiatives aimed at fostering innovation and expertise. From industry events to educational programs and strategic partnerships, the city's cybersecurity ecosystem is evolving, driven by collaboration and a shared commitment to advancing the field. This is a story of momentum — one that is being written in real-time by those who choose to make Edmonton their home.

One of the key moments in this ongoing narrative is the Government Cybersecurity Showcase – Alberta, held in Edmonton in 2024. Organized in partnership with the Government of Alberta and the Ministry for Technology and Innovation, this annual event brings together public sector leaders to explore emerging threats and technological advancements. Discussions on deep fakes, digital resiliency, AI integration, and foreign interference highlight the ever-changing cybersecurity landscape, while the showcase itself serves as a catalyst for knowledge-sharing and cross-sector collaboration (Public Sector Network, 2025).

As Edmonton looks to the future, its story continues to welcome new characters and new opportunities. Following the success of the Canadian Cybersecurity Network's CyberPath GTA, plans are underway to launch a similar initiative in Edmonton. This program will provide individuals — whether early in their careers, seasoned professionals, or newcomers to Canada — with access to networking, education, certification, and mentoring opportunities. It will serve as yet another chapter in Edmonton's commitment to growing and retaining cybersecurity talent (Canadian Cybersecurity Network, 2025).

The appeal of Edmonton extends beyond career opportunities. This is a city where life outside of work is just as fulfilling as professional ambitions. Ranked as the most affordable city in Canada and fifth globally for quality of life, Edmonton offers universal healthcare, top-tier education, and a vibrant cultural scene that enriches daily life. Whether it's the city's expansive River Valley, year-round festivals, or thriving arts and technology sectors, Edmonton provides an environment where individuals and families alike can build their futures.

Edmonton's cybersecurity ecosystem is not just thriving — it is expanding. The city is home to a diverse range of cybersecurity companies that help businesses strengthen their digital defenses. This growth aligns with national trends, as Canada's cybersecurity industry has seen a 30% expansion, reflecting the surging demand for security professionals (Technation, 2022). Furthermore, Edmonton's business-friendly climate, with a low property price-to-income ratio, makes it an attractive destination for those looking to settle down while advancing their careers (Numbeo, 2025).

With no provincial sales tax and competitive personal income tax rates, residents enjoy a higher disposable income, enhancing both their financial security and quality of life. Edmonton's rare combination of a thriving cybersecurity industry, affordability, and unparalleled quality of life makes it a compelling destination for professionals and families alike.

But this is not the final chapter. Edmonton's cybersecurity story is still unfolding. The city's growth is driven by the professionals who choose to contribute their skills, the students who become the next generation of cybersecurity leaders, and the businesses that invest in digital security as a foundation for progress.

Whether you are a seasoned expert or just beginning your journey, your story can be part of Edmonton's cybersecurity legacy. Every idea, every innovation, and every connection strengthen the city's place in the global cybersecurity landscape.

This is a story that is still being written — and Edmonton invites you to help shape its next chapter.

See end notes for this article's references.

Curtis L. Blais is a cybersecurity leader shaping national strategies and strengthening institutional security across Canada. As Cybera's shared CISO and technical lead of the National Cybersecurity Assessment under CANARIE, he plays a key role in guiding the cybersecurity direction in the higher learning space in Canada. With experience spanning government, private sector leadership, and board appointments, he brings a strategic approach to risk and security. He holds multiple certifications, a master's in leadership from Royal Roads University, and completed Harvard's Cyber Risk Management program at the top of his cohort. An accomplished author, his book *CyberDynamX* provides a practical framework for building effective cybersecurity programs.


ccn
Sponsor the
Canadian OT Report
September
AI
canadiancybersecuritynetwork.com/ot-report

Fredericton: East Coast's Not So Hidden Gem

by Ben McHarg

> "New Brunswick is the hidden gem of the cybersecurity world."
>
> —*Troy Nelson, CEO, Lastwall*

The beautiful province of New Brunswick is a vibrant hub for the cybersecurity industry, where companies can leverage a small geography, active professionals and research community. In this province, cybersecurity professionals, researchers, government and industry openly and seamlessly collaborate on projects and community issues.

Anchored in Fredericton, the community extends to the cities of Moncton and Saint John. Arranged much like a triangle in south/central New Brunswick and within 1 to 1.5 hours drive from each other. The community is an easy commute for cybersecurity professionals, allowing them to take on jobs or projects in any of the three cities. This same proximity for workers also provides companies with access to a broad and talented workforce. Within this small triangle exists a high density of industries representing all sectors, from agriculture and forestry to national defence assets and nuclear power generation.

New Brunswick has a long history of innovation. From the early days of NB Tel, a world class pioneer in telecommunications, to various startups that have become parts of global companies, such as IBM and Salesforce, the province has always punched above its weight in the creation of technology companies. And that did not change with the emergence of the cybersecurity industry.

In New Brunswick, the challenge or opportunity, to establish a vibrant cybersecurity workforce and community, was identified early. Key investments and partnerships were made by the government, industry and academic institutions to provide a cohesive strategy to build up the province as a national, if not world, leader in Cybersecurity.

Moving the pieces into place began quickly. The stage was being set for New Brunswick to become the Cybersecurity powerhouse that it is today.

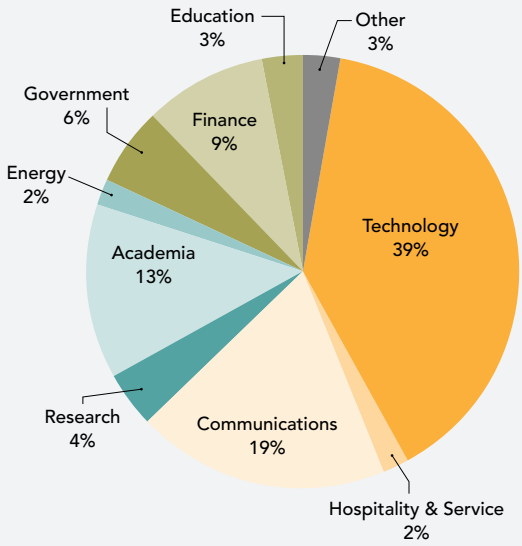
Building The Foundation for Success

Oddly enough, a key first step was creating a physical space for this new cyberspace world. Here, the city of Fredericton stepped up to create Knowledge Park, a 35-acre research and technology campus. This provided a local hub where startups could launch and grow alongside established cybersecurity businesses. Anchoring Knowledge Park is the Cyber Centre, "Canada's most advanced networking and data fiber facility," which boasts the necessary security clearance (Level II) to work with the most sensitive industries and national defence.

For research and development, Fredericton was already well positioned as the home of the University of New Brunswick (UNB); its existing world-class computer science program is ranked in the top 20% of undergraduate computer science programs globally. Adding the Canadian Institute for Cybersecurity (CIC) in 2016 further consolidated this expertise. Lead by Ali Ghorbani—the institute's founding director and Canadian Research Chair in Cybersecurity—the CIC is a comprehensive, multidisciplinary unit that draws on local research expertise in the social sciences, business, computer science, engineering, law and science, as well as other national and international cybersecurity research centres, to provide its students with training, research and development, and entrepreneurial opportunities. In fact, students, including master's and PhD graduates, have become an integral part of the talent pipeline and have made a significant impact on the cybersecurity industry.

Now operating with over 100 employees, the CIC regularly collaborates with the government and industry to solve real-world cybersecurity challenges.

Where are they now?



On the global stage, the CIC organizes the annual Privacy, Security and Trust (PST) Industry Summit. The summit is held every second year in Fredericton (with alternating years at locations around the globe) and brings together hundreds of thought leaders, industry experts and policy makers to share advances in cybersecurity research and security applications. The 2025 summit will be held in Fredericton from August 26 to 28.

Highlighting the continued strength and future importance of Fredericton and New Brunswick in the field of cybersecurity, the Government of Canada recently announced funding of $10 million over five years to establish a new Cyber Attribution Data Centre (CADC) at the CIC. Dr. Ghorbani notes that the addition of the AI-powered CADC will "strengthen the country's ability to protect critical assets and maintain public trust," and "serve as a key repository for tracking and analyzing cyberattacks while identifying their characteristics, sources and perpetrators."

> "Today marks a pivotal moment in Canada's leadership in cybersecurity and data innovation. Establishing the new CADC at the CIC is a testament to our commitment to advancing cutting-edge research, fostering collaboration between industry and academia, and enhancing our national security…"
>
> *—Dr. Paul J. Mazerolle, President and Vice Chancellor, University of New Brunswick*

Hugh Hicks, Canadian Institute for Cybersecurity; Dr. Paul J. Mazerolle; Hon. Minister LeBlanc; Dr. Frank McKenna; Dr. Luigi Benedicenti, Dean of Computer Science, UNB

> "The establishment of the CADC is an exciting step forward for both our province and our country… New Brunswick is already home to world-class talent and innovation, and this initiative further solidifies our role as a hub for cybersecurity research and development. This is a win for New Brunswick, for Canada, and for the future of cybersecurity."
>
> —*Frank McKenna, Deputy Chairman Toronto-Dominion Bank, former Canadian Ambassador to the United States and former Premier of New Brunswick*

UNB's McKenna Institute plays a central role in enhancing Fredericton and New Brunswick's reputation as one of Canada's leading cybersecurity innovation hubs. Strategically positioned within one of the nation's richest talent and innovation ecosystems, the Institute's sector-based innovation approach integrates cybersecurity and complementary enabling technologies—including responsible AI, interactive design, data governance, and 3D technologies—to stimulate significant economic growth across critical industries.

Central to the Institute's success is its commitment to human-centric, collaborative innovation. Through targeted educational pathways, talent development programs, and strategic industry partnerships, the Institute nurtures a workforce skilled in cybersecurity and fluent in related technologies like responsible AI and interactive design. Its collaborative approach ensures New Brunswick businesses not only maintain robust digital defenses but also possess the innovation potential necessary for competing effectively on the global stage. By embedding security and privacy as core principles in sector-specific initiatives, the McKenna Institute ensures robust digital resilience and fosters innovation capabilities throughout the region.

Provincial government stakeholders are also mobilized to strengthen the cybersecurity talent pipeline in other levels of New Brunswick's education system. The Department of Education and Early Childhood Development (EECD) created and adopted a cybersecurity curriculum for K-12 students as part of their general education to drive awareness of potential career paths. In 2024, EECD moved the bar forward with the launch of a Center of Excellence (CoE) in Digital Innovation. The Centre of Excellence is a partnership between the education system, community, and industry partners to help connect students to expert knowledge through virtual and experiential learning. The CoE for Digital Innovation focuses on strengthening student digital literacy skills, promoting cybersecurity, and highlighting Information and Communications Technology (ICT) career pathways.

The provincial public community colleges also jumped into action:

In 2018, the New Brunswick Community College (NBCC) developed and launched a cybersecurity program to support workforce development; since launch, about 80% of program graduates chose to stay in the province to continue their career. Shortly thereafter, the Collège Communautaire du Nouveau-Brunswick (CCNB) also added a cybersecurity program for French-speaking students.

In 2020, NBCC's College Office of Research Enterprise (CORE) leveraged the cybersecurity program's Saint John campus (located near a wide variety of industrial partners), to build the region's first Critical Infrastructure Security Operation Center (CI-SOC). The CI-SOC enables industry partners to test their security tools and procedures in a simulated environment. Additionally, the CI-SOC enables K-12 students to interact with security systems and see the real-world impact of simulated breaches on physical assets in the facility.

NBCC's CORE provides applied research and experimental development services to companies, non-profits, and governmental organizations in several areas, including information and communication technologies.

A key part of NBCC's CORE is the Information and Communication Technologies Research Group (ICTRG) The ICTRG practices socio-technical innovation: technical innovation centred on understanding the social context and the participation of technology's intended recipients. When appropriate, ICTRG applies user-centred design, universal design, and security by design.

PHOTO: JESUS SALVADOR ALEJANDRI MEZA, UNB MEDIA SERVICES

ICTRG has a dedicated team of computer scientists and engineers, comprehensive device libraries for mobile and IoT systems development, as well as tools for user interface design and usability testing to support software development and experimentation with companies and organizations. In Q2 2025, the ICTRG expects to add a 5G wireless private network to support edge computing. The 5G lab is a key example of collaboration with funding from the Canadian Foundation for Innovation, and contributions from the City of Fredericton, Research NB, and Atlantic Canada Opportunities Agency (ACOA). ICTRG has also helped New Brunswick companies like HotSpot Parking and Sensory Friendly Solutions develop revenue-generating technologies.

The Results Are In: Employment Growth

Source: Opportunities NB

37%
Tech talent growth[1] from 2020–2023.

66%
Computer and information systems professionals employment growth over the last three years.[2]

2x
Employment growth in software developers and programmers over the last three years.

No Longer a "Hidden Gem?"

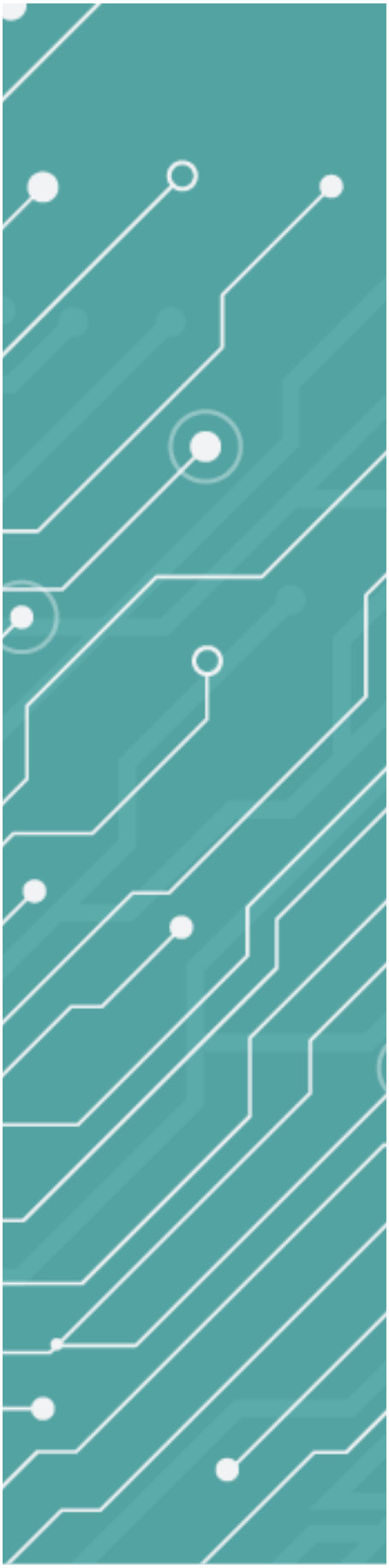
> "I think… New Brunswick is going to have a really important role to play in equipping all of Canada with cyber defences so that we can protect our democracy and protect our critical infrastructure."
>
> —*Frank McKenna, 2025*

Provincial strategies for attracting cybersecurity talent and businesses have been successful in bringing world-class companies to New Brunswick. These strategies include highlighting the benefits of labour costs and availability, strong community support for retention, established research and development, and the availability of government support.

Ensuring the world knows what Fredericton and the rest of the province have to offer is the challenge, but the message is getting out. In recent years, many companies have either announced new offices in Fredericton or plans to grow existing workforces. Amour Cybersecurity, MNP, Kyndryl, IBM, and Bulletproof are all planning to, or have already, added skilled cybersecurity positions to the province's workforce in partnership with Opportunities NB. Siemens launched their Critical Infrastructure Defense Center (CIDC) in Fredericton's Cyber Centre in 2022, and Thales officially opened its new National Digital Excellence Centre in the city in 2025. The latter will handle cybersecurity for some of the country's most sensitive industries and critical infrastructure. Showing the collaboration of

[1] Tech talent includes the following occupations categories: Computer and Information Systems Professionals; Computer, Software and Web Designers and Developers; Technology and Engineering related; and Computer and Information Systems Managers.

[2] This includes: Cybersecurity, Business and Information Systems Specialists, Database Analysts and Data Administrators Occupations.



industry, government and academia, the new centre was established in partnership with the McKenna Institute at the University of New Brunswick and the city development agency Ignite. Funding was provided by the ACOA, Opportunities NB, and Post-Secondary Education, Training and Labour.

> "This partnership is part of our commitment to supporting the province's focus on fostering local tech talent, creating meaningful jobs, and improving workforce skills training. We are leveraging the growing and diverse tech labour force in New Brunswick and its hotbed of cybersecurity talent to help organizations modernize, transform and grow. We are proud to contribute to the province becoming a world-renowned information technology hub, while advancing a dynamic and inclusive digital future in the region."
>
> *—Farhaz Thobani, President, Kyndryl Canada*

A Thriving Start-Up Culture

> "All the pieces are in place for startups in NB."
>
> *—David Shipley, President, Beauceron Security*

It is not just leading global industry that finds New Brunswick to be a strong base for cybersecurity progress. Building on the solid foundations of innovation in the past, the cybersecurity start-up ecosystem continues to thrive across the province. David Shipley—whose company, Beauceron Security, was built and continues to be headquartered in Fredericton—notes how local municipalities and the provincial government are often the early adopters of technologies from "made-in-NB" startups, helping them grow and gain credibility. In the port city of Saint John, TrojAI was founded in 2019 and has become a leading provider of artificial intelligence (AI) security solutions. "Stephen Goddard and I founded TrojAI to address a critical need for security around AI deployments," said Dr. James Stewart, CTO and Co-Founder of TrojAI. TrojAI has been recognized by Gartner, CB Insights, and OWASP as a premier AI security provider. Dr. James Stewart credits help from funding agencies like the New Brunswick Innovation Fund (NBIF) and the Nation Research Council's (NRC) Industrial Research Assistance Program (IRAP), for helping to grow their startup. Strong local support is a common theme when speaking with founders. NBIF itself has more than $4.5M invested in local Cybersecurity startups across the province.

Fredericton and New Brunswick have all the economic development strategies and resources in place for startups or businesses looking to expand and take advantage of the established ecosystem. As highlighted throughout this report, the federal government provides support through the Atlantic Canada Opportunities Agency, while provincially, Opportunities NB takes the lead on many activities. Once you know which city best suits your needs, regional economic development agencies are there for the local touch and pulling it all together, notably, Ignite (Fredericton), Envision Saint John, and Moncton Impact.

There are also many regional incubators and accelerators in the province. Provincially there is Propel and the Joint Economic Development Initiative (JEDI) for Indigenous entrepreneurs. Fredericton has UNB/Energia Ventures and Planet Hatch; Saint John has ConnexionWorks; and, Moncton has Venn Innovation.

Bringing The People Together!

> "The most rewarding thing for me is helping people make connections. Whether it is helping people find a mentor, a new employment opportunity or just finding someone they can discuss a topic of interest, it is a great feeling to be able to help make it happen."
>
> —*Julien Richard, Founder, Atlantic Cybersecurity Collective*

New Brunswick has an amazing and growing cybersecurity community. A big part of this thriving community is the Atlantic Cybersecurity Collective (ACC), which provides an active online community as well as in-person events in Fredericton, Moncton, and Saint John. Founded by Julien Richard only a few years ago to connect cybersecurity professionals in the region, this grassroots initiative is made up entirely of volunteers with no direct involvement from industry or government. The ACC is dynamic, constantly evolving, and excels in people interested in the field of cybersecurity. Mentorship and guidance are anchored in a Discord server with more than 370 members (many of whom are active contributors) and events, such as its "Unconferences," held in each of the three cities. For those looking for more regular in-person connections, each city also hosts a monthly cybersecurity meetup. These socials are non-vendor-sponsored events for like-minded folks to network and discuss cybersecurity topics of the day without any outside complications. These meetups are organized on the Discord server and through their respective BlueSky accounts:

- **Fredericton, FreddySec @freddysec.bsky.social**
- **Saint John, PortSec @portsec.bsky.social**
- **Moncton, Atlantic Cyber @atlantic-cyber.org**

Fredericton is also home to a local BSides chapter. Chris Lincoln describes this community effort:

> "BSides Fredericton is the largest security event in New Brunswick, and despite that, it's still true to the BSides spirit of building a security community—and we keep it free for attendees.
>
> I've met many great people there—attendees, speakers, volunteers, and our great sponsors who show up knowing that the goal is less to make a sale and more to support the community, including the next generation of security professionals.
>
> Yes, it's a great place to learn things or share what you've learned, but the community aspect is the most important to us. During the lockdowns, we decided that we would rather take a break than go online because we would lose that local feel. And there was so much support when we came back. We want to ensure everyone gets something out of it, it stays free, and is a way for everyone to come away with something."

The Road Ahead

The secret may be out on our "hidden" gem of a cybersecurity community, but opportunities exist, and further promotion of the province is needed. Several people interviewed for this report commented that more should be done in

sharing the value proposition; often, conversations with potential investors or expanding companies begin with an initial introduction to the province. And far too often, companies had no idea so much was happening in the cybersecurity industry here.

New Brunswick should work hard to reach the point where investors and businesses are chasing business development groups for information on how to get involved. For this to happen, the entire provincial ecosystem will need to work together. Many interviewed have expressed the need for a provincial agency or entity to take the lead. The provincial cybersecurity strategy could be renewed with further funding and support from the government and industry.

A critical component of any strategic plan is a robust and capable workforce. Local universities and colleges have been the engine attracting and producing local talent, but they have struggled to attract local students to fill their cybersecurity programs. Institutions have been lucky to have access to international students, but that window of opportunity is closing. The focus from everyone involved in the sector should target young people, under-represented and equity-deserving populations, and those displaced from other industries. Further, the provincial education system should continue to support and boost cybersecurity content in their curriculum. This will enable all students to have the base knowledge needed in a digital economy but also the visibility to career pathways and opportunities in the field of cybersecurity. Teachers and educators must have the required tools and training to deliver basic and advanced cybersecurity curriculum.

Another opportunity lies within rural or underserved areas. Investment in rural connectivity infrastructure, affordable internet, and mobile access would provide multiple benefits. More students would have reliable internet access to much needed educational resources.

New Brunswick's cybersecurity community, led out of Fredericton, is truly provincial in scope and in fact already world class. Research and development groups are thriving, startups are springing up and established businesses are seeing it in action and moving to the region as a result. New Brunswick needs to continue its strong support of the industry, improve provincial collaboration and invest in key areas to sustain this growth and propel the industry into an even more successful future.

See end notes for this article's references.

Ben McHarg is an instructor in the Cybersecurity program at the New Brunswick Community College where he specializes in several areas of cybersecurity focusing on defensive methodologies. In addition, Ben is an associate member of the Canadian Institute for Cybersecurity (CIC).

After more than 20 years in various information technology roles, Ben joined the New Brunswick Community College, where he helped create and launch the College's Post Diploma Cybersecurity program. Volunteer activities include organizing, building challenges and coaching for CyberSci (National/International Post Secondary Cybersecurity Competition) and serving as a founding member and organizer of the Atlantic Cybersecurity Collective.

Halifax: The Ultimate Destination for Cybersecurity Professionals

by Holly DeWolf

Halifax, Nova Scotia's largest city, offers a unique setting for cybersecurity professionals. With nearly half of the province's population calling this picturesque city home, Halifax is a dynamic combination of coastal beauty, historic charm, and a rapidly evolving tech industry.

A Thriving Tech Ecosystem: A Globally Competitive Industry

According to the Halifax Partnership, "Halifax is home to a globally competitive tech industry supported by a vibrant ecosystem of post-secondary education, established multinational firms, incubators and accelerators, and an active startup community that provides a collaborative, well-connected, global cluster."

Halifax is emerging as a leading cybersecurity hub, bolstered by its educational institutions, government support, thriving tech ecosystem, and focus on diversity and inclusion. Its strategic location with an established culture of research and development further positions the city as an attractive destination for cybersecurity professionals.

Educational Institutions: The Pillars of Talent Development

Educational Institutions are pivotal in developing talent. Halifax is home to several esteemed educational institutions, including Dalhousie University, Saint Mary's University, Mount Saint Vincent University and Nova Scotia Community College (NSCC). All offer cutting-edge programs in cybersecurity, artificial intelligence, and digital forensics.

Each year, Halifax welcomes students from around the globe, enhancing the local talent pool.

These institutions play a foundational role in preparing the next generation of cybersecurity professionals through co-op programs and internships. Their programs provide a path from education to successful careers in technology, actively supporting and developing a diverse range of exceptional thinkers in the field. Of note, many of the institutional resources and scholarships are tailored to support female students.

- **Dalhousie University** is highly regarded for its focus on promoting female participation in tech, providing a solid foundation for women in cybersecurity; Dalhousie University News.
- **NSCC** offers targeted training programs and scholarships for women, which are crucial for closing the gender gap in the field; NSCC Programs.

Each year, Halifax welcomes students from around the globe, enhancing the local talent pool. Graduates contribute significantly to advanced research and innovation, further solidifying Halifax's reputation as a leading destination for tech and cybersecurity professionals.

Community Support and Collaboration: Attracting Talent

The provincial government of Nova Scotia has committed to increasing the participation of women in STEM, including cybersecurity. Through various programs and funding initiatives, the government promotes a supportive environment that helps women excel in tech through Women's Economic Security.

The presence of the Canadian Naval, Army, and Airforce bases provide local talent with additional pathways to success in technology. The connection to national defense platforms means that cybersecurity in Halifax is integrated with maritime defense, critical infrastructure, and national resilience.

Halifax has implemented several initiatives aimed at attracting talent and businesses to the region. A prime example is the Graduate to Opportunity (GTO) Program. This initiative provides subsidies to businesses hiring recent graduates for innovation-focused roles, creatively supporting business growth while maintaining competitive salaries.

Additionally, business incentives provided by Invest Nova Scotia, such as the Nova Scotia Payroll Rebate and the Provinces Digital Media Tax Credit, encourage tech companies to establish themselves in Halifax. These incentives contribute to a supportive business environment, which enables Halifax-based tech industry to position itself as a leader in the cybersecurity sector.

The startup scene in Halifax has been rapidly evolving, bolstered by organizations such as Digital Nova Scotia and Volta. These organizations support local tech startups and larger organizations, creating a community that encourages growth and collaboration.

> "There are many things that make Nova Scotia's tech scene unique, but at the core I believe it's truly our community focused approach. We're connected, we're focused on collaboration, and we're proud of who we are and what we can achieve."
>
> —*Caitlin Patterson, Director of Marketing & Communications, Digital Nova Scotia*

Work-Life Balance

Halifax possesses a culture that prioritizes well-being without sacrificing impact. The concept of "calm intensity" is prevalent amongst employers who promote a balance between mission-driven work and humane expectations. Normalized flexible work arrangements are appealing in high-pressure fields like cybersecurity, allowing one to maintain a healthy work-life balance.

Retention Strategies

Halifax is recognized as one of North America's emerging tech talent markets, with significant growth in tech employment over the past five years. Keeping talent is one key to the region's success. Approximately 60-70% of local cybersecurity graduates remain in the region within the first

1-3 years after graduation. Programs like the Graduate to Opportunity are highlighted as an initiative aimed at retaining talent by offering competitive opportunities.

Though not always competing on top-dollar salaries, Halifax employers take a considered approach with their retention efforts by focusing on career development and a supportive work environment. Some creative strategies employed to retain cybersecurity talent include:

- **Mentorship Models:** Small teams allow for faster learning curves, where junior analysts gain exposure to a wide range of responsibilities quickly.
- **Upskilling and Career Development:** Organizations invest in training programs, offering access to ongoing certifications like CompTIA and CISSP.
- **University Partnerships:** Collaborations with local institutions often lead to permanent roles for co-op students.

These tactics are proven approaches that improve employee satisfaction, drive a more stable and sustainable workforce.

> "Effective retention strategies for cybersecurity professionals include competitive compensation, professional development, a positive work environment, recognition, work-life balance, innovation, and clear career progression paths. Understanding the importance of retention in cybersecurity is not just about maintaining a team; it's about safeguarding your organization's digital assets, intellectual property, and reputation."
>
> —*Stephanie LeBlanc, Senior Manager Information & Technology Services, Halifax Water*

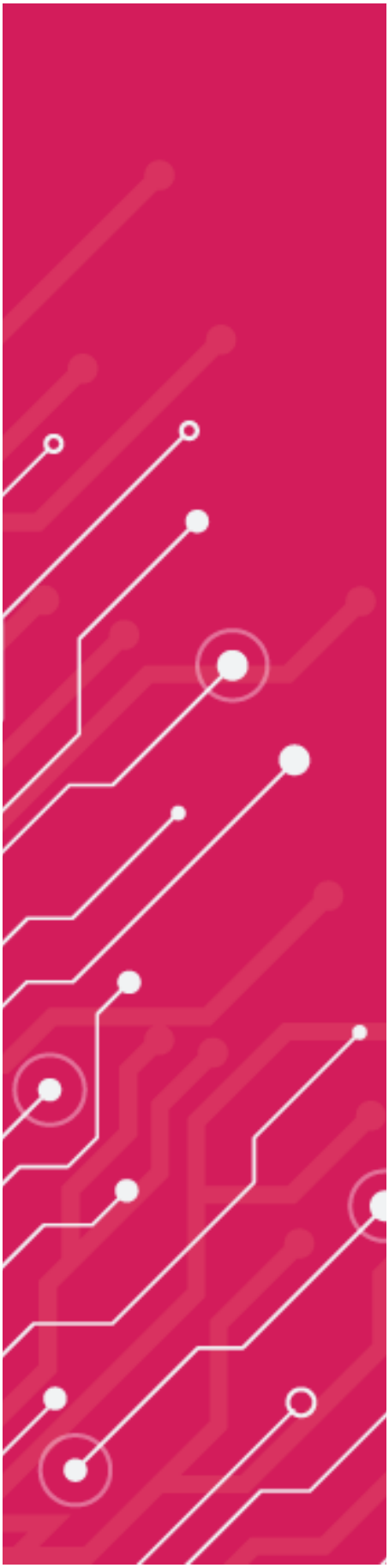
An Inclusive Workforce: Collaborating for Change

Diversity, equity, and inclusion (DEI) are critical components of a thriving cybersecurity community. Initiatives like TEAM Work Cooperative emphasize inclusive and diverse work environments, which can boost employee satisfaction and loyalty. Increasing representation of women and BIPOC individuals in cybersecurity is essential for furthering a more equitable and creative industry.

> "As a women working in IT in Halifax, I see the growing connection between tech and cybersecurity every day. Representation — when women are a part of building and protecting systems, we drive innovation and resilience. Halifax's focus on inclusion is what makes it such a powerful place to grow a tech career."
>
> —*Sheri Murphy, Senior Manager Information Technology, Halifax Stanfield International Airport*

DEI initiatives championed at cybersecurity organizations in Halifax continue to grow and improve their workforce capabilities. By promoting equity and inclusivity, Halifax harnesses diverse perspectives, drives innovation and strengthens the community.

Local companies recognized that the industry benefits when mentors are available and approachable. Women and men in leadership roles within local tech



companies seek out opportunities to participate and serve as role models, inspiring the next generation who are just entering the cybersecurity workforce. Going a step farther, many companies have formed partnerships with educational institutions to create internships and mentorship programs.

> "At Digital Nova Scotia, we've graduated over 960 participants through our Skills for Hire Atlantic Program in Data Analytics, Cybersecurity and Web Development (46% female, 52% new immigrants). The program resulted in over 600 individuals reporting securing a new job placement or continuing their education. For us, it shows a significant positive shift in the tech landscape, with more employers welcoming those with diverse backgrounds."
>
> —*Caitlin Patterson, Director of Marketing & Communications*

Building Communities: Driving Innovation

A diverse and collaborative community in cybersecurity brings several benefits to the industry, such as global perspectives, enhanced creativity, improved decision-making, and a broader skill set. Gender-diverse teams are more adaptable, innovative, and effective in responding to the evolving cybersecurity threat landscape. Furthermore, organizations that prioritize diversity tend to attract and retain talent, which is crucial for addressing the growing cybersecurity talent shortage. As with any active industry, local online networking and support groups have grown to provide spaces for individuals in cybersecurity to share experiences, knowledge, and resources.

Digital Nova Scotia offers their Digital Skills for Women+ Program, which has supported over 400 women and gender-diverse individuals exploring a career in tech. The free program covers topics from cybersecurity and programming to AI and digital marketing and was designed to reduce barriers for women and gender-diverse people to explore careers in technology.

> "Cybersecurity is not a playoff game where we are hoping to beat out the other team. Organizations, whether they compete or not, share a common goal to keep our businesses, our customers, and our communities safe. Sharing ideas from our playbooks without impacting confidentiality is key. That is something organizations in the region encourage and support."
>
> —*Jennifer Hutton, VP Information & Technology, & CPO, Steele Auto Group*

Local Organizations and Events

Halifax has a dynamic tech and cybersecurity scene with several events and meetups that foster collaboration. These events and forums are excellent opportunities to connect with like-minded individuals, learn, and collaborate. Some examples of notable events:

1. **ATLSECCON:** This is Atlantic Canada's largest information security conference, held annually at the Halifax Convention Centre. It provides a platform for networking, learning, and sharing insights on cybersecurity trends and challenges.
2. **BSides Halifax:** A community-driven cybersecurity conference that features talks, workshops, and networking opportunities. It's a great event for both seasoned professionals and newcomers to the field. *Hosted in locations across Atlantic Canada.
3. **Digital Nova Scotia:** DNS collaborates on Third Wednesdays, a casual networking event for those in tech that's been running for over 10 years.
4. **Halifax Cyber Security for Control Systems Meetup:** A group dedicated to professionals involved in cybersecurity for automated processes and control systems. They host educational sessions, discussions, and networking opportunities.
5. **The Women in CyberSecurity (WiCyS) Halifax Chapter:** plays a vital role in supporting women in the field by hosting events and workshops that foster networking and mentorship. These gatherings provide opportunities for women to engage with experts, enhance their skills, and access resources aimed at their professional growth.
6. **DEFCON Halifax Meet-Up:** A local chapter of the global DEFCON community, this meetup is a space for hackers, tinkerers, and security professionals to share ideas and projects in a relaxed environment.

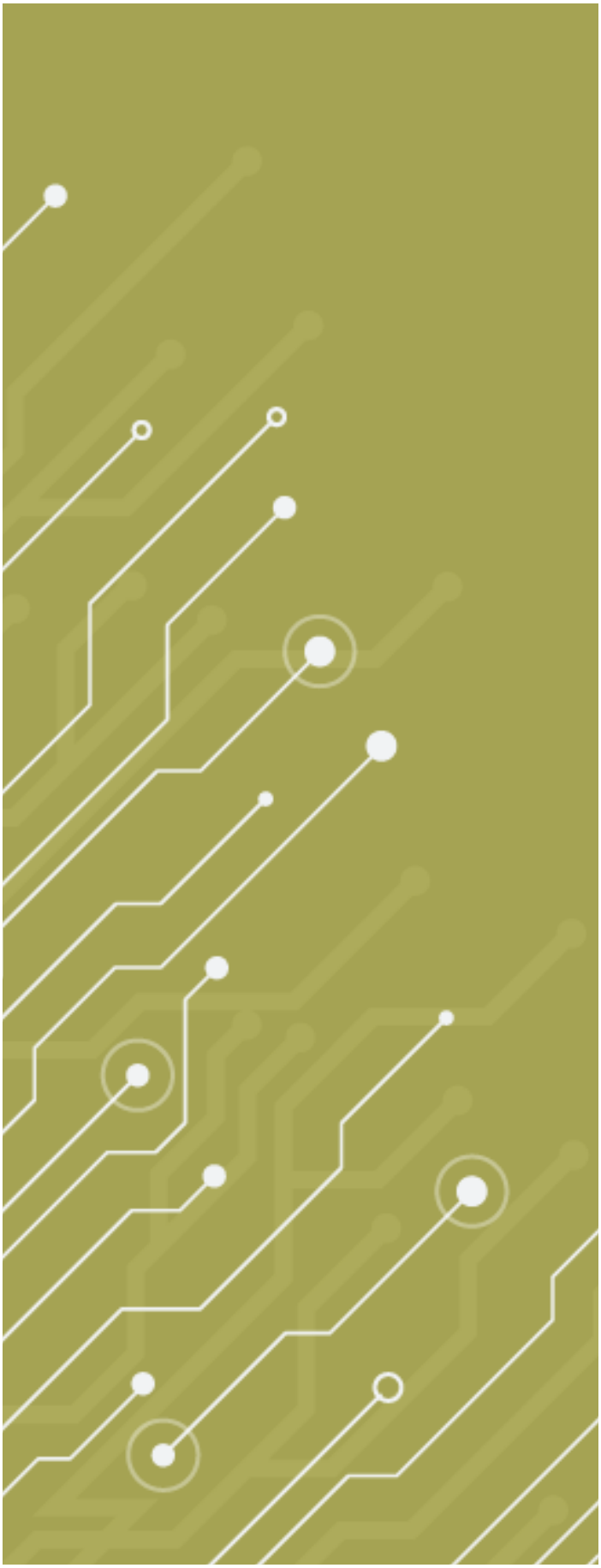
Cybersecurity conferences and meet-ups in Halifax often feature sessions dedicated to discussing the role of women in the industry, showcasing female experts, and offering mentorship opportunities. These events play an essential role in providing a platform for those looking to advance professionally while contributing to Halifax's cybersecurity footprint.

Halifax: The Place to Be

By offering a thriving tech ecosystem, strong educational resources, and a commitment to DEI and work-life balance,

Halifax is uniquely positioned as the best place to live and work in cybersecurity. As the city evolves its focus on collaboration, innovation, and inclusivity, it solidifies its reputation as a leading destination for cybersecurity professionals. More than just a career hub, Halifax is a city of charm, adventure, and pride—a place where forward thinking and purpose-driven professionals can find both community and clarity in a balanced, fulfilling lifestyle.

Holly DeWolf, Account Manager and Team Lead at GoSecure Inc., a dedicated professional specializing in building trusted relationships and delivering customized solutions to meet complex challenges. With a deep understanding of cybersecurity landscapes, Holly works closely with clients to develop strategic approaches that enhance security and resilience. Known for a commitment to excellence and a passion for problem-solving, Holly ensures that every solution is tailored to the unique needs of organizations, fostering confidence and long-term success in an ever-evolving digital world.



Kitchener-Waterloo: From Early Beginnings to the World's Leading Tech Ecosystem

by Albert Heinle

Summarizing Key Facts at a Glance

- **Early Beginnings:** Waterloo's technology hub began in the 1950s, starting with the University of Waterloo. This region has a long history of innovation and growth, contributing to its current status as one of the world's leading tech ecosystems.
- **Academic and Industry Collaboration:** With more than 42,000 students in the region, academia and industry work hand in hand. The Cybersecurity and Privacy Institute at the University of Waterloo is a prime example of this collaboration, fostering interdisciplinary research and training.
- **Billion-Dollar Companies:** BlackBerry, ESentire, Arctic Wolf, and OpenText are billion-dollar cybersecurity companies that originated in the Waterloo region. These companies have significantly contributed to the global cybersecurity landscape.

- **Quantum Computing Leadership:** Waterloo is a leader in quantum computing efforts, with institutions like the institute for Quantum Computing and the Perimeter Institute driving advancements in quantum technologies.
- **Startup Density:** Waterloo has the second highest startup density in the world, second only to Silicon Valley. This highlights the region's vibrant entrepreneurial environment.
- **Active Startup Ecosystem:** Waterloo has an active startup ecosystem, supported by organizations like the Accelerator Centre, that provide valuable resources, mentorship and funding to help startups thrive.
- **Technology job growth:** Waterloo has experienced a 46% growth in technology jobs over the last five years, making it one of the fastest-growing tech markets in North America.

Kitchener-Waterloo and its History of Building a Technology DNA

When walking through the park area of the Boardwalk, one would come across a large plaza marking the geographical separation line between Kitchener and Waterloo (commonly referred to as KW). Here, a statue of Ira G. Needles sits on a bench, holding a pen and paper that reads "150,000 Engineers—The Waterloo Plan." Ira G. Needles, a prominent figure in the development of the Waterloo region, is depicted in the artwork by George Bolieau, capturing the essence of his visionary spirit as he pens his 1956 speech. This would change the course of the region for the next decades. And, given Canada's population of around 16 million people at the time, this area, which comprises about 0.01% of the country's landmass, would have accounted for about 1% of the nation's engineers.

The plan did indeed work out in one way or another, significantly contributing to the growth of the Waterloo region. With the University of Waterloo, and businesses supporting and retaining talent, the area grew. Engineering demands constant innovation, including computing technology, software development, and data analysis. As early as 1967, the University of Waterloo established the school of Applied Analysis and Computer Science, effectively laying the foundation for future technological advancements. Together with co-op terms integrated into the programs since 1957, the academic knowledge received by the students was always augmented by practical applications.

Building on this strong foundation, the Waterloo region evolved into a hub of innovation and entrepreneurship. Over the decades, the continued concentration, attraction, and retention of talent inspired a thriving tech ecosystem that would eventually connect the region to the broader, interconnected world. Research In Motion (RIM), founded in the region, became one of the most significant tech employers. Despite its fall in the mobile phone market, RIM remains an important part of the technology history and the catalyst for many subsequent businesses in the region. Knowledge about the company and its founders became part of the official study guide for Canadian citizenship.

With information flowing freely between many endpoints, security became mission-critical, driving companies like RIM to prioritize practical implementation and innovation. This focus on cybersecurity attracted specialists from around the world, who were drawn to the region's growing tech ecosystem and opportunities for research and development.

The rise of industry giants and increase in investment have fostered a vibrant cybersecurity ecosystem.

Investment in the region has not stopped since. With cutting-edge institutions like the Perimeter Institute, the Institute for Quantum Computing, and the Communications Security Lab, Waterloo remains at the forefront of R&D in the security field.

The rise of industry giants and increase in investment have fostered a vibrant cybersecurity ecosystem. OpenText has established a widely respected and versatile cyber-practice, but the company did not start in the security space. While ESentire, the original inventors of Managed Detection and Response, has grown from a small team to the billion dollar corporation it is today. Arctic Wolf, a significant player in the industry, has its largest office and primary engineering hub in Waterloo. Magnet Forensics, which aids law enforcement agencies worldwide in conducting investigations, has recently gone public on the Toronto Stock Exchange. Networking security solutions like Auvik, Dejero and Sandvine have not only established themselves in the region but have also expanded their reach internationally. Other companies like McAfee, 1Password and Symantec

have opened local offices to benefit from the rich talent pool and the thriving tech environment.

Besides the giants, there are many cyber companies that have settled and are growing in the area as well. Agilicus, CoGuard, Cavelo, EliteSec Fairly.ai, to name a few. A full list of cybersecurity company logos has been recently compiled by the Waterloo EDC and can be found here.

Attracting and Retaining Cyber Talent

The Waterloo region and federal government have recognized the strength in this area, leading to investments and initiatives that foster growth in cybersecurity. In 2018, University of Waterloo opened the Cybersecurity and Privacy institute (CPI), which collaborates with other cybersecurity entities nationwide. For example, CPI collaborated with Kyndryl Canada to advance data privacy research and security. Meanwhile, national funds like the National Cybersecurity Consortium (NCC) inject capital into innovative projects from both industry and academia, a recent example being UPSCOPE, based out of the University of Waterloo, that looks to develop algorithms, tools and systems to tackle security and privacy.

Cybersecurity professionals are naturally curious people who want to hear from one another.

Existing companies, both giants and startups, are continuously strengthening the region's cybersecurity industry, leading to a flywheel effect that involves the need to grow and keep talent. The overall growth of the technology sector at large contributes to the ability to find early adopters and long-term customers for up-and-coming cybersecurity firms.

The investor landscape has not yet produced an institutional firm focused solely on cybersecurity in the area, but various angels, angel groups and venture capitalists are open and willing to invest in this market segment. Attracting and retaining talent will not be a problem for the next decade to come.

Institutions like the Accelerator Centre offer services to help startups grow and succeed. Taking advantage of the region's rich history and expertise in the field, advisors from these organizations have firsthand experience and are able to help with the building blocks of new cybersecurity companies in the region. In fact, the Waterloo region has the second highest startup-density in the world after Silicon Valley (source).

Meetups, Coffees and Conferences

Cybersecurity is ever-changing with the emergence of new technologies, evolving attack trends, and innovative approaches to ensure organizations can focus on what matters most to them: their revenue, operations and customers. As a result, cybersecurity professionals need to stay informed and keep abreast of the latest developments. But they don't just do it as an obligation, cybersecurity professionals are naturally curious people who want to hear from one another. And the Waterloo region offers a variety of different opportunities for that.

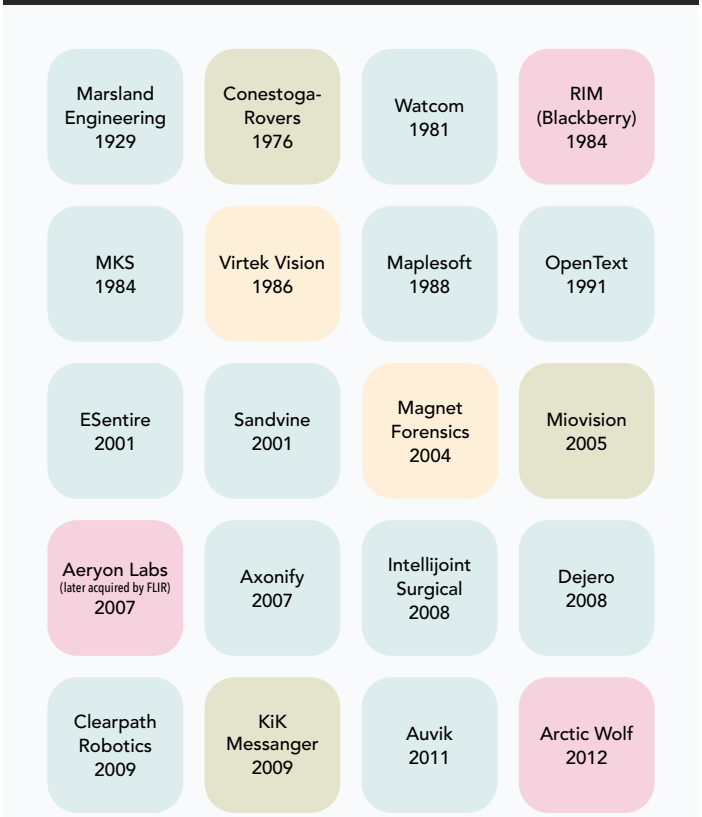
The CPI institute, as previously mentioned, holds an annual one-day conference that typically takes place in October. Past speakers have included representatives from corporations such as Magnet Forensics, BlackBerry, the public sector, and academia. In addition to inspiring talks and panels, students have the opportunity to contribute to the poster session and receive feedback from the seasoned professionals in the audience. These events play a crucial role in fostering collaboration, innovation, and professional development within the community.

Another example would be the KW Cybersecurity Meetup, which has been a cornerstone of the local cybersecurity community, providing space for professionals to connect and share knowledge. This group, which currently has about 1,250 members, met in person at the Arctic Wolf headquarters; it remained a vital networking platform as it adapted to virtual sessions during the pandemic.

As a startup hub, the Waterloo region hosts many events throughout the year ranging from beer mixers to panels with distinguished speakers. These events contribute to the tech ecosystem, offering chances for professionals to connect and exchange ideas.

In addition, numerous academic quantum and cryptography conferences are held in or around the University of Waterloo, where new ideas and approaches are regularly designed and discussed. These conferences are essential for advancing research and fostering innovation in the field.

Sample of successful technology companies founded in Waterloo region and founding dates



Challenges, Wish-lists and Future Outlooks

The Waterloo region has been cultivating its cybersecurity landscape for over 30 years, creating a robust foundation for future growth. However, rising housing-costs are among some of the greatest concerns for those who reside in the region, potentially deterring new talent and causing current professionals to worry about their children's ability to enter the housing market. This issue is common across industry in the region, not just cybersecurity.

As part of a wish-list, it would be beneficial to see more events and exchanges hosted or sponsored by local cybersecurity companies. While Blackberry frequently sponsors academic research symposiums, increased involvement from other firms in the region could facilitate new partnerships and exchange of ideas, aligning with the global trend of combining resources and services into more comprehensive solutions. Furthermore, institutional seed funding for new ideas in the cybersecurity space could drive significant innovation in the region.

On a federal level, additional incentives for non-cybersecurity companies to enhance their cybersecurity measures would benefit all industries and provide more opportunities for business among local companies. Active efforts are underway and positive outcomes are expected in the next few years, making local cybersecurity support more accessible.

The future outlook for the Waterloo region is promising. The industry is actively shaping trending topics like post-quantum cryptography. And Waterloo's diversified portfolio of talent, academic directions, and industry practitioners ensures a broad focus on cybersecurity efforts. The tech sector has grown by 46% in the last five years, and is expected to continue. But to maintain this competitive edge, the region must foster innovation and compete on the international stage. Canada is currently ranked as the fifth-largest cybersecurity hub globally, much can be attributed to the role of the Waterloo region, a trend likely to continue for years to come.

Dr. Albert Heinle is driven by a mission to combat the global surge of data breaches and misconfigurations. Albert co-founded CoGuard in 2020 and serves as Chief Technology Officer. Prior to CoGuard, Albert held development positions at FLIR Systems, Inc., Aeryon Labs and Sortable. He completed a Ph.D. in Computer Science at the University of Waterloo in the area of Symbolic Computation.

Montreal: A Thriving Tech and Cybersecurity Hub

by David Pigeon

Montreal is one of Canada's most dynamic technology hubs, it is home to breakthrough advances in artificial intelligence, a world-class video game industry, and a rapidly evolving cybersecurity scene. What sets the city apart isn't just the diversity of its sectors, but the way they intersect, collaborate, and scale together.

Montreal as a Tech Hub

This reputation is built on a foundation of strong academic institutions, a multilingual and highly skilled workforce, and a steady flow of ideas from both startups and established firms. Whether in applied research, software development, or digital infrastructure, Montreal has become a magnet for forward-thinking companies and talent.

What truly powers this ecosystem is a culture of collaboration between universities, entrepreneurs, researchers, and global enterprises. It's a city where innovation isn't confined to labs or boardrooms, but thrives in meetups, Capture the Flag (CTF) competitions, co-ops, and everyday partnerships that move ideas into action.

Some of the industries shaping Montreal's tech scene:

- **Artificial Intelligence**—Home to Mila (Yoshua Bengio's AI research institute), IVADO, and Meta AI Research (FAIR), the city has become a global leader in AI research and development.
- **Video Game Industry**—With major studios like Ubisoft, WB Games, Eidos, Behaviour Interactive, and Gameloft, Montreal has built a reputation as a world-class gaming hub.
- **Fintech & Blockchain**—Companies like Nuvei and Lightspeed are driving digital payment solutions and business innovation.
- **Cybersecurity**—A growing sector supported by local startups, research institutions, and major enterprises.

Montreal is more than just a tech city, it's widely seen by those in the ecosystem as a launchpad for innovation, where AI, gaming, cybersecurity, and fintech collide to shape the future.

A Community-Driven Cybersecurity Ecosystem: With Olivier Bilodeau

To better understand what makes Montreal's cybersecurity community so unique, we spoke with Olivier Bilodeau, a well-known figure in the local scene. Olivier is a researcher at Flare Systems, co-founder of MontreHack, and the president of NorthSec, one of the largest CTF competitions in North America.

At the core of Montreal's cybersecurity strength lies its passionate and engaged community. Events like NorthSec, MontreHack, OWASP Montreal, and BSides Montréal are central pillars of this ecosystem–fostering education, competition, and collaboration. These gatherings are more than just technical conferences, they are incubators for future talent, bringing together security experts, students, and researchers in a highly interactive setting.

NORTHSEC: FROM LOCAL PASSION TO GLOBAL RECOGNITION

Originally founded as HackUS at Université de Sherbrooke, NorthSec has evolved into one of the largest CTF competitions in North America. What started as a student-run event in a university cafeteria has transformed into a world-class cybersecurity competition and conference, attracting over 1,250 participants annually. The event serves as both a proving ground for elite cybersecurity talent and a hub for industry networking.

Over time, NorthSec has evolved beyond just competition. It now offers advanced training workshops, panel discussions, and interactive security talks--ensuring that participants receive both hands-on experience and industry insights. The event is also known for fostering a tight-knit community where professionals, students, and researchers come together to push the boundaries of cybersecurity.

At the core of Montreal's cybersecurity strength lies its passionate and engaged community.

What truly sets NorthSec apart is its commitment to technical excellence. Unlike many other CTF competitions, its challenges are entirely custom-built, pushing even the most experienced participants to their limits. Additionally, the inclusion of a hardware hacking village, reverse engineering sessions, and lock-picking workshops adds an extra layer of practical security training.

> "We started in a cafeteria with a few motivated students. Today, NorthSec brings together 1,250 participants, hosts a top-tier conference, and runs a CTF recognized around the world. It's Montreal shining in the cybersecurity space."
>
> —*Olivier Bilodeau*

MONTREHACK: A HANDS-ON TRAINING GROUND FOR CYBERSECURITY PROFESSIONALS

MontreHack is a monthly cybersecurity training meetup that takes a unique approach, rather than passive lectures, participants work in teams to solve real-world security challenges. It has become a key entry point for aspiring cybersecurity professionals, allowing them to develop skills, connect with experts, and prepare for larger competitions like NorthSec.

MontreHack plays a vital role in bridging the gap between theory and practice. It offers security enthusiasts and professionals a place to hone their penetration testing, reverse engineering, and digital forensics skills. Many NorthSec competitors have trained at MontreHack before competing, proving its effectiveness as a preparatory ground for the best talent in the field.

Another unique aspect of MontreHack is its annual holiday challenge exchange, where participants design and solve challenges for one another, fostering a strong culture of collaboration and continuous learning. The event has inspired similar training programs in other cities, positioning Montreal as a leader in hands-on cybersecurity education.

> "Events like MontreHack, NorthSec, and OWASP Montreal aren't just conferences. They're talent incubators, places where the next generation of cybersecurity experts is forged."
>
> —*Olivier Bilodeau*

BSIDES MONTRÉAL & CYBERCHILL: BUILDING A STRONGER COMMUNITY

BSides Montréal provides a community-focused alternative to large industry events. Held alongside GoSec, it fosters deeper, technical discussions in an intimate setting where professionals can connect, share insights, and contribute to the community without the distractions of a vendor-driven agenda.

Montreal also benefits from regional cybersecurity hubs, such as CyberChill in Drummondville, founded by Dominic Villeneuve, which supports knowledge-sharing and networking among security professionals across Quebec.

Cybersecurity Employers Powering the Ecosystem

Montreal's strength doesn't just lie in its events or startups, it's also home to a strong core of well-established firms that provide cybersecurity careers across all disciplines. Companies like CGI, IBM, PwC, EY, and Google have made significant investments in the city, with Google actively involved in Montreal through its Mandiant and Threat Analysis Group (TAG) operations. These firms collectively employ thousands of professionals in roles ranging from security analysts and architects to compliance officers, incident responders, and penetration testers.

They offer not only stability, but also pathways for growth, helping new graduates and experienced professionals in developing their skills within structured, high-impact environments. These companies play a vital role in retaining local talent and offering opportunities to work on national and global projects, all while staying anchored in Montreal.

At the same time, a growing number of mid-size and enterprise-class firms are helping to democratize access to cybersecurity services. These organizations are making cybersecurity more accessible to SMBs, non-profits, and municipalities who might otherwise lack the in-house capacity to defend themselves effectively. This mix of large, mid-sized, and emerging players contributes to a balanced and sustainable ecosystem, ensuring that cybersecurity isn't just the domain of tech giants, it's woven into the city's economic fabric.

Challenges Facing Montreal's Cybersecurity Ecosystem

Post-pandemic, one of the challenges that stands out and is echoed by community leaders like Olivier Bilodeau is the struggle to find suitable spaces for meet-ups and events. "Before COVID, it was easier to get large rooms in big offices," Olivier shared. "Now, even companies with space aren't offering them because

their employees are remote, and they don't want to re-open just for occasional events." This has made it increasingly difficult for grassroots cybersecurity meetups like MontreHack, OWASP Montreal, and even parts of NorthSec to find accessible, affordable venues.

Olivier pointed out that access to free or low-cost venues used to be a non-issue thanks to places like the Notman House or company-provided meeting spaces. But now, community organizers are facing a logistical barrier that directly impacts the frequency and reach of these events. Despite this, groups like CyberEco are stepping in to help by lending out space when possible, proving once again that community support is what keeps Montreal's cybersecurity scene alive and growing.

FUNDING & INVESTMENT GAPS

Funding remains a consistent hurdle for many cybersecurity startups in Montreal. While sectors like AI and fintech have gained widespread investor attention, cybersecurity often flies under the radar. Olivier touched on this reality, noting that although there's innovation happening, startups in this space often face an uphill battle securing the capital they need to grow. "There are great ideas here," he said, "but unless you're working on something that's buzz worthy like block chain or generative AI, it's harder to get the right doors to open."

This funding gap limits not just the pace at which local companies can scale, but also their ability to attract and retain top talent, purchase tooling, or expand internationally. The ecosystem needs stronger bridges between innovators and investors who understand the value and urgency of developing cutting-edge security technologies.

BRIDGING THE INDUSTRY-ACADEMIA GAP

Montreal is home to several highly regarded universities, but many graduates stepping into the workforce still lack the practical cybersecurity skills required by employers. Olivier mentioned that while theory is essential, "you don't always learn reverse engineering or hands-on incident response at school. The labs are often too basic, or everyone just copies the same answers."

Community initiatives like MontreHack help fill this gap by offering real-world problems in team settings, but there is a growing need for deeper, structured collaboration between industry and academia. More internships, co-op programs, and industry-sponsored research projects would better prepare students and strengthen the talent pipeline for the city's security ecosystem.

Future Trends & Opportunities for Montreal

The momentum behind Montreal's cybersecurity ecosystem shows no signs of slowing. While challenges remain, the foundations are solid and the opportunities are massive. What's clear is that this city is not just following the cybersecurity curve; it's helping to bend it.

One of Montreal's strongest assets lies in its bilingual, globally-minded workforce. As the world continues to digitize, companies are expanding their operations beyond borders and Montreal offers a rare advantage. This cultural and linguistic duality adds a richness to Montreal's identity, giving it a natural fluidity to connect across borders and build trust in diverse markets.

There is a growing need for deeper, structured collaboration between industry and academia.

Montreal is also well-positioned to lead in AI-driven cybersecurity. While some sectors are only starting to explore machine learning, local researchers have been experimenting with it for years. The city's AI backbone bolstered by institutions like Mila offers fertile ground for developing next-generation detection algorithms, behavioral analytics, and automated threat response tools.

On the startup front, the emergence of cloud security, DevSecOps, and threat intelligence-focused firms marks a natural evolution. As organizations move to cloud-native infrastructure, the need for agile, intelligent, and automated security solutions grows. Montreal's startup scene is rising to meet that demand, with new companies appearing at the intersection of development, operations, and security.

Finally, collaboration remains the city's secret weapon. Public-private partnerships, inter-university research projects, and community-led initiatives like MontreHack and OWASP Montreal continue to bridge gaps and open doors. Whether it's a policy paper, a CTF challenge, or a cybersecurity co-op program, there's a shared understanding in Montreal: the future of cybersecurity is built together.

With its deep talent base, strong academic ecosystem, innovative startups, and collaborative spirit, Montreal is more

PHOTO: OTTAWATOURISM

Ottawa-Gatineau: Canada's Twin Engines of Tech and Cybersecurity

by François Guay

Ottawa and Gatineau form a single and dynamic tech ecosystem, yet too often they've been treated as separate players, when in reality, this bilingual capital region is a singular powerhouse. With Ottawa on one side of the river driving national policy and Gatineau on the other cultivating Quebec's innovation, their combined strengths create a cross-border hub of technology and cybersecurity. It's time to move beyond outdated rivalries. By aligning strategies, investments, and talent initiatives, Ottawa-Gatineau can emerge as one united force – not just competing in the global tech arena, but leading it. Collaboration across the municipal and provincial divide will unlock the region's full potential, allowing it to truly "build the future – together."

Home to Canada's seat of government and the majority of key federal agencies — including Canadian Security Intelligence Service (CSIS), Communications Security Establishment (CSE), National Defence (DND), and Public Safety, Ottawa-Gatineau is uniquely positioned to lead the development of a fully integrated national cybersecurity strategy.

A Region Rich in Tech Talent

With over 90,000 technology professionals in the workforce, Ottawa-Gatineau boasts one of the highest concentrations of tech talent in North America. According to CBRE's 2024 Tech Talent report, 12.3% of all jobs in the area are in tech, tying San Francisco for top spot on the continent and more than double the North American average. This critical mass of expertise did not appear overnight: the region added 31,300 tech jobs in the last five years alone, representing a growth of 51.7%. Such depth of talent spans software engineers, AI researchers, cybersecurity analysts, and more. It's no wonder Ottawa ranks as a top-ten tech market overall and #1 for women's representation in tech jobs (24%). This diverse, highly educated talent pool, fed by local universities and a rich startup culture – is the engine driving innovation across Ottawa-Gatineau's public and private sectors. It fuels breakthroughs in emerging fields from cybersecurity and artificial intelligence to autonomous vehicles and IoT. The synergy between Ottawa's Kanata North Technology Park and Gatineau's growing AI & cyber sector creates fertile ground for new ideas. In short, the region's talent advantage is a magnet for companies and a foundation for sustained high-tech growth.

The region added

31,300

tech jobs in the last five years alone.

City Initiatives to Foster Innovation and Retain Talent

The City of Ottawa has made high-tech growth a pillar of its economic strategy. Kanata North, the city's sprawling 550-hectare tech park, was recently designated a Special Economic District in Ottawa's Official Plan. Home to over 540 companies and 30,000+ jobs in Ottawa's west end, Kanata North contributes more than $13 billion annually to Canada's GDP. By recognizing it as a special district, Ottawa signals the importance of this hub to the city's identity and its national image. The city is also investing in infrastructure and policies to make Ottawa a magnet for tech workers – promoting affordable living, quality transit, and co-op programs that keep new graduates local. Ottawa's cost of doing business remains among the lowest in North America, with tech wages around $60,000 CAD on average, making it an attractive place for startups and multinationals alike.

Across the river, the City of Gatineau has been pursuing its own innovation ambitions. It is taking advantage of its proximity to Ottawa along with Quebec's R&D incentives to pitch a Cybersecurity Innovation Zone, aiming to cluster companies and researchers in Gatineau. While the Province of Quebec has put this proposal on hold in 2023 due to insufficient private-sector commitments, Gatineau hasn't slowed its efforts. The city, through its agency ID Gatineau, continues to attract and fund tech enterprises with strategic support. For example, ID Gatineau's Local Fund offers up to $300,000 in financing to help startups launch or expand. Gatineau also benefits from Quebec's competitive tax credits for R&D and a cost-effective business climate that draws entrepreneurs and global firms to the Outaouais region. Both cities actively promote bilingual talent development and quality of life – key factors not only for attracting new firms, but also for retaining skilled workers who might otherwise be lured to larger markets.

INVEST OTTAWA AND AREA X.O: CATALYSTS FOR GROWTH

As Ottawa's lead economic agency, Invest Ottawa has launched thousands of startups and scale-ups, creating over 6,350 jobs and attracting $293 million in foreign investment since 2012. Its innovation hub, Bayview Yards, anchors this success with incubation, acceleration, and corporate collaboration.

A key asset is Area X.O, a 1,866-acre smart mobility test site and Canada's largest autonomous vehicle R&D facility. Equipped with 5G networks and real-world testing environments, it became a NATO DIANA test centre in 2024 — putting Ottawa-Gatineau on the map for defense and dual-use tech innovation.

Together, Invest Ottawa and Area X.O offer a full innovation pipeline from startups to multinationals, and in partnership with ID Gatineau, promote the region as a unified cybersecurity cluster on the global stage. By pooling their assets through Kanata North's telecom heritage, downtown Ottawa's government market, Gatineau's skilled workforce and cost advantages – they aim to attract even more global cyber firms, talent, and investment to Canada's capital region.

ID GATINEAU: ACCELERATING INNOVATION AND DRIVING ECONOMIC DEVELOPMENT IN OUTAOUAIS

ID Gatineau, the City of Gatineau's economic development agency, mirrors Invest Ottawa's role by helping businesses launch, expand, and create sustainable jobs. It offers strategic advice, mentorship, and access to financing. This organization has played a key role in securing major investments like Telesat's new campus, bringing 300 high-skilled jobs to the region.

While Gatineau's proposed cybersecurity innovation zone is on hold, ID Gatineau continues to grow the region's cyber niche through partnerships, events, and support programs. Leveraging Université du Québec en Outaouais (UQO), Cégep training, and proximity to federal cybersecurity hubs, it promotes Gatineau as a cost-effective, innovation-ready location. ID Gatineau ensures the Quebec side of the capital region remains a vital part of this twin-city tech engine by working closely with Invest Ottawa and IN-SEC-M.

Cybersecurity Communities and Talent Networks

Ottawa-Gatineau is home to over 90 cybersecurity firms and eight post-secondary institutions feeding a strong, collaborative cyber talent ecosystem. But just as vital are the grassroots communities that connect professionals, students, and employers.

OWASP Ottawa runs monthly meetups at uOttawa, offering hands-on demos and discussions for developers and security pros. These inclusive events keep skills sharp and foster community knowledge sharing.

WiCyS (Women in CyberSecurity) has an active presence through its Ontario affiliate and Carleton University chapter, hosting events that help bridge the gender gap in cyber, contributing to Ottawa's top ranking for women in tech (24%).

The Ottawa Cyber Security Meetup (with over 1,700 members) adds to this dynamic landscape, hosting events that bring together professionals across sectors for networking, career growth, and industry insight.

In-Sec-M, based in Gatineau, brings together industry, academia, and government across Canada. Locally, it partners with Invest Ottawa and ID Gatineau to connect regional firms to national cyber opportunities. Training is also hands-on and accessible. CyberQuébec at Cégep de l'Outaouais helps SMEs strengthen their cyber posture through applied research. Algonquin College, La Cité, and others provide certificate and diploma programs that supply a steady stream of skilled graduates to the workforce.

Together, these meetups, training programs, and networks create a tightly knit, inclusive cybersecurity ecosystem — one that attracts companies, supports professionals, and fuels the region's continued growth as a cyber hub.

Federal Government's Footprint and Funding

As Canada's capital, Ottawa-Gatineau benefits from a dense federal presence that fuels demand for cybersecurity innovation and provides steady funding for R&D.

On the Ottawa side, agencies like CSE and Shared Services Canada drive demand for secure digital solutions, often piloting tech with local firms. Major players like the Canada Revenue Agency, Treasury Board, and DND also anchor Ottawa's role in cybersecurity and defense innovation.

On the other hand, federal departments like Employment and Social Development Canada, Public Services and Procurement Canada, and Environment and Climate Change Canada are headquartered in Gatineau, all of which require robust IT and security services. The city also benefits from coordinated federal-provincial investments, like those supporting Telesat's new campus.

Most critically, the federal government presents real-world challenges, from digital ID to critical infrastructure, making Ottawa-Gatineau a national test bed for cyber innovation and public-private collaboration.

Finally, Ontario's Critical Technology Initiatives ($107 million) and the Cybersecurity Excellence Initiative support startups and scale-ups across Ottawa. In Quebec, federal programs have filled the gap through targeted investments and research funding (e.g., NCC, NSERC, IRAP) while the proposal for a Cyber Innovation Zone is still pending.

Academic Engines: Cyber Innovation Through Education

Ottawa-Gatineau's universities and colleges are central to its cybersecurity edge — producing talent, driving research, and partnering with industry:

- **University of Ottawa (uOttawa):** Its Cyber Hub unites 40+ researchers across disciplines. The IBM Cyber Range offers crisis simulation training, while partnerships (e.g. with the University of Luxembourg) keep research global and bilingual talent flowing.
- **Carleton University:** A hub for security research, Carleton's CyberSEA Lab and Cyber Reference Lab (with General Dynamics) let students tackle real-world defense

scenarios. Programs in AI, privacy, and cybersecurity bridge tech and business needs.

- **UQO (Université du Québec en Outaouais):** With 20+ years in cyber research, UQO delivers French-language cyber programs and is part of Quebec's broader cyber resilience network (IMC²). Its holistic approach prepares graduates for roles in both government and industry.
- **Cégep de l'Outaouais & La Cité:** These colleges offer hands-on diplomas and certifications in cybersecurity and networks, while CyberQuébec supports SMEs with applied research and student engagement. Algonquin College adds to this pipeline with its cyber analyst program.

Joint R&D across institutions, often involving the National Research Council (NRC), Ericsson, and others, turns academic insight into startups and industry pilots. The region's post-secondary network forms a full talent pipeline, from diploma to PhD, anchored in real-world innovation.

Major Players in the Cyber Tech Sector and Recent Highlights

The Ottawa-Gatineau region hosts an impressive mix of multinational tech companies, homegrown unicorns, and emerging startups. This critical mass of companies provides jobs, investment, and global connections that sustain the ecosystem. Some major tech and cybersecurity players and their recent developments include:

Shopify – Ottawa's poster child for startup success, now a global e-commerce giant. Headquartered downtown, Shopify has thousands of employees and continues to innovate in online retail platforms. In 2023, Shopify refocused its core business by divesting some logistics operations, but also announced a $5 million investment in a local AI research partnership, underscoring its commitment to Ottawa and the broader Canadian tech community. Shopify's presence has spawned a generation of spin-off entrepreneurs and talent who have gone on to start new ventures in the region.

BlackBerry QNX – Based in Kanata, QNX (a division of BlackBerry) develops secure operating systems running in over 175 million vehicles worldwide. It anchors Ottawa's autonomous vehicles cluster alongside 100+ other companies. Recently, BlackBerry announced plans to separate or sell off parts of its business, but QNX remains a crown jewel due to its critical role in automotive software. In 2024, QNX partnered with TTTech Auto to develop advanced driver safety systems in Ottawa, expanding its R&D team. The autonomous shuttle tests on Ottawa streets and the annual CAV Canada conference are testaments to QNX's leadership and the city's commitment to intelligent transportation.

Fortinet – A global cybersecurity vendor known for firewalls and network security, Fortinet has a significant R&D presence in Ottawa. It quietly grew its Ottawa office through acquisitions of local firms and now employs hundreds of engineers working on cutting-edge security software. Fortinet's Canada Innovation Centre in Kanata was bolstered in 2023 as the company began a push into secure SD-WAN and cloud security development. The firm is actively hiring in Ottawa for roles in threat intelligence and software development. Its presence provides local professionals an avenue to work on global cybersecurity challenges without leaving the region. Fortinet also runs an Early Talent program with Carleton University, offering internships that often lead to full-time jobs.

Telesat – One of Ottawa's legacy tech companies (founded in 1969), Telesat is a satellite communications leader. While headquartered in Ottawa, its major new project Lightspeed, is landing in Gatineau: a $6.5 billion low Earth orbit satellite network with a campus opening in late 2025. This project, supported by federal and Quebec loans, is creating 300 jobs in Gatineau for satellite operations and engineering. Telesat's Lightspeed aims to provide global broadband and secure communications, including for Arctic sovereignty and defense. The company's expansion reinforces the region's status in aerospace and communications tech. It's also a prime example of cross-border synergy – Ottawa provides much of the corporate leadership and R&D, while Gatineau reaps new jobs and facilities.

Ciena – A U.S.-based networking systems company, Ciena has its largest R&D center situated in Ottawa (after acquiring local startup Nortel's optical business). Ciena's Ottawa lab drives innovation in high-speed fiber optics, crucial for secure and reliable internet backbone. In 2024, Ciena announced a $50 million expansion of its Ottawa campus to accelerate work on 800G optical networks and advanced research in quantum-safe encryption for data in transit. This investment will add jobs and deepen Ottawa's expertise in telecommunications.

Thales Canada & General Dynamics (GD) – Both companies have sizable operations in Ottawa, focusing on defense and security. Thales (with a Kanata office) works on secure communications and critical systems (like Ottawa's light rail signaling). General Dynamics (with over 1,000 staff in Ottawa) develops mission systems for the Canadian Armed Forces and others. GD's launch of the Cyber Lab at Carleton is one example of their community engagement. In 2025,

Thales announced Ottawa would be one of its global AI research hubs for defense applications. These defense primes not only provide high-paying jobs but also pull local suppliers and startups into their supply chains, stimulating smaller tech firms.

EMERGING STARS

The region also has a cadre of high-growth startups and scale-ups making waves:

Field Effect Software – An Ottawa-based cybersecurity company offering an all-in-one threat monitoring platform. Field Effect secured $34.5 million in Series A funding in late 2022 to accelerate global expansion. In 2023–24 it used a $30 million growth facility to acquire a U.K. security firm, expanding its reach. The company, founded by ex-CSE experts, exemplifies the spin-off innovation coming from federal talent.

MindBridge AI – A fintech-security crossover, MindBridge's AI-powered auditing platform detects anomalies in financial data. Recognized as one of Canada's fastest-growing firms in 2024, MindBridge has clients worldwide and is deeply rooted in Ottawa's AI scene. It frequently partners with University of Ottawa researchers on AI explainability and was showcased at the Impact AI conference in Ottawa (which itself has become Canada's fastest-growing AI conference).

Assent – An Ottawa compliance software company (recent unicorn) that ensures supply-chain security and regulatory compliance for global manufacturers. After raising over $350 million in 2021, Assent continued hiring in Ottawa through 2023, tapping into local software talent.

Kinaxis – A supply chain software leader based in Kanata, which isn't a pure cybersecurity firm but deals with secure supply chain planning. Kinaxis has been expanding its workforce and in 2023–24, announced new AI features for its platform, developed in its Ottawa R&D center.

This is only a sampling – other notable names include Amazon (with a growing Ottawa office focusing on cloud services), Nokia and Ericsson (driving 5G R&D), IBM (where Ottawa is a key site for IBM Canada, especially after acquiring Cognos), Kanata's L-Spark Accelerator (which has spun out companies in SaaS and cyber), and more. In sum, Ottawa-Gatineau's company landscape ranges from giants to startups, all feeding the innovation cycle. A recent (January 2025) city economic snapshot noted over 1,800 knowledge-based companies in the region employing 91,000+ people in tech-related roles, a remarkable density.

To put some of these key players in perspective, below is a snapshot of selected organizations driving Ottawa-Gatineau's cyber-tech ecosystem:

Name	Type	Role in Ottawa-Gatineau Tech Ecosystem
Kanata North Tech Park	Special Economic District (Ottawa)	Canada's largest tech park with 540+ companies; 30,000+ jobs generated and $13 billion+ GDP output. Now recognized in Ottawa's Official Plan to spur further growth.
Invest Ottawa & Area X.O	Economic Dev. Agency & R&D Facility	Lead incubator/accelerator, created 6,350+ jobs since 2012. Operates Area X.O, an 1,866-acre smart mobility/cyber test range (now a NATO DIANA site). Catalyzes startup growth, foreign investment, and tech commercialization.
ID Gatineau	Economic Dev. Agency (Gatineau)	Supports business setup/expansion in Gatineau with coaching and funding. Key partner in cross-border initiatives. Helped attract Telesat's new campus (300 jobs) and runs local funds up to $300k for startups.
Communications Security Establishment (CSE)	Federal Agency (Ottawa HQ)	Canada's cyber intelligence and security agency. Large Ottawa footprint that drives demand for cybersecurity solutions. Through its Cyber Centre, it engages with industry and academia on cyber defense challenges.
University of Ottawa (Cyber Hub)	Academic & Research	Trains 1,500+ HQP (highly qualified professionals) in cyber. Houses the IBM Cyber Range for immersive cyber crisis training. Active in multidisciplinary cybersecurity R&D and talent development.

Table continues on the next page.

Name	Type	Role in Ottawa-Gatineau Tech Ecosystem
Université du Québec en Outaouais (UQO)	Academic & Research	20+ years in cybersecurity research and training. Offers specialized cyber programs (e.g. DESS in cybersecurity) and adopts a holistic cyber curriculum. Contributes French-language cyber talent and research in Outaouais.
Shopify	Homegrown Tech Company (Unicorn)	E-commerce platform leader headquartered in Ottawa. Puts Ottawa on the map globally; invests in the local tech ecosystem (e.g., funding AI, participating in SaaS North). Employs thousands; beacon for talent attraction.
BlackBerry QNX	Major Company (Automotive Software)	Develops secure operating systems for autonomous and connected cars. Anchors a cluster of over 100 Connected and Autonomous Vehicles (CAV) firms in Ottawa. Partners with carmakers and tech firms, leveraging Ottawa's Area X.O for testing.
Fortinet	Major Company (Cybersecurity)	Global cybersecurity vendor with Ottawa R&D hub. Hiring and expanding in Ottawa, the company is working on next-gen network security and zero-trust solutions. Engages with local universities on talent pipeline.
Telesat	Major Company (Satellite Comm)	Ottawa-based satellite operator investing $6.5 billion in Lightspeed LEO network. New Gatineau campus is opening in 2025 with 300 jobs, which enhances the region's space-tech profile and partnerships (federal and Quebec-backed).
Field Effect	High-Growth Startup (Cybersecurity)	Ottawa startup providing holistic cyber threat monitoring (Covalence platform), raised $34.5 million Series A funding in 2022. The company is expanding globally and through acquisitions. Founded by former intelligence experts, Field Effect is keeping local cyber talent engaged.
MindBridge AI	High-Growth Startup (AI/Cyber)	Ottawa fintech/cyber startup using AI for fraud and anomaly detection in finance. Recognized among fastest-growing tech firms. Embodies Ottawa's AI prowess and is often featured at Impact AI conference.

(Sources: Invest Ottawa; City of Ottawa; Area X.O; Canada.ca; Invest Ottawa Blog; KNBA; Businesswire; PRNewswire.)

Industry Events Fueling Collaboration and Growth

Ottawa-Gatineau's tech vitality is also evident in the high-profile industry events it hosts annually. These conferences and meetups not only showcase the region's expertise but also foster the connections that drive business and innovation:

BSides Ottawa – A flagship community-driven cybersecurity conference, BSides Ottawa has grown into Canada's largest grassroots security event. Organized by local volunteers and enthusiasts, it provides an open platform for both seasoned experts and newcomers to present research, run workshops, and engage in hacking challenges. BSides Ottawa 2024, for instance, was a sold-out affair with hundreds of attendees, and BSides Ottawa 2025 is scheduled for Nov 20–21 at the Ottawa Conference & Event Centre (OCEC) – a move to a bigger venue reflecting its rising popularity. The event's inclusive vibe and low cost (often under $50) lower barriers for participation. Many credit BSides for seeding new ideas and even start-ups – a talk at BSides might spark a collaboration that leads to a venture. It also helps companies scout local talent in an informal setting. Overall, BSides embodies the strong infosec community spirit in Ottawa-Gatineau.

CANSEC – Each spring, Ottawa hosts CANSEC, Canada's premier global defense and security trade show. Held at the EY Centre near the airport, CANSEC draws over 12,000 attendees and 40+ international delegations from military, law enforcement, and industry. It's the place in Canada to showcase new defense tech, from armoured vehicles to cybersecurity software, and to connect with procurement officials. Ottawa's defense contractors and security startups benefit immensely from this at-home

exposure. CANSEC is organized by the Canadian Association of Defence and Security Industries (CADSI) and has been in Ottawa since 1998. Its significance to the region is huge: it reinforces Ottawa's brand as a defense innovation hub and brings global customers literally to the city's doorstep. Local firms often align product launches or demos with CANSEC to capture this audience. And beyond the expo floor, there's an entire week of side events and VIP meetings that stimulate investment and partnership deals. In essence, CANSEC puts a spotlight on Ottawa-Gatineau's dual-role as Canada's political capital and a defense tech capital.

SAAS North – In the software startup realm, SAAS North has emerged as the Canadian hub for SaaS (Software-as-a-Service) companies. Co-founded by Ottawa's L-Spark accelerator, it has been held in Ottawa's Shaw Centre every year since 2016. By 2024 it became the largest in-person SaaS conference in Canada, drawing over 2,000 attendees and 800 companies for two days of networking and talks. Founders, investors, and corporate innovators from across the country (and beyond) gather in Ottawa each November for SAAS North, making it a key event for deal-making and learning the latest in scaling tech businesses. The conference's growth mirrors Ottawa's own emergence as a SaaS hotbed – with companies like Shopify, Klipfolio, ReWind, and Assent built here. SAAS North mixes practical how-to scaling advice with big-name keynotes (recent editions featured CEOs from unicorn startups, partners from top VC firms, etc.). For Ottawa entrepreneurs, it's a chance to connect without flying to Silicon Valley or Toronto; for outsiders, it's often a first look at Ottawa's vibrant startup scene. The 2024 edition introduced fun pitch events like "The Masked Investor" and "Founders Feud" to spice up the agenda. This blend of business and creativity keeps SAAS North engaging and also showcases Ottawa's collaborative culture in tech.

OTHER NOTABLE EVENTS

The region's event calendar is packed. BSides Ottawa (cybersecurity) and SAAS North (software) as mentioned, but also:

Impact AI – Canada's fastest-growing AI conference, held in Ottawa, highlighting the latest in artificial intelligence and often featuring local startups and researchers.

CAV Canada – An annual conference on Connected and Autonomous Vehicles co-hosted by Area X.O and partners, underscoring Ottawa's leading role in autonomous tech.

Defence and Security Breakfasts by local chambers, Invest Ottawa's AccelerateOTT summit for entrepreneurs, and sector-specific meetups (e.g. Health Tech, GameDev).

CIS – The Canadian Identity Summit – which holds an annual event focused on the IAM space, bridging government, academia, and the private sector.

Even mainstream business events like TiECon Canada or the Ottawa Business Journal's Techopia Live sessions contribute to cross-pollination of ideas.

Across the river, Gatineau has begun hosting the Outaouais Tech Summit and partnering with Ottawa events to ensure Francophone inclusion.

These events and forums are more than just conferences; they are catalysts that strengthen networks across start-ups, government, academia, and industry. The knowledge shared on stage often finds its way into new strategies back at the office or lab. The contacts made over coffee breaks lead to partnerships or hires. The robust event scene in Ottawa-Gatineau is a reflection of a mature and collaborative ecosystem – one where stakeholders actively engage with each other to push the envelope of innovation.

Federal Capital Synergy: A Unique Advantage

The Ottawa-Gatineau tech ecosystem is unlike any other in Canada due to the constant interplay with the federal government and national institutions. The presence of policymakers, regulators, and large public sector customers in the same city means tech innovations here can quickly influence (and be influenced by) government priorities. For example, when Canada's Cyber Security Innovation Network fund or an AI Advisory Council was established,

The presence of policymakers, regulators, and large public sector customers in the same city means tech innovations here can quickly influence (and be influenced by) government priorities.

Ottawa companies and universities were at the table shaping those conversations. Likewise, federal adoption of cloud computing, or digital ID initiatives, provides savvy Ottawa firms a home advantage before scaling outwards.

This synergy is evident in initiatives like the Ontario–federal joint investments in critical tech, and the quick alignment between Innovation, Science and Economic Development Canada (ISED) and local economic agencies on attracting companies. A case in point: when a foreign cybersecurity firm is deciding on where to establish a Canadian office, they don't just recognize Ottawa-Gatineau as a talent pool, but also its proximity to federal contracts and national R&D centers (like NRC labs, Defense Research, Development Canada, etc.). The combined marketing by Invest Ottawa and ID Gatineau emphasizes this two-in-one value: access to Ottawa's federal ecosystem and Quebec's innovation ecosystem in one region.

Conclusion: One Capital, Infinite Possibilities

Ottawa-Gatineau stands today as a twin-city powerhouse of technology and cybersecurity, where government, industry, and academia intersect to create something greater than the sum of their parts. The region's strengths – a deep talent bench, supportive city initiatives, flagship organizations like Invest Ottawa/Area X.O and ID Gatineau, active professional communities, strong federal backing, top-notch universities, and a roster of global and local tech companies – all reinforce each other. This CyberTowns report highlights how Canada's Capital Region has evolved into a global innovation hub, from drones and self-driving cars to cloud software and cyber defense.

True success will require an even deeper alignment: governments, private sector leaders, and educational institutions must work hand in hand, removing barriers and working toward common goals. It's not just about co-hosting events or aligning on investments — it's about forging an integrated, future-ready region where innovation thrives across the river, across sectors, and across traditional divides.

To realize the full potential of this region, we must go beyond collaboration, we must fundamentally shift our mindset. Ottawa and Gatineau cannot continue to be viewed as separate cities. They are, together, a single, powerful ecosystem with the capacity to lead globally in technology and cybersecurity. By embracing Ottawa-Gatineau as one interconnected, interdependent community, and by fully mobilizing public, private, and academic collaboration, the region will not just compete on the world stage — it will lead it. But perhaps the most important ingredient is the shared spirit that must continue to grow: a commitment to lead together, not apart. The opportunity is here — if we choose to fully seize it.

François Guay is the visionary founder of Canada's largest cybersecurity network, the Canadian Cybersecurity Network (CCN), which unites over 44,000 members from diverse sectors, including individuals, businesses, universities, professional associations, diversity groups, and government agencies, representing nearly 1,000,000 people across the country. Under François's leadership, CCN has become a cornerstone in fostering collaboration, innovation, and security in Canada's rapidly evolving cybersecurity ecosystem.

Québec City: Fortified by Firewalls

by Julien Turcot

Preface: Where Old Walls Meet New Frontiers

Imagine a place where centuries-old stone walls watch over data centers, and the past and future coexist in every networked corner. Cobbled streets meet fiber optic cables, and the echo of canons has been replaced by the click of keyboards defending the cyber frontier.

This is Québec City.

With its unique blend of tradition and innovation, Québec City has quietly become one of the most dynamic cybersecurity hubs in North America. From world-renowned universities to scrappy startups, government leaders to underground hackers, the city is writing its own digital legend—one that's powered by collaboration, research, and relentless curiosity.

The Pulse of Cybersecurity in Québec

What's more, Québec City is not just a symbolic center of security, it's also physical. Tucked within the historic Place D'Youville sits Bell Canada's regional hub, one of the most strategic points in the nation's digital infrastructure. Here, critical network cables from across the country converge, making it one of the most neurally sensitive nodes in Canada's internet backbone. This concentration

of connectivity underlines the city's importance not just as a home for cybersecurity companies, but as a literal gateway to national digital resilience.

It begins with people. Québec City's cybersecurity ecosystem is rooted in its people—the thinkers, the builders, the defenders. With over 100 cybersecurity-focused businesses and a workforce of approximately 5,000 professionals, the region is more than a cluster of companies—it's a living, breathing network of talent and purpose. Each firm, from scrappy startups to established global players, contributes to a local culture where innovation is constant and cyber vigilance is second nature.

The city's reputation as a cybersecurity stronghold has not gone unnoticed. In recent years, there's been a marked increase in the number of students enrolling in cybersecurity programs, professionals relocating to the area, and businesses opening regional offices to tap into the city's unique blend of talent and proximity to government and academia. Networking groups, hackathons, and mentorship circles continue to blossom, further energizing the community.

There's been a marked increase in the number of students enrolling in cybersecurity programs, professionals relocating to the area, and businesses opening regional offices.

Québec's people are not just responding to threats—they are reimagining what cybersecurity can be.

Industry giants like CGI (GIB.A TSX/GIB NYSE) and Alithya (ALYA TSX/Nasdaq) call this city home. Standing alongside homegrown heroes like GoSecure (founded in 2002), they work with a new generation of entrepreneurs building startups in threat intelligence and managed detection and response (MDR).

And the bench runs deep. Québec's consulting ecosystem includes veterans like LGS (IBM), DMR (now Fujitsu), Cofomo, Levio, and TechnoConseil, each bringing expertise to public- and private-sector digital transformation. Newer names like Vumetric, Fortica, Egyde, and Victrix (acquired by France's Alan Allman Associates and merged with Société Conseil Lambda in 2023) round out a field that is as diverse as it is skilled.

CQSI 2015: A Defining Chapter in Québec's Cybersecurity History

The CQSI (Colloque québécois sur la sécurité de l'information) has long served as one of Québec's most important industry events. This conference is organized entirely by dedicated volunteers from the ASIQ (Association de la sécurité de l'information du Québec), an association that has been fostering knowledge sharing, professional networking, and the growth of the cybersecurity community since 1983.

While Hackfest has been a pillar of community engagement and technical brilliance, the 2015 edition of the CQSI conference, organized by Anne-Marie Faber (then with Egyde) and Julien Turcot (then with Check Point), marked a pivotal high point in Québec's cybersecurity journey. This was the year the community did something extraordinary. By harnessing the momentum of a creative and cultural phenomenon, Game of Thrones, they turned what had been a traditionally dry subject into something cinematic, immersive, and magnetic. Attendees weren't just coming to learn, they were stepping into a world.

That world connected everyone: the government with grassroots hackers, manufacturers with researchers, and Québec with the global cybersecurity stage. This flagship conference, hosted in the heart of Québec City, brought together a remarkable lineup of thought leaders and field experts who shaped national cybersecurity conversation. It became the tipping point—where cybersecurity in Québec stopped being niche and started becoming a movement.

Attendees were treated to keynote speeches from major figures such as Michel Juneau-Katsuya, a former intelligence officer and media commentator; Robert Massé, a veteran cybersecurity strategist; Jean-François Beuze, a respected voice in cyber diplomacy and crisis response; and Brian Shields, the whistleblower and lead investigator in the infamous Nortel breach.

Government leadership was also on full display with powerful contributions from Martin Coiteux, then Quebec's Minister of Public Security, and Richard Olszewski of the Conseil du trésor (Treasury Board for the Province), aligning public policy and digital defense.

From GoSecure-led panels to hands-on sessions on Advanced Persistent Threat (APT) response (led by Pascal Fortin), cyber-governance, and international threat landscapes,

CQSI 2015 was not just a conference, it was a summit of minds that left a lasting impression on all who attended. The quality of the conference reached levels comparable to RSAC, delivering the kind of experience typically reserved for audiences ten times the size. For a 900-attendee event, it was, at the time, out of this world. The bar was raised and Québec took notice. Today, it remains a gold standard in Québec's history of cybersecurity events.

An Ecosystem Forged in Collaboration

What makes Québec City truly stand out is not just the number of players but how they play together.

The city's educational fabric includes Cégep de Sainte-Foy, host of the popular HackerSpace initiative—an innovative community hub for students, alumni, and cyber-curious locals. HackerSpace is a launchpad for collaboration, experimentation, and passion-driven learning. With workshops, CTF practices, and mentorship sessions, it's cultivating a new wave of defenders eager to take their first steps into the world of ethical hacking.

Universities and colleges here are not ivory towers. They are launchpads. At Université Laval, cybersecurity is woven into the core of management, AI, and governance. Their Department of Management Information Systems offers a graduate microprogram in information security governance and a specialized diploma in information systems auditing—while researchers at Centre de recherche en technologies de l'information et affaires (CeRTIA) explore how AI can be ethically applied to cyber governance. Laval is also home to the Centre de sécurité internationale (CSI), where cyber policy intersects with global governance and digital rights.

Meanwhile, Cégep Limoilou is building the future with one technician at a time by offering programs in network administration and cybersecurity as well as programs that focus on real-world experiences. Other colleges like Cégep Garneau are beginning to introduce modules on ethical hacking, secure software development, and digital forensics—geared toward both new students and mid-career professionals looking to upskill.

The circuit continues to expand. Most recently, QuébecSec has joined the ranks—bringing fresh energy and talent into the fold. Positioned as an accessible, community-driven event, QuébecSec bridges the gap between seasoned professionals and newcomers through high-quality talks, technical deep-dives, and inclusive networking.

Together, these institutions have created a complete pipeline. Québec City's students can now go from first exposure to full employment in cybersecurity without ever leaving the region. Co-op placements, capstone projects with industry, and regional mentorship networks are all reinforcing the loop between learning and doing.

It's not just about education, it's about immersion, it's about building a generation that understands not only the technology but the culture of cybersecurity. And in Québec City, that culture is thriving.

ISACA Québec: Guiding Governance and Professional Growth

No less essential is the presence of ISACA Québec, the Québec City chapter of the global ISACA organization. With a mission rooted in promoting the advancement of IT governance, cybersecurity, and risk management, ISACA Québec serves as a pillar for ongoing education and professional certification.

Each year, the chapter organizes conferences, training sessions, and community meetups tailored for professionals pursuing certifications like CISA, CISM, CRISC, and CGEIT. Its events are not only a source of learning but also a space for networking and mentorship—helping practitioners stay ahead in a rapidly evolving field. The chapter plays a key role in fostering responsible leadership and innovation, making it an indispensable part of the city's cyber ecosystem.

Québec's Cybersecurity Voices: Podcasts That Resonate

In Québec City, the cyber conversation never stops—it simply changes format. Podcasts have become one of the most dynamic extensions of the region's cybersecurity culture, offering year-round platforms for analysis, commentary, and connection. They provide a space where researchers, practitioners, and leaders can share ideas long after the conference badges have been packed away.

Three flagship podcasts stand out as key contributors to the province's thought leadership:

1. PolySécure–Led by Nicolas-Loïc Fortin, this podcast is rooted in academic rigor and research, offering deep dives into digital policy, cyber ethics, and risk governance. With frequent contributions from professors and public policy leaders, it connects theory to frontline challenges. Collaborators include Ingrid Dumont, Isabelle Besançon, Christine Dugoin-Clément, and Cynthia Lopez-Gagousse, whose voices add richness and perspective to the conversation. Listen here: PolySécure

2. French Connexion–Raw, bold, and unapologetically operational, this podcast brings listeners into the trenches of modern security operations. Hosted by prominent figures like Patrick Mathieu (co-founder of Hackfest and Offensive Security Lead at Duo Security), Steve Waterhouse (retired Captain, cybersecurity instructor, and media commentator), and Damien Bancal (French journalist and founder of Zataz.com), the show balances deep expertise with engaging commentary. The team also includes Richer Dinelle, Guillaume Morissette, Gabrielle Joni Verreault, and Jacques Sauvé, each bringing their unique lens to the conversation. With a blend of humor, critique, and unfiltered perspectives, French Connexion breaks down the realities of modern cybersecurity—whether it's threat response, public policy, or ethical hacking. This podcast also serves as a platform for cross-continental dialogue between Québec and Europe, staying true to its tagline: "Sécurité sans frontières." Listen here: French Connexion–Sécurité.fm

3. GoCast–Produced by GoSecure and led by Julien Turcot, GoCast explores the front lines of threat intelligence, incident response, and managed detection, often featuring guest experts from across North America. With a strong narrative and a focus on current events, strategy, and innovation, it serves both as a window into GoSecure's operations and a broader industry platform for sharing cutting-edge insight. Listen here: GoCast on YouTube

These aren't just podcasts—they're a chorus of voices shaping the cultural backbone of Québec's cybersecurity movement. From early-career professionals to seasoned CISOs, listeners tune in for inspiration, strategy, and solidarity.

And with each episode, these digital broadcasts continue the work started by CQSI, Hackfest, and countless meetups: making cybersecurity human, collaborative, and compelling.

The Circuit That Connects It All

The Circuit Québécois des événements en cybersécurité (CQÉC) is more than just a banner—it is a community movement. Built to unite and uplift, the CQÉC defines itself as a « communauté liante québécoise de la cybersécurité favorisant la diversité, l'inclusion, le partage, et l'accessibilité. » It brings together diverse voices, ensures accessible learning opportunities, and fosters a spirit of collaboration that transcends competition.

Once upon a time, Québec's cybersecurity landscape was vibrant but fragmented—each event forging its own path, each organizer building in parallel. It was a world of brilliant voices, but not yet a unified chorus.

Then came Anne-Marie Faber, organizer of the GoSec Conference at the time, who had a vision to unite the province's top cybersecurity events under one banner. That idea became the CQÉC, a collaborative framework connecting events like BSides Montreal, GoSec, Hackfest, and now ITSEC.

The CQÉC wasn't just a logo or mailing list. It was, and remains, a cultural connector—a way for organizers to share

resources, align calendars, support each other's growth, and foster a year-round conversation that extends far beyond the podiums.

These events don't just coexist, they reinforce one another. They form a network where learning, innovation, and community-building thrive. Thanks to the groundwork laid by the CQÉC, Québec's cybersecurity gatherings now move with a shared sense of purpose: to elevate the province's digital defenses, and to ensure every practitioner finds not just a seat at the table, but a family at the fire.

The Spirit of Hackfest

Each fall, the heart of Québec's cyber community converges in a whirlwind of exploits, exchanges, and ideas. Founded in 2009 by Patrick Mathieu and a small team of passionate hackers, Hackfest has since evolved into Canada's largest hacking conference, welcoming over 1,500 attendees in 2023 alone. What began as a grassroots gathering has become a benchmark for technical excellence and underground credibility.

Speakers at Hackfest have included not just elite researchers and red teamers, but also policy-makers, educators, and public advocates. The diversity of voices—from developers unveiling new tools to intelligence veterans sharing war stories—creates an electric blend of content that ranges from deeply technical to philosophically provocative.

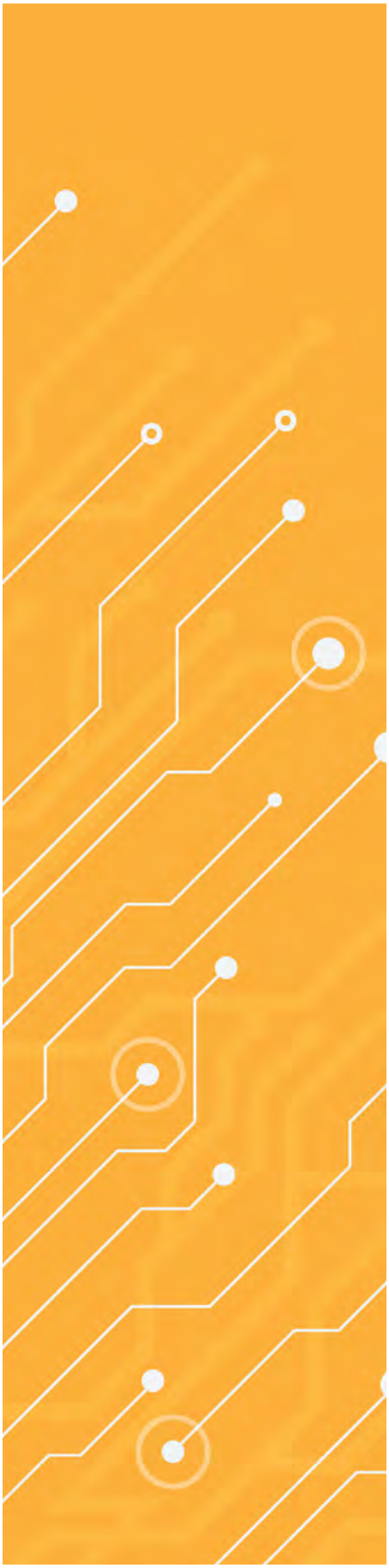
Québec City has proudly hosted a wide array of renowned cybersecurity speakers over the years with names that resonate across the global infosec community. From international experts like Jayson E. Street, Cheryl Biswas, and Gabriel Ryan, to local pioneers like Philippe Arteau, Kristina Balaam, and Damien Bancal, Hackfest has drawn some of the most respected voices in the field. Even Canada's political leaders have taken the stage; Éric Caire, Minister of Cybersecurity and Digital Technology of Quebec, has been a visible presence, underscoring the province's commitment to cyber policy and innovation.

Hackfest is more than a conference. It's a rite of passage. The co-founder, Patrick Mathieu, said this in a recent interview: "Hackfest continues to grow, providing an essential platform for sharing constantly evolving knowledge."

The event's programming reflects the full spectrum of cybersecurity, with tracks dedicated to reverse engineering, offensive security, privacy law, cyber policy, and hacker ethics. There are Capture-the-Flag competitions, underground villages, social engineering labs, and spontaneous hallway meetups where careers are launched and collaborations begin.

The conference has grown, so has its cultural footprint. Hackfest is now a brand synonymous with passion and purpose. It's where veterans reconnect, students make their debut, and the community, for one long weekend, becomes a family.

The next installment, slated to take place from October 13 to 18, 2025, is already on the radar for professionals from across North America and Europe. Because if you're in cybersecurity, Hackfest isn't just a date. It's a pilgrimage.



SEQCure: Focusing on Security in Research and Education

Amid Québec City's array of cybersecurity conferences, SEQCure stands out for its unique mission—bringing together security professionals and academic researchers to tackle the specific challenges of protecting information in research environments and public institutions.

Organized annually, SEQCure is a bilingual event that targets professionals from the education and research sectors, creating a space to explore threats, incident response techniques, identity and access management, data privacy, and cyber risk in an increasingly connected world. Hosted in part by leading institutions in Québec and supported by government and industry, SEQCure has become an essential forum for cross-sector collaboration.

It's a place where ambition and lifestyle collide, where cybersecurity professionals can shape their careers and build meaningful lives.

With workshops, technical deep-dives, and policy-oriented panels, SEQCure ensures that Québec's academic and research communities stay not only informed but empowered. The event provides a direct channel for translating best practices from the cybersecurity industry into the higher education and research landscape. In doing so, SEQCure continues to reinforce Québec's role as a province where cybersecurity is truly embedded in every layer of society—from startups to scholars.

Mapping the Pulse: Québec's Cybersecurity Events and Podcasts

FLAGSHIP EVENTS:

- **Polar Conference**—A cybersecurity symposium organized by Hackfest Communication, bringing together experts for a focused dialogue on key security topics in an intimate setting (Next edition: October 16, 2025).
- **Rendez-Vous Numérique**—A digital transformation and cybersecurity forum hosted in Québec City, focusing on innovation, government leadership, and public-private partnerships.
- **Hackfest**—Canada's largest hacking conference, held annually in Québec City.
- **QuébecSec**—An inclusive and technical event with strong community engagement.
- **SEQCure**—A research- and education-focused bilingual event addressing institutional cybersecurity.

PODCASTS AMPLIFYING THE CULTURE:

- **PolySécure**—Academic rigor meets digital governance Listen here
- **French Connexion**—Cross-continental hacker insights and commentary Listen here
- **GoCast**—Insights from the field, led by GoSecure's Julien Turcot Listen here

These events and podcasts create an ongoing rhythm that educates, challenges, and inspires the ecosystem year-round. Whether you're tuning in or showing up, there's always a way to plug into Québec's cyber community.

Why Québec City?

The question isn't just why *now*—it's why *here*.

Québec City is more than a beautiful backdrop for conferences and campus labs—it's a place where ambition and lifestyle collide, where cybersecurity professionals can shape their careers and build meaningful lives. A city that honors its heritage while engineering the digital frontier. With a cost of living that remains lower than many major Canadian cities, cybersecurity professionals here can enjoy the best of both worlds: a thriving career and a high quality of life. From affordable housing to accessible transit and vibrant cultural scenes, Québec City offers an appealing package for both families and individuals.

Another unique feature lies in the city's bilingual culture. As one of the few major North American cities where French is the dominant language while English is widely used in professional and academic settings, Québec City offers a rare environment for cross-cultural collaboration. This multilingual advantage gives cybersecurity professionals and companies the flexibility to operate globally while remaining deeply rooted in a rich, local identity.

For professionals seeking a destination that offers purpose, progression, and a sense of place, Québec City stands apart. It is where historic charm meets future-forward innovation. Where education, government, and industry unite to create pathways and not just pipelines for talent.

From labs at Université Laval's to the vibrant floors of Cégep Limoilou, from the bustle of Place D'Youville to the cafes hosting security meetups, the entire city feels wired for collaboration. And with over 100 cybersecurity businesses already calling it home, the local job market is both deep and diverse—spanning startups, multinationals, consultancies, and public-sector entities.

Québec offers something rare in the tech world: stability and inspiration. Salaries are competitive. The cost of living is manageable. Families find not just jobs but communities. Outdoor adventures are minutes from your door, and rich cultural experiences are baked into everyday life. It's a city that feeds both intellect and soul.

And it's only just beginning. Every year brings more students, more innovators, more conferences, and more chances to connect. The next cybersecurity leader could be walking the ramparts, coding in a basement, or attending a local CTF.

This is Québec City, where the future of cybersecurity isn't just studied or deployed—it's lived.

Powering the Future

Once fueled by curiosity and a grassroots spirit, Québec City's cybersecurity community is now a full-fledged ecosystem—with the numbers to prove it. Over the past decade, the city has seen exponential growth in the number of cybersecurity professionals, students, and entrepreneurs. They are all drawn to this region by foundational initiatives like CQSI, Hackfest, and the CQÉC.

Today, Québec trains thousands of students annually in programs tailored to digital defense, governance, and intelligence. Enrollment in cybersecurity-focused college and university programs has more than doubled since 2015, and participation in local events ranging from workshops to national conferences has surged. What was once a tight-knit group of early adopters has become a movement that inspires the next generation of defenders.

The government has not stood idle. The formation of the Ministère de la Cybersécurité et du Numérique (MCN) marked a turning point in the province's cyber journey, representing the first time a Canadian province has established a dedicated ministry for cybersecurity and digital transformation. Backed by significant funding through Investissement Québec, this initiative brings political weight and long-term vision to the community's ambitions. The MCN doesn't just support the industry—it actively shapes it through public-private partnerships, strategic hiring, and the deployment of secure digital services across the province. This isn't just about job creation—it's about embedding cybersecurity into the DNA of governance and public trust.

Organizations like Hackfest continue to nurture community through meetups, best-practice exchanges, and technical training, while Québec City's innovation offices channel capital and policy in ways that matter. Hackfest has evolved beyond a single event—its influence extends year-round through its community engagement, podcast production, and collaboration with public and private sectors. Together, they're turning bright ideas into businesses, students into specialists, and local ambition into international recognition.

From fortified ramparts to hardened firewalls, from centuries-old universities to bleeding-edge labs, Québec City is not just witnessing the cybersecurity revolution—it's leading it. Its past gave it wisdom. Its present gives it momentum. And its future? Well—that's yours to write.

Julien Turcot is a recognized Information Security executive leader with more than 20 years of experience in driving large scale technology security initiatives, cyber resiliency programs and risk management. He is currently the SVP of Sales at GoSecure. He has helped organizations, large and small and across the public and private sector, to understand risk posture and put in place strategies and the right architecture to manage it. He is widely recognized as an industry thought leader and experienced practitioner, capable of translating technology challenges into actionable business solutions and is a renowned public speaker at international cyber security conferences.

PHOTO: © DESTINATION TORONTO

Toronto: The 6ix of Cybersecurity, Canada's Cyber Capital

by Shazeen Ahmed

Toronto at the Forefront: Leading Canada's Cybersecurity Revolution

Spanning Lake Ontario's northwestern shore, the Greater Toronto Area (GTA), famously coined as the 6ix by a popular recording artist, consists of six local boroughs (Etobicoke, North York, Scarborough, York, East York and Toronto) and the bustling cities of Mississauga and Brampton. As the largest city in Canada, the population of the GTA exceeds 7.1 million, with significant growth in just the past two years (over half a million). This area has evolved into a global hotspot, with significant worldwide influence in entertainment, culture, business, and technology. Toronto is also recognized as one of the largest and fastest-growing tech hubs in North America, making it a natural focal point for the thriving cybersecurity industry. Specific sectors like finance, anchored by the Toronto Stock Exchange, and healthcare, with an increasing focus on medical record digitization, drive significant demands for advanced cybersecurity solutions in the Toronto area.

Toronto's thriving technology ecosystem, dense concentration of businesses, and proximity to world-class academic institutions like the University of Toronto, Toronto Metropolitan University, and York University form a powerful foundation for its dominance in cybersecurity. This, coupled with

Toronto's charming city character, marked by diversity, livability and a dynamic metropolitan energy, collectively places the GTA as one of the best places to live and work in cybersecurity in Canada. Over half of Toronto's residents were born outside Canada (Statistics Canada, 2022), which contributes to the region's diverse talent pool and brings together global perspectives to cybersecurity challenges.

The cybersecurity industry in the Toronto region is a remarkable cornerstone of Canada's tech sector. It is made up of key anchor companies like Apple, Amazon, Google and IBM with unique local innovators like Protexxa and SailPoint that reflect a diverse ecosystem. Key institutions, including MaRS Discovery District and the Rogers Cybersecure Catalyst (the Catalyst) at Toronto Metropolitan University foster this growth through dynamic talent development and startup support. MaRS has supported over 1,400 startups since its inception in 2010, including several in cybersecurity, while the Catalyst reported in 2023 to have impacted over 7,000 individuals from its groundbreaking programs.

As Canada's most populated region, the GTA naturally has a dense concentration of cybersecurity professionals creating a diverse network and talent pool. This is evident in recruitment trends, where more than half of employers cite employee referrals as the most effective hiring channel. The presence of cybersecurity focused groups such as Toronto Area Security Klatch (TASK), ISC2 Toronto, and frequent industry events further amplify these connections and offer professionals opportunities to network and build relationships. This compelling community structure not only distinguishes the Toronto region, but also gives it a competitive edge in attracting and retaining top cybersecurity talent.

All in all, Toronto's position as a global leader in cybersecurity is no accident. Its ecosystem is heavily driven by its proximity to world-class academic institutions and a dynamic mix of established companies and innovative startups. This blend creates the optimal condition for growth in cybersecurity, where diverse perspectives and expertise come together to tackle complex challenges. The region's commitment to fostering innovation, dense concentration of tech talent and supportive community networks, further amplifies its appeal. Initiatives from key players like the Rogers Cybersecure Catalyst demonstrate Toronto's ability to nurture talent and drive industry advancements. As Canada's largest and most diverse city, Toronto attracts top professionals and fosters an inclusive environment that empowers everyone, including underrepresented groups. These strengths put the GTA at the forefront of cybersecurity and set the stage for continued leadership.

A Cybersecurity Magnet: Toronto's Attraction

In the midst of a hub where leading tech giants and startups collide, the GTA turns its vibrant ecosystem into a magnet for cybersecurity talent and businesses. In fact, Toronto is home to more tech workers than U.S. metropolitan cities like Los Angeles, Seattle, and Washington, D.C., trailing only to New York and Silicon Valley. Toronto's charm can be attributed to its economic strength, academic institutions, and innovative programs. As Canada's tech epicenter, the GTA combines government incentives, educational partnerships, and cutting-edge initiatives to attract individuals and businesses. This not only ensures a steady flow of

talent but also interest and investment in this critical field.

One of the GTA's standout strategies is its support for technology, and by extension, cybersecurity, businesses through incubators. The MaRS Discovery District, a true cornerstone of Toronto's innovation scene, has nurtured more than 1,400 startups since 2010, including cybersecurity ventures, one of which is Private AI, a local innovative company which leverages artificial intelligence for data protection and privacy solutions. The DMZ at Toronto Metropolitan University has supported many startups as well, including MedStack, which leveraged the incubator's resources and support to develop a transformative SaaS platform for cloud-based compliance and security solutions in healthcare. Together, these organizations exemplify the GTA's strategic approach to cultivating a balanced and growing cybersecurity ecosystem. It is one that supports local entrepreneurs and businesses while positioning the area as a global magnet for top talent by attracting innovators wanting to shape the future of cybersecurity.

The MaRS Discovery District has nurtured more than **1,400** startups since 2010.

The GTA is home to world-class educational institutions offering a comprehensive range of traditional undergraduate and graduate degree programs, diplomas, and certificates in cybersecurity. However, what sets Toronto apart is its unique and innovative cyber education initiatives that go beyond traditional academia. At the forefront of this momentum, is the Catalyst, which is Toronto Metropolitan University's national centre for training, innovation, and collaboration. Based in Brampton, this institution is curating its innovative programs to meet industry demands. The Catalyst pioneers many first-of-their-kind offerings which cater to individuals, organizations, and entrepreneurs. These programs are truly setting a precedent for cyber education at a global scale and creating new standards. Notably, CyberStart Canada is a youth-focused initiative which empowers the next generation of professionals to explore cybersecurity in a safe and engaging environment, igniting early interest in the field. The Catalyst Fellowship Program is another standout initiative, which fosters a collaborative space for original research and industry engagement to tackle present-day cybersecurity challenges. Furthermore, the Catalyst Cyber Clinic is a free program for organizations aiming to provide foundational cyber support to nonprofits and social impact organizations. Delivered by students and alumni from the Catalyst's cyber programs, the Cyber Clinic provides emerging professionals with hands-on experience as Clinic Consultants. By doing so, the program not only helps vulnerable organizations bolster their cybersecurity and improve their overall resilience but also fosters the development of a skilled regional cybersecurity workforce.

Toronto's diverse educational landscape is a significant factor in its success as a cybersecurity hub. It is home to six publicly-funded universities and four private universities, offering a wide range of academic programs in cybersecurity and related fields. Additionally, Toronto has five publicly-funded community colleges and over 200 registered private career colleges, providing a plethora of options for students seeking training and certification in cybersecurity. Moreover, the Canadian Centre for Cyber Security's database for post-secondary cyber security related programs lists nearly 50 entities in Ontario.

Through these visionary initiatives and traditional educational institutions, Toronto is not only nurturing cybersecurity talent, it is also addressing the diverse needs of its community. By empowering underrepresented groups and supporting vulnerable organizations, Toronto is demonstrating its commitment to creating a secure and inclusive digital sphere. In turn, this makes Toronto an attractive destination for aspiring and entry level cybersecurity professionals.

Keeping it Local: Securing Toronto's Cyber Talent

The Greater Toronto Area is undeniably a significant hub for cybersecurity professionals in Canada. But the question is, how do we *keep* our talent here? Retaining top talent is crucial for this region to maintain its leadership in the industry. Factors such as quality of life, competitive salaries, career advancement opportunities, and local support

networks all contribute to why professionals choose to remain in the area. Retaining this expertise is truly the key to sustaining Toronto as Canada's cyber capital.

Toronto has consistently been recognized in the Economist Intelligence Unit's Global Liveability Index, ranking as the 9th most livable city globally in 2023. However, in 2024, the city dropped down to 12th place, primarily due to the apparent "acute housing crisis" that affected its infrastructure score.

Estimating cybersecurity salaries in the GTA is complex due to the field's nebulous subfields and differing roles like analysts, architects, and engineers. Even with the scarcity of region-specific workforce data, the available figures reinforce Toronto's appeal. According to Robert Half's 2025 Canada Salary Guide, cybersecurity analysts earn between $86,000 and $133,000 annually, while related positions such as security architects and data security analysts range from $83,000 to $165,000. These competitive wages show the region as a hub for mid and senior level professionals, with clear potential for advancement and higher salaries. Furthermore, evidence from the public sector reinforces this trend. Ontario's 2024 Public Sector Salary Disclosure, includes 1,316 entries for "cyber security" and 72 for "cybersecurity" across all sectors who earn $100,000 or more. Though not exclusive to the GTA, these results highlight robust compensation even in government roles. These salary figures and opportunities for growth provide a compelling reason for talent to remain.

Salary for Cybersecurity Analyst in Toronto, ON

75TH PERCENTILE
$132,983

50TH PERCENTILE
$109,776

25TH PERCENTILE
$86,048

Source: Robert Half

Another strong anchor for industry professionals in Toronto is the sense of community. The ISACA Toronto Chapter, with 3,700 plus members, is the largest chapter in Canada and the 5th largest in the world. Similarly, the ISC2 Toronto Chapter has recently achieved a notable milestone, reaching 1,000 registered members after a remarkable 500% growth in just two years since formalizing its membership process. This rapid expansion is a testament to the thriving cybersecurity ecosystem in Toronto, where professionals are eager to connect, learn, and grow together. Beyond these flagship organizations, Toronto boasts a diverse array of groups catering to various interests and demographics within the cybersecurity field. For instance, OWASP Toronto focuses on application security through regular meetups and workshops, while DefCon Toronto offers a space for enthusiasts and hackers to collaborate and share knowledge. Groups like Women in CyberSecurity (WiCyS) Toronto Affiliate and Leading Cyber Ladies Toronto champion women in the field, offering mentorship, networking, and career growth opportunities. These are just a snapshot of the many organizations that make Toronto a hub for cybersecurity talent retention.

SIDEWALK SHUTDOWN: TORONTO'S SECURITY CLASH

The cancellation of the Sidewalk Toronto project in May 2020 offers a revealing glimpse into the values and priorities of the local community. Proposed by Sidewalk Labs, a subsidiary of Google, the ambitious plan aimed to transform Toronto's Quayside into a cutting-edge smart neighbourhood. However, concerns over data privacy and surveillance sparked significant criticism. Dr. Ann Cavoukian, Ontario's former Information and Privacy Commissioner, was initially brought on as a privacy advisor to ensure robust privacy protections. However, she resigned a year into the project, sharing concerns that Sidewalk Labs failed to guarantee adequate data security and prevent potential surveillance. Her departure amplified public and expert criticism over privacy risks, contributing to the project's growing scrutiny.

While these organizations and programs play a crucial role in fostering professional growth and collaboration, their impact extends far beyond surface level networking. These groups play a pivotal role in making Toronto a place where cybersecurity professionals call home. Industry connections like these are truly an anchor for the Toronto cybersecurity industry. These organizations not only provide career opportunities but also foster a sense of belonging among members. For many professionals, these organizations serve as a platform to engage with peers, share knowledge, and stay informed about emerging trends, all of which are critical for personal and professional development. This sense of community is particularly vital in retaining top talent, as it creates an environment where professionals feel valued, supported, and motivated to remain in the region long-term.

Toronto has something to offer everyone, making it a magnet for cybersecurity professionals seeking both career growth and a high quality of life. Its relatively low crime rates, especially when compared to other major urban centers, contribute to a secure environment. The extensive public transportation network ensures connectivity within the GTA, making it easy for residents to navigate and access key areas. Toronto's thriving economy, competitive salaries, and robust professional networks create a compelling ecosystem for retaining top talent. The region can comfortably sustain its dominance in the cybersecurity industry by continuing to invest in these core strengths while creating an environment where professionals feel motivated to build their careers here long-term.

Connecting the Dots: Toronto's Cybersecurity Community

With a wide range of different organizations and professional networking groups that support working individuals or those interested in the field, the GTA has a thriving cybersecurity community. These groups provide numerous opportunities for individuals to engage with the cybersecurity ecosystem through offerings like conferences, meetups, training programs, mentorship opportunities, and much more. Standouts like the Toronto Area Security Klatch (TASK), BSides Toronto, ISACA Toronto, and the ISC2 Toronto Chapter fuel the cybersecurity community and engagement within.

However, like many regions, the GTA's cybersecurity community faces challenges related to gender representation in the workforce. Women only make up between 20% to 25% of the global cybersecurity workforce, with underrepresentation more pronounced in leadership roles. This lack of diversity not only limits the talent pool but also stifles innovation, diverse perspectives are critical for solving new and complex cybersecurity challenges. The GTA wonderfully fosters this need by offering several specialized groups aimed at supporting and empowering women in the field. Organizations such as Leading Cyber Ladies Toronto, WiCyS Toronto Affiliate, and Women in Security and Privacy (WISP) Toronto Chapter are making significant strides in creating inclusive spaces for women to network, learn, and advance professionally. These groups often provide tailored events that are specifically designed to address the unique challenges women face in the cybersecurity industry. Nour Moussa, a local industry professional and PhD student at the Toronto Metropolitan University's Ted Rogers School of Management, emphasizes the importance of visibility and celebration in fostering inclusivity, She envisions a future where visible minority women thrive,

> "You will find celebration of others to be a common theme in cyber within our GTA community. It's important that we continue to showcase and celebrate each other's challenges, wins and journeys. I want others, particularly visible minority women, to see themselves in this field, to see all the different options they have and how they too can be successful…that they can make their mark, and be respected for what they bring to the table."

Programs such as the Catalyst's Emerging Leaders Cyber Initiative (ELCI), based in downtown Toronto, also aims to foster inclusion and develop leadership skills in the cybersecurity sector.

The ELCI demonstrates a strong blend of industry and academic expertise, exemplified by the support of Mastercard Canada. This collaboration not only strengthens the program's curriculum but also reinforces its commitment to building a diverse community of cybersecurity leaders. Professionals from across the country gather in Toronto to participate in this cutting-edge program, highlighting the GTA's role as a national hub for talent development and innovation. As Tracy Haire, an industry leader from Cohort 3 of ELCI, reflected,

> "This program made many of us aware of our capabilities and really helped us come out of our shells. As we began sharing our stories and experiences, it brought us closer together as a community."

Beyond sharpening skills and bonds, such initiatives demonstrate their lasting impact on the local landscape by fortifying industry connections.

This spirit of connection extends to Toronto's vivacious events, where the community gathers to share knowledge and grow. The regional cybersecurity ecosystem thrives on flagship events and conferences that play a pivotal role in strengthening the community's sense of connection. These events not only draw national attention but also invite global experts to the area, facilitating knowledge sharing and enabling meaningful exchanges within Toronto's cyber community. One such example is SecTor, Canada's premier IT security conference. Born from the vision of TASK founders who were frustrated by the lack of a central Canadian equivalent to U.S. events, SecTor brings together experts worldwide to share research and industry trends. SiberX is another GTA-based company that hosts various events and training programs to connect public and private sectors, cybersecurity experts, and organizations making global impacts. Initiatives include Operation Defend the North, a cybersecurity readiness table top exercise simulating cyber attacks on critical sectors aimed to strengthen Canada's cyber security readiness and resilience. These gatherings don't just educate, they bind the Toronto cyber ecosystem.

In line with the community's emphasis on growth and development, CyberPaths GTA serves as an excellent resource for the local cybersecurity community. Launched in 2024, this GTA-focused pilot project from the Canadian Cybersecurity Network provides a roadmap for cybersecurity professionals at various stages of their cybersecurity journey, including new immigrants and those who recently relocated to Toronto. The program provides tailored access to a comprehensive suite of resources, connecting participants with city and community services, including support for immigration, business services, education, certification, networking, and mentorship opportunities. CyberPaths addresses the unique needs of Toronto's diverse community by providing resources that help individuals navigate their professional lives in the city. It not only supports skill development and career advancement but also plays a vital role in strengthening the GTA's cybersecurity ecosystem as a whole.

From networks and inclusivity programs to events and resources, Toronto's cybersecurity community forms an interconnected hub. By

empowering professionals across all career stages and fostering a culture of collaboration, the GTA has the ultimate foundation to drive the community forward. As the city continues to grow and prepare for future challenges, its dedication to fostering resilience and embracing diversity reinforces its status as a leader in cybersecurity.

Detour Ahead: Navigating Challenges in Toronto's Cybersecurity Industry

While Toronto is emerging as a leading cybersecurity hub, it faces several challenges that require innovative solutions to ensure sustained growth. One significant issue is the persistent divide between experience and education, which hinders progress in the field across the globe. "There is a gap in what's being taught in school and what's being practiced in the industry," explains cybersecurity thought leader Evgeniy Kharam. Many senior cybersecurity roles are often filled by professionals transitioning from traditional tech fields like network engineering, leaving behind recent graduates who lack hands-on experience. This emphasis on practical expertise over formal education creates a bottleneck in the talent pool, exacerbating the gap between supply and demand for skilled professionals. Kharam encourages those entering the field to look beyond just technical knowledge and tap into human-centric skills that are increasingly vital to modern cybersecurity roles. Soft skills such as communication, adaptability, and emotional intelligence are often overlooked in traditional training but are essential in real-world settings. For example, these skills enable clear communication of risks and solutions in stakeholder education; calm and effective management of crises in incident response; and compliance in enforcing governance.

However, true success demands a fresh approach to hiring, one that regards new ideas and perspectives. Employers must consider alternative pathways to integrate early-career talent and recognize the value of certifications and degrees, especially those from innovative programs that emphasize hands-on learning. Such an approach should no longer be the exception but rather the standard. Furthermore, employers should take an active role in fostering hands-on experience by providing internship programs, mentorship opportunities, and on-the-job training initiatives. This will support the potential of a broader range of candidates and the overall cybersecurity ecosystem.

Beyond the experience and education gap, the rapid advancement of AI and automation presents another critical challenge. While these technologies enhance efficiency and enable advanced threat detection, they also contribute to workforce disruptions. In cybersecurity, for example, AI-driven tools are increasingly automating routine tasks such as log analysis, threat detection, vulnerability scanning and preliminary incident triage, reducing traditionally junior functions. According to Gartner's projections, generative AI will reduce the need for specialized education for 50% of entry-level cybersecurity roles by 2028. This shift poses significant challenges for early-career professionals who rely on these roles as stepping stones to gain experience and advance their careers. This also worsens the broader talent shortage in cybersecurity, leaving organizations struggling to find more senior level candidates. As automation continues to reshape the industry, stakeholders who invest in continuous learning programs that focus on AI-augmented cybersecurity skills, and develop collaborative frameworks between educational institutions and industry will ensure curriculum relevance in the workforce.

True success demands a fresh approach to hiring, one that regards new ideas and perspectives.

Toronto's rich diversity includes a large number of skilled immigrants who could significantly strengthen the cybersecurity sector, yet many encounter obstacles that prevent them from fully integrating into this field. Challenges such as unrecognized foreign credentials, limited access to local professional networks, and unfamiliarity with Canadian workplace norms often prevent them from entering into the cybersecurity workforce. This untapped talent pool represents not just a missed opportunity but a drag on the development of Toronto's cybersecurity ecosystem. To overcome these hurdles, targeted upskilling and certification programs for immigrants are critical. These efforts should focus on aligning their existing skills with the needs of local employers and offering practical support for navigating the Canadian job market. One promising example is the Toronto Region Immigrant Employment Council (TRIEC) which focuses on connecting employers to programs to recruit and retain immigrants and fostering connections that

ease workplace integration. Expanding such efforts with a cybersecurity focus could strengthen the local industry.

Intensifying cyber threats, coupled with growing economic pressures, are significantly complicating the cybersecurity landscape. The rapid expansion of emerging technologies is matched only by growing vulnerabilities, which further destabilize the ecosystem. Growing threats of cyberattacks on critical infrastructure is a rising concern, gaining prominence in the cybersecurity landscape.

Toronto critical systems have also been affected by these threats as evidenced by the 2021 ransomware attack on the Toronto Transit Commission (TTC) which disrupted communication systems and services. Similarly, SickKids Hospital faced a ransomware incident in 2022 that impacted its operations. However, the City of Hamilton's 2024 cyber incident truly serves as a cautionary example of the devastating consequences of a cyberattack on a municipal government. It highlights the financial and operational strain caused by cyber threats, with costs over $7 million. The City of Hamilton's response has been substantial, allocating over $52 million for capital restorative projects related to the cyber incident. The City of Toronto's proactive approach to cybersecurity, led by the Office of the Chief Information Security Officer (CISO) demonstrates the importance of proactive municipal action in protecting critical infrastructure. With $35.1 million dedicated to municipal cybersecurity in 2025, it is reinforcing the City's vision to position Toronto as a "Global Leader in Urban Cyber Innovation" as stated by the Office of the CISO.

Beyond the complexities within the cybersecurity industry itself, external factors also pose significant barriers to attracting and retaining talent. One such factor is Toronto's notoriously challenging transportation system. Home to some of the busiest highways in the world, the city's traffic situation is far from ideal and results in lengthy commutes. In fact, Toronto has the highest commuting time in Canada, as reported by Statistics Canada in 2024. Commutes over an hour long have become increasingly common, and the proportion of commuters affected has increased for the third straight year, as of May 2024. Several factors can be attributed to this growing problem. Persistent traffic congestion, reduced public transit service, ongoing construction projects, and frequent transit closures have all played a role in prolonging commute times. For those traveling from outside the city, distance remains a significant hurdle and barrier for wanting to work in the GTA. As one industry professional, who wished to remain anonymous, noted, "the real challenge is distance for people outside of Toronto who are commuting back and forth." To tackle this persistent traffic issue, the city has been taking action. For example, significant investments are being made to expand and upgrade public transit infrastructure. Projects like the Ontario Line and the Eglinton Crosstown LRT lead the way and aim to provide faster, more reliable transportation options. Additionally, the City of Toronto's Congestion Management Plan is further addressing traffic congestion through a combination of advanced technologies, such as smart traffic signals and intelligent intersections, alongside proven traffic management strategies. Through these efforts, Toronto is paving the way for a more connected and commuter-friendly future, making it an even more attractive destination for industry talent and residents.

Shaping Tomorrow: GTA's Path Forward

Toronto is at the forefront of emerging trends and the rapid evolution of technologies like AI, quantum computing, and cloud security. A study commissioned by the National Research Council of Canada projects that by 2045, quantum applications, including cybersecurity, will fuel a $138 billion market, creating over 200,000 jobs nationwide. Yet, hostile actors increasingly exploit AI for election interference and cyber espionage, demanding not just technical expertise but a broader grasp of social and geopolitical awareness. 2022 Future Skills Centre report notes that 61% of employers expect cybersecurity skills to shift within three to five years, emphasizing the urgency of adaptable training programs. This evolving landscape highlights the importance of preparing professionals to operate in an environment where AI is both a tool and a threat. The World Economic Forum's Global Cybersecurity Outlook 2025, reinforces this, suggesting that developing skills to both operate and defend against AI is crucial for the next-generation cybersecurity workforce. Locally, Toronto is responding with timely educational offerings such as Humber Polytechnic's new Cybersecurity and Artificial Intelligence graduate certificate program, which aims to equip graduates with these highly sought after skills. Following these footsteps, institutions should continue to ensure that educational curricula are regularly updated to mirror the demands of the current cyber landscape.

The GTA's cybersecurity future is not only shaped by its current strengths but also by its ability to adapt to the evolving geopolitical landscape. Recent initiatives like the "Buy Canadian Cyber," launched on March 25, 2025 by the Catalyst and In-Sec-M showcase this adaptability. Developed in response to U.S. tariffs threatening Canada's economic stability, this centralized platform connects organizations with homegrown cybersecurity solutions

and aims to boost domestic resilience and global visibility. Lester Chng, Senior Cybersecurity Advisor at the Catalyst, explains "we now have a one-stop shop to find all the Canadian cyber companies." Within days, over 50 GTA-based firms self-listed on BuyCanadianCyber.ca, signaling strong local engagement. Chng also emphasizes the initiative's broader significance for the Canadian cybersecurity industry, especially in such uncertain times "it's one of the strongest supports for the community." This focus on community-building demonstrates the value of empowering Canadian innovation by supporting local businesses, not only in Toronto but across the nation. These efforts are essential for protecting Canada's digital future and turning challenges into global opportunities.

Building a resilient cyber workforce also requires supporting inclusivity and multiple entry points.

It's no question that the GTA's cybersecurity future is bright. Toronto is building a strong foundation for its digital economy by introducing youth to cybersecurity early on and sparking interest. Programs that engage students not only address the growing demand for skilled professionals but also ensure that young voices are included in shaping the industry's future. Initiatives like ElleHacks, a hackathon designed to bridge the gap in tech and innovation, provide a platform for women and gender-diverse students, to share ideas and learn from one another. As founder and cyber leader, Farzia Khan explains, "ElleHacks was born from the idea that innovation thrives when everyone has a seat at the table." Beyond ElleHacks, Farzia's newer initiative, NextGen Digital Defender helps youth champion cybersecurity through storytelling, interactive workshops, and accessible resources. This focus on inclusivity and innovation ensures the GTA remains a hub for diverse and skilled cyber professionals in the years to come. Similarly, HackStudent, a Toronto youth focused initiative aims to teach Canadian youth cybersecurity through workshops, and speaking engagements with students at conferences and schools. By demystifying cybersecurity and making it accessible to young learners, these programs inspire curiosity, and curate pathways for future careers.

Building a resilient cyber workforce also requires supporting inclusivity and multiple entry points. A recent poll shed light on the strategies that newcomers and entry-level professionals perceive as most effective for breaking into the field. When asked how aspiring professionals can boost their chances, 54% of respondents emphasized the importance of joining cyber groups or communities, highlighting the role of networking and collaboration in career advancement. Meanwhile, 26% recommended building home labs to experiment, and 20% suggested obtaining certifications.

Looking ahead, the GTA's ability to adapt to emerging trends and invest in its talent pipeline will be critical to maintaining its leadership in the global cybersecurity landscape. By fostering an innovative and collaborative ecosystem, the region is well-positioned to address future challenges and capitalize on new opportunities. The region's commitment to empowering the next generation of cybersecurity leaders ensures a brighter and more secure digital future for all. However, the path forward requires ongoing effort. As Toronto continues to address its challenges (i.e. transportation barriers and workforce disruptions caused by automation), it must remain persistent in creating new and fresh pathways that allow all of its workforce to thrive. In this dynamic city, progress demands momentum, not complacency. It's about embracing change and advancing the Canadian cybersecurity landscape. By solidifying its reputation as a hub for innovation, community and resilience, Toronto is setting a precedent for global cybersecurity leadership.

See end notes for this article's references.

Shazeen Ahmed is a dynamic and experienced privacy professional with a diverse background spanning public and private sectors. Her unique perspective at the intersection of privacy and cybersecurity stems from extensive expertise in privacy programs, data protection, risk management, and compliance. Passionate about cross-functional collaboration, she excels at working with diverse teams to support strategic organizational goals. Her contributions have been recognized through multiple awards, highlighting her commitment to driving organizational success and innovation.

Vancouver: Come for the Beauty, Stay for the Community

by Michael Argast

The emerald city on Canada's west coast is a glittering hub of enduring cybersecurity strength. With thousands of local cybersecurity experts, a mature student pipeline, industry titans investing in core technologies, innovative startups, and a thriving community scene, the Vancouver Lower Mainland is quickly becoming a global leader in the cybersecurity industry.

Education: The Future Talent Pipeline

The pipeline of cybersecurity talent in British Columbia starts early with a joint venture between the provincial Government, IBM, and Palo Alto offering a program for high school students to learn technical skills. A variety of capture the flag events from CyberTitan, ISACA, and CyberSCI also host both high school and college students to direct their creativity into developing strong cybersecurity skills.

> "Our Cybersecurity GRC post-degree diploma is an excellent example of what happens when we begin our program design and development with industry needs at the centre of our focus and processes. The result of course is a scope of training that is customized and truly reflective of the emerging needs and trends from those who would hire our graduates to help perform this essential work across our community."
>
> *—VCC Dean of continuing studies, Adrian Lipsett*

This continues into the post-secondary education system, ranging from micro-credentials to undergraduate and graduate programs. Some programs, like those offered by British Columbia Institute of Technology (BCIT) and New York Institute of Technology-Vancouver (NYIT) have been

running for over a decade. To keep pace with the growing demand, many other institutions are releasing new programs to keep up with growing demand. All this translates to hundreds of students being brought annually into the workforce

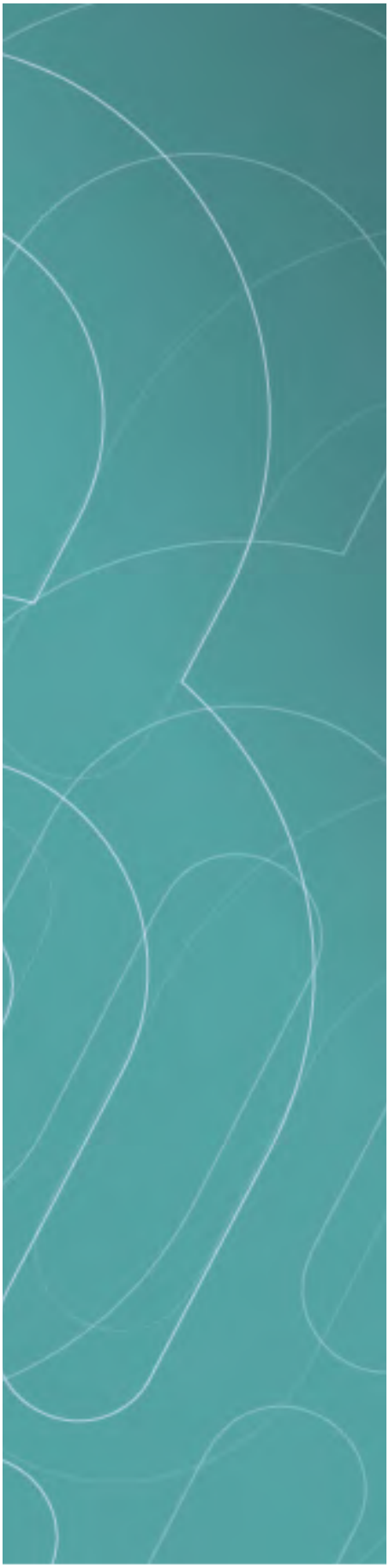
> "Our graduates are already making a significant impact working in key sectors across British Columbia that are critical to a healthy economy, including leading organizations such as Fortinet, Seaspan, Telus, BCAA and prominent universities."
>
> —*Irene Young, Campus Dean, NYIT Vancouver*

Institution	Program	Credential
University of British Columbia (UBC)	Cybersecurity Strategy and Risk Management Microcertificate	Microcertificate
Simon Fraser University (SFU)	Master of Cybersecurity	Master's Degree
New York Institute of Technology (NYIT) Vancouver	Master of Science in Cybersecurity	Master's Degree
Vancouver Community College (VCC)	Cybersecurity Governance, Risk, and Compliance Post-Degree Diploma	Post-Degree Diploma
British Columbia Institute of Technology (BCIT)	Digital Forensics and Cybersecurity	Various Credentials

Vancouver Cybersecurity is a Team Sport: Building Stronger Communities

Cyber sprouts or silver locks, cybersecurity professionals all need to continue to network to find opportunities, learn new trends and security strategies from peers, and share best practices and tips. If you are interested in cybersecurity, there is a community for you in Vancouver.

> "Vancouver is the perfect blend of tech innovation and breathtaking natural beauty, making it an ideal spot for cybersecurity professionals to come together, collaborate, and be inspired. Here, you'll find an engaged cyber community, strong industry support, and countless opportunities to connect, learn, and explore everything this incredible city has to offer."
>
> —*Mary Carmichael, ISACA Vancouver President*



Event Name	Frequency/ Timeframe	Number of Participants	Focus Areas
ISACA Vancouver	Monthly luncheons and evening events	Approximately 100	Presentations and networking for IT governance, risk management, and security.
BSides Vancouver	Annually in March or April	Around 600	Community-driven presentations, networking, and vendor fair.
CanSecWest	Annually in Spring (March)	1,000-1,500 per year	Presentations and Pwn2Own hacking contest focusing on applied digital security.
OWASP Vancouver	Approximately every other month	50-100	Presentations and networking focused on application security.

In addition to the above, here are some events that add to the active community of like minded individuals, including, siberX, WiCys, DefCon604, VanCitySec, various capture the flag competitions, and more.

> "...BSides Vancouver… success came down to a few things: the economy, the geography, and most of all, the people. Vancouver's vibrant tech scene and outdoor lifestyle attract bright minds—many of whom live near downtown. That density helped our community thrive, not just during the main conference, but through our monthly satellite pub nights too. Unlike other cities where downtown empties out after 5 PM, Vancouver's energy sticks around—and I believe that was a major catalyst."
>
> *—Alex Dow, BSides organizer and founder of Mirai Security*

Vancouver is also an event destination of choice, people travel from across British Columbia, Canada, and around the world to attend the events and conferences because of the community, incredible environment, and opportunities to learn from global experts. Cybersecurity events are so regular and open, a visitor or newcomer to town can almost always find an event on any given week to network and learn, making Vancouver a welcoming city for all. Luncheons, outdoor events, hackathons, ISACA's cybersecurity trivia events, full blown conferences, there's something for everyone.

Vancouver offers incredible opportunities for individuals from diverse backgrounds and welcomes people from around the globe. The city boasts a vibrant LGBTQIA2S+ community and various special interest groups, such as WiCys and SheLeadsTech, which actively support career development.

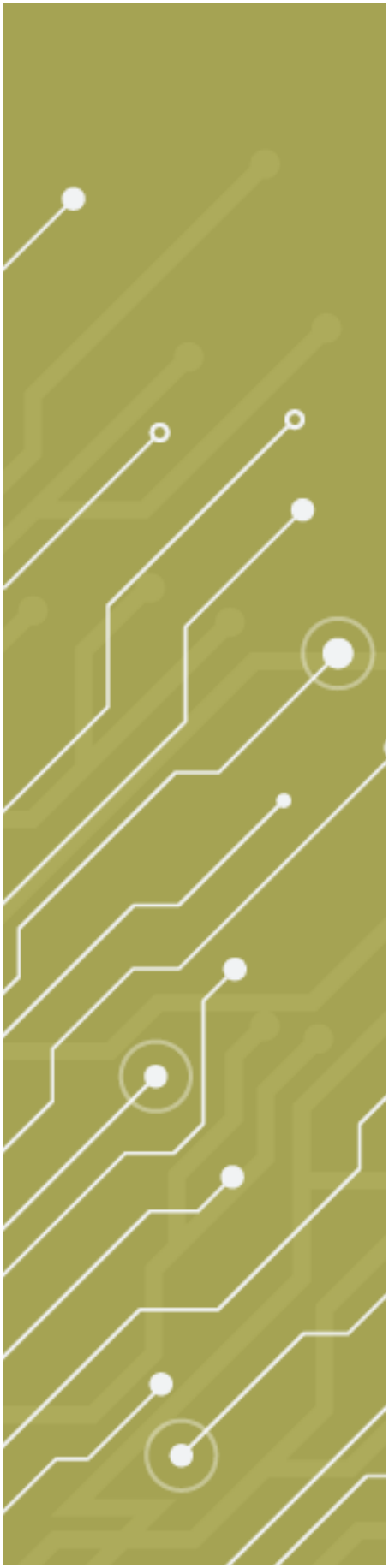
Startups and Security Stalwarts: Inventing the next generation of security products and services

Cybersecurity graduates and professionals don't just work to secure their companies. They are also busy developing new technology and services in Vancouver that make a difference worldwide. Similar to how Checkpoint established a flourishing cybersecurity startup ecosystem in Israel, prominent companies such as Sophos, Absolute, and Fortinet have significantly contributed to the development of a new generation of startups in Vancouver, encompassing both cybersecurity and other sectors.

> "Burnaby is home to our research and development arm. We have a long history of innovation and investment in British Columbia's Lower Mainland, opening our first threat intelligence and R&D centre in Burnaby, B.C. in 2000. Since then, we've massively expanded our operations, making Canada our global hub for FortiGuard Labs, Fortinet's threat intelligence and research centre."
>
> —*Gord Phillips, RVP for the Western Canada Region at Fortinet*

Company Name	BC Employees	Focus Areas (of Technology/Services)
Fortinet	1,900+	Network security, firewall solutions, threat detection, secure networking
Absolute Software	300	Endpoint security, data risk management, device management
Trulioo	250	Provides global identity verification and compliance solutions for businesses
Sophos	200+	Endpoint protection, firewall solutions, threat intelligence, cloud security
Diligent	150	Provides GRC software for governance, risk, compliance, and ESG management.
GeoComply	100+	Offers geolocation compliance and fraud prevention solutions for online businesses.
D3	100+	Provides SOAR solutions for automated incident response and cybersecurity operations.

Table continues on the next page.



Company Name	BC Employees	Focus Areas (of Technology/Services)
Ping Identity	~100	Identity and access management, authentication solutions, fraud prevention
Telus Security Solutions	100	Threat detection, data protection, risk management
StandardFusion	30	Offers an all-in-one GRC platform, unifying governance, risk, compliance, audit, and policy management into a centralized solution.
Kobalt.io	20	Cybersecurity, privacy and compliance programs for small and mid-sized companies
Mirai	15	Offers tailored cybersecurity consulting services, specializing in governance, risk management, compliance, cloud security, and application security.
idMelon	<10	Provides passwordless authentication solutions by transforming existing devices into FIDO2 security keys.
Iron Spear	<10	Penetration testing, security consulting, vulnerability assessments

Titans

Vancouver's dynamic cybersecurity community spans schools, startups, and established firms. Industry leaders have strategically built and expanded their teams in the Lower Mainland, tapping into local talent and attracting global expertise.

But the strong cybersecurity community in Vancouver doesn't just include schools, community and security startups and stalwarts. A number of industry titans have chosen to build or develop cybersecurity teams in the Lower Mainland to tap into this top talent pool and ability to bring global talent to this emerald city. Four such industry giants include:

1. AMAZON WEB SERVICES

Amazon employs thousands of its team members in Vancouver, transforming the historic Canada Post building on West Georgia Street, now known as The Post, into a stunning local headquarters. This iconic mid-century landmark occupies a full city block in downtown Vancouver and has been revitalized to house 1.1 million square feet of office space. Many of these talented individuals are dedicated to developing cutting-edge technologies that secure Amazon Web Services, making a global impact.

2. MICROSOFT

From their bustling headquarters on Granville Street and several satellite locations throughout Vancouver, Microsoft conducts vital research through their Windows Anti-Malware team. This team plays a crucial role in defending one of the world's most widely used business operating systems, ensuring robust security for users globally.

3. CISCO

Cisco, a global leader in networking, acquired OpenDNS in 2015 for $635 million to launch Cisco Umbrella. OpenDNS, known for its advanced DNS resolution services and robust phishing protection, has become the foundation of Cisco's cloud security strategy. This powerful platform uses advanced cloud security to protect users from online threats, offering comprehensive security solutions for businesses worldwide. In Vancouver, Cisco has utilized this acquisition to build a strong presence, with local teams contributing to the development and enhancement of Cisco Umbrella, ensuring top-tier security for their global client base.

4. MASTERCARD

Mastercard, a global leader in payments, has established the Global Intelligence and Cyber Centre of Excellence in Vancouver. This center focuses on advancing their capabilities in cyber and intelligence (C&I), AI, and IoT. Employing over 230 local experts, the center is driving innovation and enhancing security solutions for the digital economy. In addition to fostering local talent, the center has filed over 30 patents aimed at securing cyberspace, reducing malicious bots, and enhancing biometric security algorithms. The center also features an "Experience Centre" where local, national, and international tech communities collaborate on cybersecurity innovation. This initiative not only strengthens Vancouver's vibrant tech ecosystem but also positions Canada as a global powerhouse in cybersecurity.

Challenges

Although Vancouver has a lot to offer, it is not without challenges. The incredibly high cost of housing makes it difficult to purchase a home. Rental properties are also expensive and can be challenging to find. Additionally, the cost of living in Vancouver is amongst the highest in Canada. All of the above impact bootstrap capital and drive founders to take earlier exits. Despite the growing number of academic offerings and training programs, including the availability of co-op jobs and internships, early career opportunities remain limited. While there are standout programs at companies like Fortinet, the overall pipeline has yet to expand significantly. Many founders opt to relocate to American cities like San Francisco due to better access to capital, favourable tax policies, and a more developed startup scene, including a robust venture and investor community.

Come to Learn and Build, Stay to Thrive

Whether you are launching your career as a student, building your first security startup, or expanding the reach of your global enterprise, Vancouver is the ultimate destination for cybersecurity professionals. With a vibrant community, supportive environment, and a thriving business climate, Vancouver offers everything you need to excel and innovate in the field of cybersecurity.

Michael Argast is an experienced cybersecurity professional with over 20 years of industry experience. He is the co-founder and CEO of Kobalt.io, a rapidly growing cloud-focused security services provider.

Victoria: Where Nature Meets Innovation

by Harry Lofts

Victoria, a beautiful mix of nature and innovation, has quietly become a powerhouse of cybersecurity talent and development. This report highlights why Victoria punches above its weight in the cybersecurity marketplace, focusing on its unique blend of educational opportunities, a thriving tech sector, and a strong sense of community.

With a projected global cost of $10.5 trillion annually for cybercrimes, the demand for cybersecurity professionals is more critical than ever. Recognizing this need, institutions like the University of Victoria offer programs such as the Master of Engineering in Telecommunications and Information Security to equip graduates with the skills to protect digital infrastructures. The success of these programs is evident in the high post-graduation employment rate, averaging around 83%. This strong educational foundation, combined with the city's other attractive qualities, lays the groundwork for Victoria's evolving cybersecurity ecosystem.

Victoria boasts a growing hub of approximately 1,172 high-tech companies, with a substantial portion dedicated to cybersecurity services and products. This number is steadily increasing as security leaders relocate to the island

Employment Rates of Recent Graduates

In labour force
100%

Median annual salary
$84,300

83%
In a job related to their program

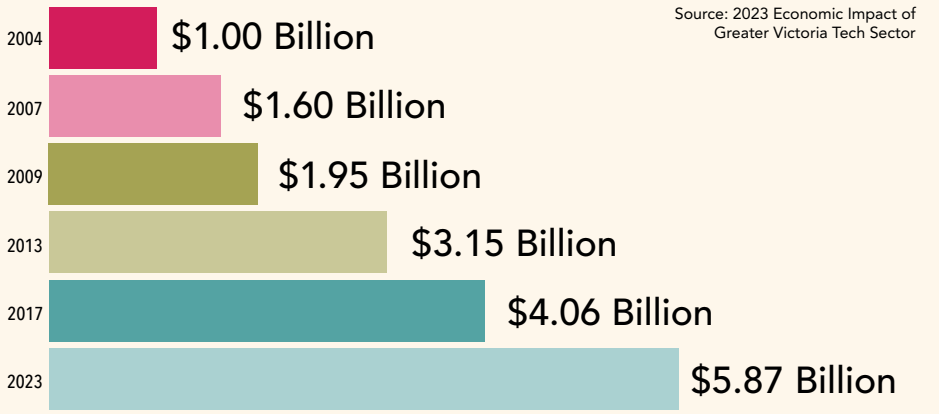
89%
Said the knowledge and skills gained were useful to their job

0%
Were self-employed

Results are based on: University of Victoria, Bachelor of Engineering in Computer Engineering; Source: BC Student Outcomes Data Viewer

and identify market gaps, both within Canada and from around the world. The past five years have seen a 20% increase in cybersecurity-related businesses, with job growth in the sector outpacing the national average by 15%. This upward trajectory aligns with the broader tech sector's growth, highlighted in VIATEC's 2023 Economic Impact Report, which noted a 52% surge since its last report.

Total Revenues of the Technology Sector in Greater Victoria



Victoria's appeal extends beyond its thriving tech sector and educational opportunities. The city's attractive lifestyle also plays a significant role in drawing cybersecurity professionals away from larger hubs like Ottawa and Toronto. The island's prime location boasts a mild climate year-round, catering to those with an adventurous spirit outside of work. Additionally, its proximity to major tech hubs like Vancouver and Seattle, coupled with the prevalence of remote work options in the cybersecurity sector, allows professionals to enjoy a fulfilling career in an idyllic setting. It is the best of both worlds.

> "Simply because it's home to hundreds of technology companies, not all of whom necessarily advertise that they're here, but there is a very vibrant tech scene and with that comes requirements for cyber security capabilities. The province of BC also punches well above its weight when it comes to digital identity and cyber security. So it's not surprising that there's some great cyber talent here in Victoria."
>
> —*Ian Paterson, CEO at Plurilock*

Local companies like BCI are providing incentives to attract and retain talent within Victoria through their Internship program. It builds a great cyber team by providing real and meaningful projects and a collaborative place to work. Being plugged into the local cyber scene, companies like BCI are constantly bringing in fresh talent by:

- **Teaming up** with groups like Gartner and ISACA.
- **Sharing knowledge** at conferences and events, such as Victoria International Privacy & Security Summit (VIPSS).
- **Getting the word out** on tech and cyber jobs through attending conferences and job fairs.
- **Holding hiring events** and meeting aspiring students.

While compiling my research one thing I noticed was the fact that Victoria has a very strong sense of community. It is a community where you can meet 10 people you know at every conference without fail. This sense of community is reinforced through locally run events like VIPSS, BSides Victoria and OWASP Victoria. BSides organizer Will Whittaker mentioned such events provide great opportunities for knowledge exchange and development, as well as networking with industry leaders. Will also highlighted the importance of knowledge transfer, where senior professionals are able to share real-world experiences with the next generation. This also allow organizations to get involved with grassroots talent, all the while ensuring a focus on technical innovation rather than executive trends.

OWASP Victoria, run by Roberto Salgado, focuses specifically on web application security, providing education and awareness through workshops and presentations, while also promoting open-source contributions. Roberto highlighted the noticeable talent gap within the offensive security community, specifically a lack of those with experience in simulated environments that replicate real-life scenarios. This is where OWASP comes in, providing real-world and hands-on experience for those seeking to enter more advanced roles related to offensive security. This quote from our interview summarizes this perfectly:

> "So they miss a lot of the fundamentals and jump right into hacking (based on) whatever they can copy/paste online (and extract) some basic stuff here and there...It's easy to kind of get started and get into it and get some initial results and success, I see a lot of people at that level. But to take it to the next level, you know you (will eventually) reach a cap or a point where if you don't understand the fundamentals or what is happening under the hood, you're not going to be able to progress further. And I'm seeing less people that are taking the time to learn those fundamentals, you know, learn that networking stuff, (and) learn how the code works. And they're just trying to jump right into hockey. So you get a lot of applicants who are kind of at the low and mid-tier (levels) are kind of stuck because they don't have a fundamental knowledge. Where I think traditionally a lot of people did."
>
> —*Roberto Salgado, Chief Executive Officer at Websec Canada*

Unfortunately, like the rest of the country and indeed the world, Victoria does have its challenges. Its geography is both a blessing and a curse. With other hubs having more active job markets in comparison, a lot of talent is lost to other major hubs such as Vancouver and even to U.S. companies in Silicon Valley, mainly in Seattle. Remote work has also become extremely competitive, and many companies are going to great lengths to employ talent through untraditional hiring. All this combined with a lack of VC's within the community and a lack of incentives for companies to either start or relocate here creates an environment which leaves room for improvement.

> "Companies are purposely putting in place very specific programs that go against typical HR hiring guidelines in order to allow and attract talent from different regions. So even if HR has a policy that (an employee) has to be in office or that (a hiring manager) has to be living in the city just to find the right people; I know that (companies) are saying we're going to make this role hybrid: We're going to make this role completely remote and to the point where if they have to come into head office, we will pay for their travels."
>
> —*Marleen Mavrow, Director, GRC & Privacy Officer; Director, SheLeadsTech, ISACA Vancouver Chapter*

Another challenge is the lack of entry-level jobs. This trend has been consistent for many years within the industry but is now especially prevalent as cybersecurity professionals are being affected by rounds of layoffs with tightening security budgets. In line with this is the lack of competitive wages when compared to other provinces and particularly to the U.S.

> "Probably the biggest challenge is a general challenge for the entire technical industry in Victoria and that is there are vanishingly few jobs for juniors. This has always been true."
>
> —*Will Whittaker, Principal Security Engineer at Change.org and BSides Organizer*

On a personal note, I have also noticed a lot of social media hype around cybersecurity being the new way to get a six-figure job within 30 days of completing a boot camp. Victoria is not immune to this and an influx of talent will mean more competition and put professionals at a disadvantage in the coming years, especially at the entry level.

So what does Victoria do about these challenges? There are some steps which our leaders are recommending. One of which is to highlight the lifestyle here to attract talent and business investment. With so much to offer in the way of business potential, as well as a more friendly environment

for a workforce to enjoy throughout the whole year, a better work-life balance is achievable here.

Another way is to embrace the accelerating AI race to increase productivity and efficiency for professionals. A concern with AI's rapid ascension is that it will replace employees at low-level engineering positions or those in DevSecOps. From what I have seen, AI isn't to be feared, it is to be leveraged to work symbiotically with us to achieve a safer world.

> "Generative AI obviously is a huge shakeup, and I see it as an additive and an accelerator, not so much a replacement."
>
> —*Marleen Mavrov*

With increased participation by both the talent and employers at local events like OWASP and BSides, as well as associations like the Victoria Chapter ISACA and the Victoria Innovation, Advanced Technology & Entrepreneurship Council (VIATEC), Victoria can concentrate and enhance its presence on the national and international stage by connecting with key figures in the industry and convince them to look at why Victoria is a cybersecurity powerhouse.

Many professionals highlighted untapped benefits that are often overlooked by businesses here in Canada. One example is the Scientific Research and Experimental Development Tax Credit Program, where businesses can take advantage of significant tax incentives for Canadian-controlled companies conducting R&D in Canada, effectively making Canadian developers cheaper for American companies setting up satellite offices. There are also many advantages of establishing a subsidiary in Victoria, drawing on the existing pool of senior talent and the cultural alignment with North American markets.

Finally, I would recommend attracting more venture capital through targeted investment incentives. The city could implement tax breaks, matching fund programs, grants, subsidies, and increased funding for local tech incubators and accelerators. Additionally, the city could develop programs to help local tech companies become investment-ready and organize networking events to connect them with potential investors.

In summary, Victoria's unique blend of natural beauty and technological innovation has fostered a small yet significant cybersecurity ecosystem. The region's attributes, including its growing talent pool, an expanding community of cybersecurity businesses, the attractive lifestyle, and a strong sense of collaboration, position it as an appealing location for both professionals and companies in the cybersecurity domain. However, challenges such as talent retention, limited entry-level opportunities, and a need for greater investment capital must be addressed to ensure continued growth. By strategically highlighting its lifestyle advantages, embracing technological advancements like AI, strengthening its community networks, promoting the use of government incentives, and actively working to attract venture capital, Victoria can overcome these barriers and further solidify its position as a leading cybersecurity hub. Continued focus on nurturing talent, fostering an inclusive and collaborative ecosystem, and proactively addressing the limitations to growth and investment will be essential for securing a vibrant and prosperous future for Victoria in the global cybersecurity landscape.

See end notes for this article's references.

Harry Lofts, Director of Governance, Risk and Compliance at iCompliance, is a cybersecurity professional with a focus on healthcare and retail banking compliance. He is dedicated to helping small and medium-sized businesses create compliance programs that protect critical personal and business information, meet regulatory requirements, and create a safer and more secure digital world for all.

PHOTO: SALVADOR MANIQUIZ

Winnipeg: Where East meets West with a Handshake

by Gerrit Bos

I heard all the clichés when I decided to move to Winnipeg for an innovative cybersecurity position: "Do you know how cold Winnipeg is? How about the long winters and how windy it gets?" What's more, people didn't believe I chose Winnipeg for information security. But I did, and I have no regrets. Although I have since relocated, I continue to work with my colleagues in Winnipeg and appreciate Winnipeg for all it offers, from the cybersecurity culture to the opportunities. Despite the self-deprecating humility often found among Winnipeggers, the Canadian Cybersecurity Network (CCN) affirmed my appreciation as Winnipeg was ranked fourth in the 2024 CyberTowns report.

So, the secret is out and Drew Carmichael did an excellent job last year highlighting some reasons why. I won't repeat what he wrote, but I encourage you to flip back to pages 30-33 of the 2024 report.[1] I would like to, however, offer a few more observations. First, population growth, while Winnipeg is not among the highest in Canada, this translates to more predictable housing prices and cost of living. Conversely, some of Canada's high-growth areas are associated with rising home prices and growing income gaps. And yes, Winnipeg has long, cold winters and is almost always windy, but Winnipeggers' ability to handle anything winter throws their way is unparalleled. Schools seldom close, the airport manages cold and icy conditions like

a champ, and the road-clearing efforts are impressive. I have been amazed that car washes operate successfully right through the coldest parts of winter without car doors freezing. From the world-renowned Festival du Voyageur[2] to the use of the Red River Floodway and associated Duff-Roblin Parkway Trail for skiing and snowboarding, Winnipeggers find ways to revel in winter activities. For those who have lived in Winnipeg for more than a year, I believe they would agree with me that the city should be ranked higher. If you are interested in why this is so from a cybersecurity perspective, read on!

Overview of the Cybersecurity Community

Winnipeg's cybersecurity community mirrors that of Manitoba in character and attitude. From the early days of confederation, Manitoba has been very independent, almost fiercely so, joining the Canadian Federation on its own terms. Manitoba is "compass-agnostic" and relates equally well with the East as the West of Canada. The province also has strong connections into the U.S. and into Canada's North. From a transportation perspective, Winnipeg's place on the popular board game "Ticket to Ride" is well earned. Manitoba, with Winnipeg as its capital, brings a "can do" attitude to everything it does.

Winnipeg's cybersecurity culture is vibrant, independent, yet open and accessible.

Winnipeg's cybersecurity culture can be traced back to the early days of hacking. The community is independent and yet cooperative, forward-looking yet grounded in the history and geography of the city and province. A prime example is Winnipeg's participation in the CyberTitan,[3] a cybersecurity competition for middle and high school students. Timothy King from the Information and Communications Technology Council (ICTC) highlights Sisler Cyber Academy's role in initiating CyberTitan in 2016: "Sisler High School was pivotal in (launching) Canada's longest running and largest national student cyber competition, now in its eight year." CyberTitan offers hands-on experience in cyber threat environments to students. Sisler High School and other Winnipeg schools are strong, courteous competitors, fostering a supportive environment.

Michael Legary, founder of Seccuris Inc. and former CIO of the City of Winnipeg, began his career in Networking and Information Security at 17 with the Government of Manitoba. He remains active in the Winnipeg cybersecurity scene, which is deeply rooted in relationships and thrives on word of mouth and handshakes. Not as flashy as in Toronto or Vancouver, Legary highlights the accessibility and welcoming nature of Winnipeg's cybersecurity culture, citing conferences and events like BSides, SkullSpace, as well as capture the flag competitions.

The post-secondary sector in Winnipeg combines independence with a strong culture of sharing and cooperation. All the colleges and universities are members of MRnet Inc. and participate in its governance and programs. Through MRnet, they are connected to the Canada-wide post-secondary ecosystem, allowing for sharing of experiences, and at a practical level, actionable threat intelligence such as indicators of compromise. As Kim Benoit, CIO of University of Winnipeg, and past-chair of the MRnet board says: "Most Universities cannot go (at) it alone on all issues of Cybersecurity. We need each other; we need to work together, and in strengthening each other, we improve the cybersecurity posture of the entire sector in Manitoba, and Canada-wide." These institutions contribute to the cybersecurity culture through technical programs and community integration. A number of the helpful folks I interviewed were adjunct instructors at a post-secondary institution.

Winnipeg's cybersecurity culture is vibrant, independent, yet open and accessible. It values individual talents while fostering a supportive, sharing environment. If this culture appeals to you, you will quickly feel at home in Winnipeg.

Strategies for Attracting and Retaining Cybersecurity Talent

The primary strategies for Winnipeg to attract and retain Cybersecurity talent are organic. They fall in three categories, the people, the positions, and the place.

Winnipeg's greatest assets are its people. When we moved, we quickly made life-long friends. The people of The Peg (the local nickname for itself) are gregarious, resilient, and industrious. They are independent yet cooperative. Michael Legary notes that Winnipeg, about five hours drive away from the nearest large metropolis, is self-sufficient and excels in whatever is thrown at it. It might sound like

the city is isolated, but Legary highlights the healthy work-life dynamics and vacation opportunities that Winnipeg offers. James Teitsma, Executive Vice President of Conquest Planning adds that Winnipeg offers better commutes and a more relaxed lifestyle than many other metropolitan areas. In James' view, this total package has resulted in a significant base of IT professionals and practitioners, who are competent, capable, and well connected.

These strengths are evident in Winnipeg's information security community. Opportunities to connect through formal and informal networks are abundant and accessible. Michael Himbeault, Director of Cybersecurity at Neo Financial illustrates this by pointing to events like Tech Thursdays, BSides, DC204, Longcon, and consultant networks formed by established and new professionals.[1] There is also a growing Slack group[2] with over 330 cybersecurity professionals that connects community members with opportunities and support, which was instrumental during the pandemic. Many of these members are Winnipeg expats who continue to collaborate and show support. You can take people out of The Peg, but not The Peg out of people.

The second organic strategy for attracting and retaining cybersecurity talent in Winnipeg is the variety of positions available. The city hosts diverse businesses, including numerous Crown Corporations with cybersecurity needs. James Teitsma, former Minister of Government Services, points to the many organizations who work together to meet these needs, creating positions along a continuum of skills and experiences. Successful startups like Skip the Dishes and Neo Financial also round out the breadth of cybersecurity professionals required. Michael Legary, an experienced educator, emphasizes that the demand for cybersecurity talent in Winnipeg exceeds the supply, stating: "The opportunities in Winnipeg are active, and they are NOW!"

The third strategy for attracting cybersecurity talent is Winnipeg itself. The city boasts a vibrant culture, shorter commutes, and vacation destinations. Winnipeg's excellent transportation infrastructure should also be highlighted here, allowing residents to fly to major cities for business and return the same day. Winnipeg also has miles and miles of multi-use trails, which are consciously built into the design of new subdivisions.

[1] Michael mentioned that these are sometimes called 'Body Shops', but in Winnipeg there is almost no negative connotation to these networks.

[2] I am not a member of the group, but a good friend and colleague asked if it was OK to share the invite link. They agreed, but please treat receiving it as a privilege.

Tourist attractions The Forks and the annual Folklorama Festival[4] showcase Winnipeg's diverse cultures. Unique spots such as the Canadian Museum for Human Rights and the Red River Mutual Trail offer experiences not found in other major cities. Despite these highlights, the city's essence is hard to capture fully, the years that I lived there are not sufficient for me to totally get it.

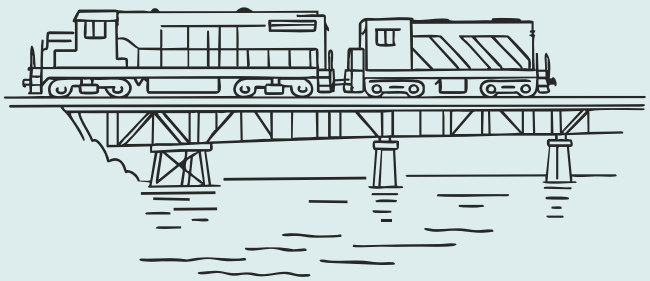
While organic activities are key to attracting IT and cybersecurity talent, Winnipeg also benefits from incubators, investor groups, and non-profits supporting startups and entrepreneurs.

Residents of the Peg have a strong, but understated, sense of humour that the place is very flat. I once saw a laughable sign in Birds Hill park just north of the city on a multi-use (bike and hiking) trail where park staff installed a "Steep Hill ahead" warning. Walking this steep incline both ways did not change my heart rate, to say the least. Jokes aside, Winnipeg's flat terrain and annual spring flooding deeply affect residents. The Red River Floodway projects illustrate the city's pragmatism and cooperation, significantly reducing flood damage.

While organic activities are key to attracting IT and cybersecurity talent, Winnipeg also benefits from incubators, investor groups, and non-profits supporting startups and entrepreneurs. The Manitoba Technology Accelerator drives Winnipeg's position as the start up capital of Western Canada through investment, mentorship, and infrastructure support.[5] ISACA, with Craig McGrath as the president of the Winnipeg chapter, fosters a positive atmosphere and community connections. Overall, Winnipeg presents a well-rounded and inviting environment for new enterprises and job-seekers.

Barriers and Challenges

Like any city, there are some barriers and challenges. Winnipeg can at times make people feel isolated, which can impact family relations despite good transportation connections. Salary caps in the public sector and crown corporations can deviate up to 30% from market rates, making it difficult to hire and retain quality staff. While this is widely



A TALE OF TWO BRIDGES

Southern Manitoba is a vast flood plain,[1] with much of the flood water coming from the Red River, which flows north from Fargo, North Dakota. The combination of local run-off, spring rains, snow-melt, and the swelling Red River can cause devastating floods. Decades ago, Manitobans realized Winnipeg could not thrive due to annual flooding risks to infrastructure. The Red River Floodway, a massive waterway[2] bypassing the city, was built to divert floodwaters and protect Winnipeg. Initially nicknamed "Duff's Ditch"[7] after Premier Duff Roblin, the floodway has since become an affectionate term. The floodway now features a park and multi-use trail along its length. The project's success required significant cooperation and compromise. Here are two additional examples that illustrate some of the less tangible aspects of what makes Winnipeg and Manitoba thrive:

1.The "Lego Bridge:" Winnipeg's railways, crucial for east-west connections, needed a stronger, higher bridge. Engineers built a modular "Lego Bridge," which was later disassembled and repurposed.[8]

2.CEMR Bridge: The privately owned CEMR bridge across the floodway was not raised to the flood height standard, saving costs but presenting risks. Each spring, heavily loaded railway cars are parked on the bridge to mitigate flood risks.[9]

These projects illustrate the importance of risk/benefit calculations and multi-disciplinary cooperation, similar to cybersecurity needs.

[1] There are some exceptions, like La Riviere, as Steve Boyko accessed April 18, 2025) pointed out to me.

[2] The floodway is 46 kilometers long, and at the time of completion, it was the second largest earth-moving project in the world behind the Panama Canal.

acknowledged, James Teitsma highlights remote work opportunities and Winnipeg's quality of life as counterpoints to these challenges. He also pointed out that even some hockey players were initially hesitant to join the Winnipeg Jets, but were happy to stay because of the community and the culture.

Another challenge is the slow pace of integrating non-traditional employees into cybersecurity. Winnipeg's relationship-based culture can be a barrier, but progress is being made and things are looking up. Craig McGrath notes increased participation from women, LGBTQ, and indigenous communities. GlitchSecure[6] exemplifies inclusive values while helping companies with continuous security testing and real-time penetration testing. Their inclusive approach brings together different viewpoints, which helps in finding creative solutions and tackling problems more effectively.

Future Outlook

Winnipeg's steady growth, diverse economy, and strong work ethic position it well for the future. While humility sometimes prevents showcasing its strengths, when Winnipeg does, people take notice. The city has a positive story to tell, especially in cybersecurity. We live in a time when the future holds many uncertainties, but Winnipeg's future is bright. The city has weathered economic, political, technological, and environmental storms, and is well-prepared for future challenges.

In cybersecurity there are many potential storms on the horizon, including uncertainties in AI and quantum technologies, political changes, and increasing threats from bad actors as well as nation states. Winnipeg's cybersecurity community is resilient, well-connected, and committed. By making Winnipeg your home, working hard, and engaging with the community, you can contribute to its success. With continued effort, Winnipeg could rank even higher in future CCN surveys, perhaps even first place! Let's shake on that!

See end notes for this article's references.

Gerrit Bos is the Chief Information Security Officer for MRnet Inc., a Not-for-Profit supporting Manitoba's postsecondary sector with shared Networking and Security services. He has more than 30 years' experience in Information Technology, the last fourteen years in Information Security—more if you count his hacking days in University.

Conclusion & Recommendations

Canada stands at a defining moment in its cybersecurity journey. As the CyberTowns report reveals, world-class talent, innovation, and community strength are thriving across 12 distinct cities, each offering unique advantages in workforce development, educational excellence, quality of life, and economic opportunity.

But this momentum must not stay siloed. To lead globally, Canada must unify locally bridging regional strengths across all 10 provinces and 3 territories to build an interconnected cybersecurity ecosystem. We must leverage Calgary's OT/energy expertise, Toronto's density of enterprise and academic anchors, Montreal's hacker culture, Victoria's work-life magnetism, and Fredericton's cyber-education legacy, among others. This national model of distributed excellence can only succeed through intentional collaboration.

Canada has a generational opportunity to outcompete the world.

Cybersecurity professionals want more than just jobs, they want to live, work, and learn in vibrant communities that invest in them and their families. Canada has a generational opportunity to outcompete the world not by paying the most, but by being the most desirable place for talent and technology to thrive.

> "Canada doesn't have to pay the most, or be the biggest, to become the global home of the best cybersecurity talent. We have to create the strongest community; one where world-class people, research, and technology come together in places they want to live and grow with their families."
>
> *—François Guay, Founder, Canadian Cybersecurity Network*

Key Recommendations for National Action

1. **Establish a national cyber talent strategy** that includes shared metrics, regional partnerships, and scalable micro-credential programs tailored to emerging technologies like AI and quantum security.
2. **Accelerate inter-provincial collaboration** by funding cross-city initiatives, shared innovation hubs, and federal incentives for community-building across cities of all sizes from St. John's to Whitehorse.
3. **Expand newcomer integration pathways** through credential recognition, mentorship programs, and multilingual career supports to harness untapped global talent already in Canada.
4. **Support affordability and livability** through housing, transit, and remote work policies that ensure mid-career talent can stay and raise families in every corner of the country.
5. **Create national cyber community programs** that link students, professionals, educators, and industry through events, mentorship, and collaborative platforms year-round.

Final Thought

If Canada can mobilize the strengths of all its CyberTowns, it won't just have a great cybersecurity industry, it will build one of the world's most trusted and resilient digital societies.

References

Calgary

[1] Data about Calgary's population, accessed 8 February 2025

[2] Report Library | Data and industry resources | Calgary Economic, accessed 8 February 2025

[3] Cybersecurity: Global Talent Spotlight | CBRE, accessed 8 February 2025

[4] Demographics | Economic Indicators | Calgary Economic, accessed 18 February 2025

[5] Ibid

[6] CREA | National Price Map, accessed 18 February 2025

[7] CS 2024 Report to Community F4 (2), accessed 9 March 2025

[8] Folk Fest | CFMF, accessed 9 March 2025

[9] Flames unveil arena plans, expect new home to help attract talent | NHL.com, accessed 18 February 2025

[10] Arts Commons Transformation Project, accessed 18 February 2025

[11] About Us » CIFF, accessed 9 March 2025

[12] Beakerhead at TELUS Spark, accessed 9 March 2025

[13] Diversity, Equity & Inclusion - Calgary Pride, accessed 9 March 2025

[14] GlobalFest–Alberta's Most Explosive Festival!, accessed 9 March 2025

[15] Cybersecurity job market analysis 2024: Key findings and insights, accessed 8 February 2025.

[16] Ammolite Security - Cybersecurity Company, accessed 15 March 2025.

[17] URL for SAIT and quote: Cyber Security Programs, accessed 9 March 2025.

[18] Cybersecurity Post-Diploma Certificate | Bow Valley College, accessed 9 March 2025.

[19] INFORMATION SECURITY | Faculty of Science | University of Calgary, accessed 9 March 2025.

[20] Fortinet Commits $30M Toward Cutting-Edge Cybersecurity Tech Hub in Calgary - Calgary.Tech, accessed 10 February 2025

[21] Finding, Fueling & Fostering Calgary's Future | Opportunity Calgary, accessed 18 February 2025.

[22] Platform Calgary | Calgary's Home for Innovators, accessed 9 March 2025

[23] M-Tech Innovations, accessed 9 March 2025.

[24] TECTERRA ANNOUNCES $5.2M LEGACY PROGRAM FOR ALBERTA BASED POST-SECONDARY INSTITUTIONS–TECTERRA. Accessed 9 March 2025

[25] Calgary Reports Driving Tech Forward.pdf, accessed 18 February 2025.

[26] CATE Centre | ENFOCOM Cyber, accessed 11 March 2025.

[27] Canadian financial sector faces rising cybersecurity challenges: report | Investment Executive, accessed 9 March 2025

[28] Cybersecurity job market analysis 2024: key findings and insights, accessed 9 March 2025.

[29] Cyber Security Salary in Canada in 2025: Trends & Insights, accessed 9 March 2025.

[30] Canada Cybersecurity Salaries: What Can You Expect to Earn?, accessed 9 March 2025.

[31] CS4CA Summit 2024 - Canada | QG Media | 11 June ... | Qwoted, accessed 9 March 2025.

[32] 2024 Calgary CISO Executive Summit, accessed 9 March 2025.

[33] BSides Calgary 2025, accessed 9 March 2025.

[34] Calgary Cyber Security for Control Systems | Meetup, accessed 9 March 2025.

[35] History, accessed 15 March 2025.

[36] SecuredNet | PCI Compliance & Pentesting, accessed 9 March 2025.

[37] #bsidescalgary #bsides #cybersecurity #sponsorship | James Cairns, accessed 9 March 2025.

[38] Amenaza Technologies Limited - Home Page, accessed 9 March 2025.

[39] Many cybersecurity pros report low job satisfaction—all while trying to fend off increasing threats from hackers | Fortune, accessed 9 March 2025.

[40] Alberta King's Printer, accessed 9 March 2025.

[41] Stubified, accessed 9 March 2025.

[42] Varcoe: Calgary No. 2 among Canadian cities most vulnerable to tariffs | Calgary Herald, accessed 9 March 2025.

Edmonton

Alberta Machine Intelligence Institute. (2025, February 11). About—Alberta Machine Intelligence Institute. Retrieved from Alberta Machine Intelligence Institute.

Art Gallery of Alberta. (2025, February 20). Collection | About |Art Gallery of Alberta: Art Gallery of Alberta. Retrieved from Art Gallery of Alberta.

Boily, C. (2024, March 7). The Edmonton Region's tech sector sees strongest growth ever, fuelling Alberta's tech momentum. Retrieved from Edmonton Global.

Canadian Cybersecurity Network. (2025, Februrary 23). Cyberguardians. Retrieved from The Canadian Cybersecurity Network.

CBRE Research. (2024). Scoring Tech Talent 2024. CBRE Inc.

City of Edmonton. (2025, February 17). Economic Action Plan | City of Edmonton. Retrieved from www.edmonton.ca

Concordia University of Edmonton. (2025, February 17). Master of Science in Information Technology - Concordia University of Edmonton. Retrieved from Concordia University of Edmonton.

Cost of Living in Edmonton, Alberta | Cost of Living Index | ERI. (2025, February 18). Retrieved from Economic Research Institute.

Cybera Inc. (2025, February 11). About us - Cybera. Retrieved from Cybera - A Connected Future for All Albertans.

CyberSN. (2025, February 23). The Importance of Cybersecurity Tallent Retention | CyberSN. Retrieved from CyberSN.

Edmonton Global. (2025, February 17). Who We Are | Edmonton Global. Retrieved from Edmonton Global.

Edmonton Research Park. (2025, February 17). Edmonton Research Park | Building Global Innovation, Locally. Retrieved from Edmonton Research Park.

Edmonton Unlimited. (2025, February 17). Impact - Edmonton Unlimited. Retrieved from Edmonton Unlimited.

Edmonton Unlimited. (2025, February 17). Inovation in Edmonton - Edmonton Unlimited.

Government of Alberta. (2022). Alberta Technology and Innovation Strategy (ATIS). Edmonton: Government of Alberta.

Government of Alberta. (2025, February 17). Innovation Employment Grant | Alberta.ca. Retrieved from Government of Alberta.

Guay, F. (2024, May 23). Edmonton a technology colossus in the making. Retrieved from Canadian Cybersecurity Network.

Invest Alberta. (2025, February 17). Shaping the Future of AI with Innovation and Talent. Retrieved from Invest Alberta.

ISC² . (2024, October 31). 2024 ISC² Cybersecurity Workforce Study. Retrieved from ISC².

Nacario, A. (2025, February 5). How Much Does it Cost to Live in Edmonton in 2025. Retrieved from Moving Waldo.

NAIT. (2025, February 17). NAIT. Retrieved from NAIT - A Leading Polytechnic Committed to Your Sucess.

Numbeo. (2025, February 23). Quality of Life Comparison Between Edmonton and Toronto. Retrieved from Numbeo.

Public Sector Network. (2025, February 23). Government Cybersecurity Showcase–Alberta - Public Sector Network. Retrieved from Public Sector Network.

Technation. (2022, October 17). Canada's cybersecurity industry sees 30% growth. Retrieved from Technation.

The City of Edmonton. (2025, February 17). Edmonton: Smart City | City of Edmonton. Retrieved from The City of Edmonton.

Thomas, K. (2025, February 17). Canada Unveils $6.5M for Four Edmonton-Based Technology Innovators to Diversify Alberta Economy. Retrieved from Calgary Tech.

Zip Recruiter. (2025, February 18). Salary, Cybersecurity in Edmonton, AB (Feb 2025). Retrieved from Zip Recruiter.

Fredericton

https://blogs.unb.ca/newsroom/2024/12/federal-funding.php

NBCC 2021 survey of 2020 graduates

https://nbcc.ca/core/research-projects
critical-infrastructure-security-operations-centre

https://www.techimpact.it/publications

Opportunities NB

Greater Toronto Area

blogTO. (2024, July). Toronto has fallen off the list of the world's most liveable cities.

Canada's National Quantum Strategy. (2024, December 3). Innovation, Science and Economic Development Canada. Retrieved March 3, 2025.

City of Toronto. (n.d.). City of Toronto. Congestion Management Plan.

City of Toronto. (n.d.). Office of the Chief Information Security Officer. 2025 Budget Notes.

City of Toronto. (n.d.). Technology.

City of Toronto. (2020). Update on Waterfront Toronto's Quayside Project. Item - 2020.EX19.4.

CTV News. (2025, January 18). The Toronto region's population has topped 7 million. Here is what you need to know.

Education – City of Toronto. (n.d.). Retrieved March, 2025.

5 Years of Cyber Impact. (2023). 2018-2023.

Future Skills Centre. (2022). A Race for Talent. Insights from Canadian Cybersecurity Employers. Retrieved 2025

Gartner Unveils Top Eight Cybersecurity Predictions for 2024. (2024, March 18). Gartner. Retrieved April, 2025, from

Global Cybersecurity Outlook 2025 | World Economic Forum. (2025, January 10). Publications. Retrieved April, 2025.

Humber Polytechnic. (n.d.). Cybersecurity and Artificial Intelligence - Humber Polytechnic. Faculty of Applied Sciences & Technology. Retrieved 2025.

ISC2. (2024, April 25). ISC2. Women in Cybersecurity: Inclusion, Advancement and Pay Equity are Keys to Attracting and Retaining More Women.

Metz, C. (2022, March 21). Toronto's Tech Industry Is Quietly Booming. The New York Times. Retrieved March, 2025.

'Not good enough': Toronto privacy expert resigns from Sidewalk Labs over data concerns. (2018, October 21). CBC. Retrieved 2025, from

Public sector salary disclosure 2024: all sectors and seconded employees. (2025, March 28). Ontario.ca. Retrieved April, 2025.

Robert Half. (2025). Cybersecurity Analyst in Toronto, ON.

Statistics Canada. (2022, November 4). Focus on Geography Series, 2021 Census of Population.

Statistics Canada. (2024, August 26). The Daily — More Canadians commuting in 2024. Retrieved April 5, 2025.

To, M. (2025, January 16). City of Hamilton budgets over $52M for 2024 cyberattack response. CHCH. Retrieved March, 2025.

Victoria

members.viatec.ca Victoria's Tech Sector Surges: New Economic Impact Study Reveals $7.8 Billion Contribution - VIATEC

techcouver.com Impact Study from VIATEC Highlights Steady Growth for Tech Industry on Vancouver Island

victechjournal.com VIATEC report highlights tech's impact - Victoria Tech Journal

viatec.ca 2023 Economic Impact of Greater Victoria Tech Sector - Victoria...

vicnews.com Study shows $7.8 billion economic contribution from Victoria tech sector

github.com index.md - OWASP/www-chapter-victoria - GitHub

infosecmap.com BSides Vancouver Island - InfoSecMap

crestwoodsearch.com BSides Vancouver Island | Crestwood Search

meetup.com OWASP Victoria Chapter | Meetup

techdogs.com Bsides VI 2024 - TechDogs

weforum.org AI-driven cybercrime is growing, here's how to stop it | World...

cybersecurityventures.com Cybercrime To Cost The World $10.5 Trillion Annually By 2025

funding.ryan.com SR&ED Tax Credits | Research & Development Funding Canada | Ryan

canada.ca Scientific Research and Experimental Development (SR&ED) tax...

pwc.com SR&ED tax credit consulting & financing solutions | PwC Canada

canada.ca Scientific Research and Experimental Development (SR&ED) tax incentives - Canada.ca

kruzeconsulting.com Canada R&D Tax Credits - Kruze Consulting

engage.isaca.org Home - Victoria Chapter - ISACA Engage

builtin.com Senior Director, Digital Transformation & Technology Innovation - BCI - Built In

privateequityinternational.com BCI | Institution Profile - Private Equity International

pehub.com Macquarie and BCI to take Renewi private for £707m - PE Hub

bci.ca Private Equity - British Columbia Investment Management Corporation - BCI

bci.ca Our Locations and Contact Information - BCI

bci.ca Student Work Terms and Internships at BCI | Work with us

aijobs.net Data Governance Analyst Co-op/Intern (Summer & Fall 2025) at BCI - CA Victoria, Canada

bci.wd10.myworkdayjobs.com Quantitative Equity Co-op/Internship (Summer and/or Fall 2025 and/or Winter 2026)

infosecmap.com VIPSS 2025–Victoria International Privacy & Security Summit`

microserve.ca 27th Annual Victoria International Privacy & Security Summit | Microserve Canada

outcomes.bcstats.gov.bc.ca BC Student Outcomes - Gov.bc.ca

uvic.ca Engineering and computer science graduate students - Co-operative Education - UVic

www2.gov.bc.ca Industry Intelligence - Province of British Columbia - Gov.bc.ca

Winnipeg

[1] https://canadiancybersecuritynetwork.com/cybertown (accessed March 20, 2025)

[2] https://en.wikipedia.org/wiki/Festival_du_Voyageur (accessed April 11, 2025)

[3] https://etalentcanada.ca/for-educators/programs/cybertitan (accessed March 20, 2023)

[4] https://folklorama.ca/ (accessed April 11, 2025)

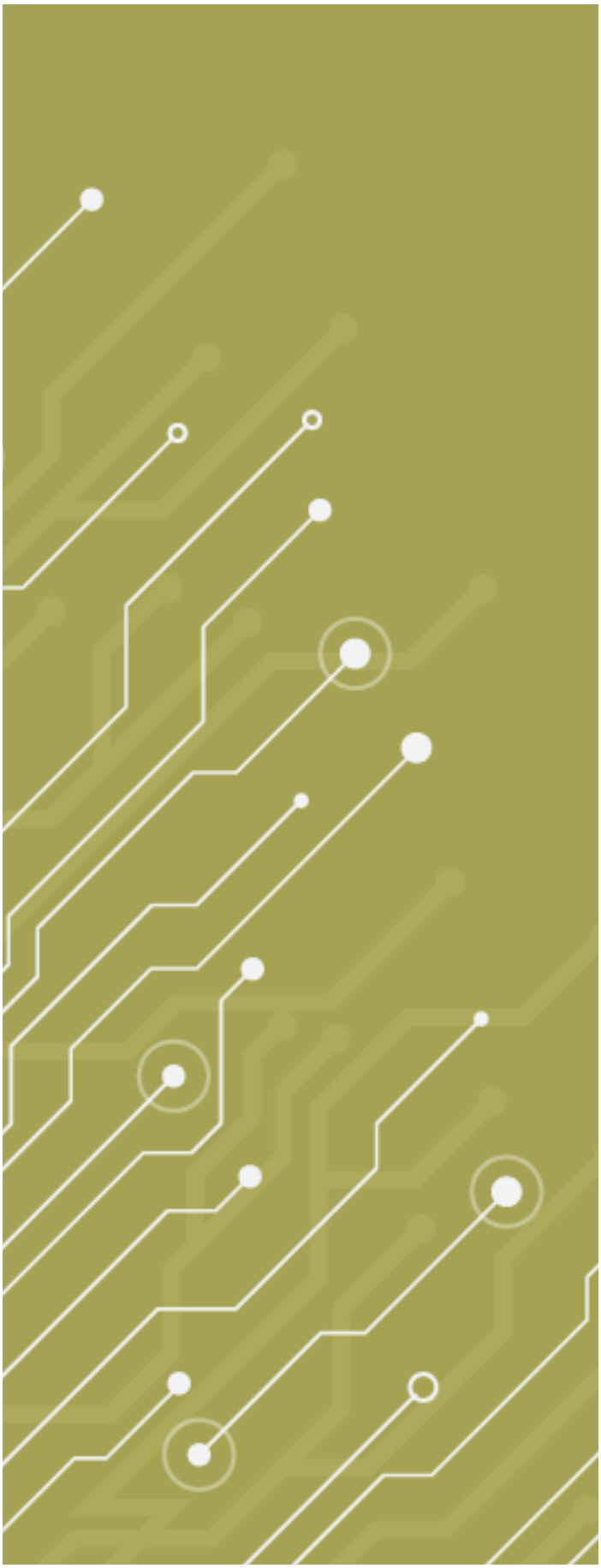
[5] https://mbtechaccelerator.com/ Accessed April 7, 2025.

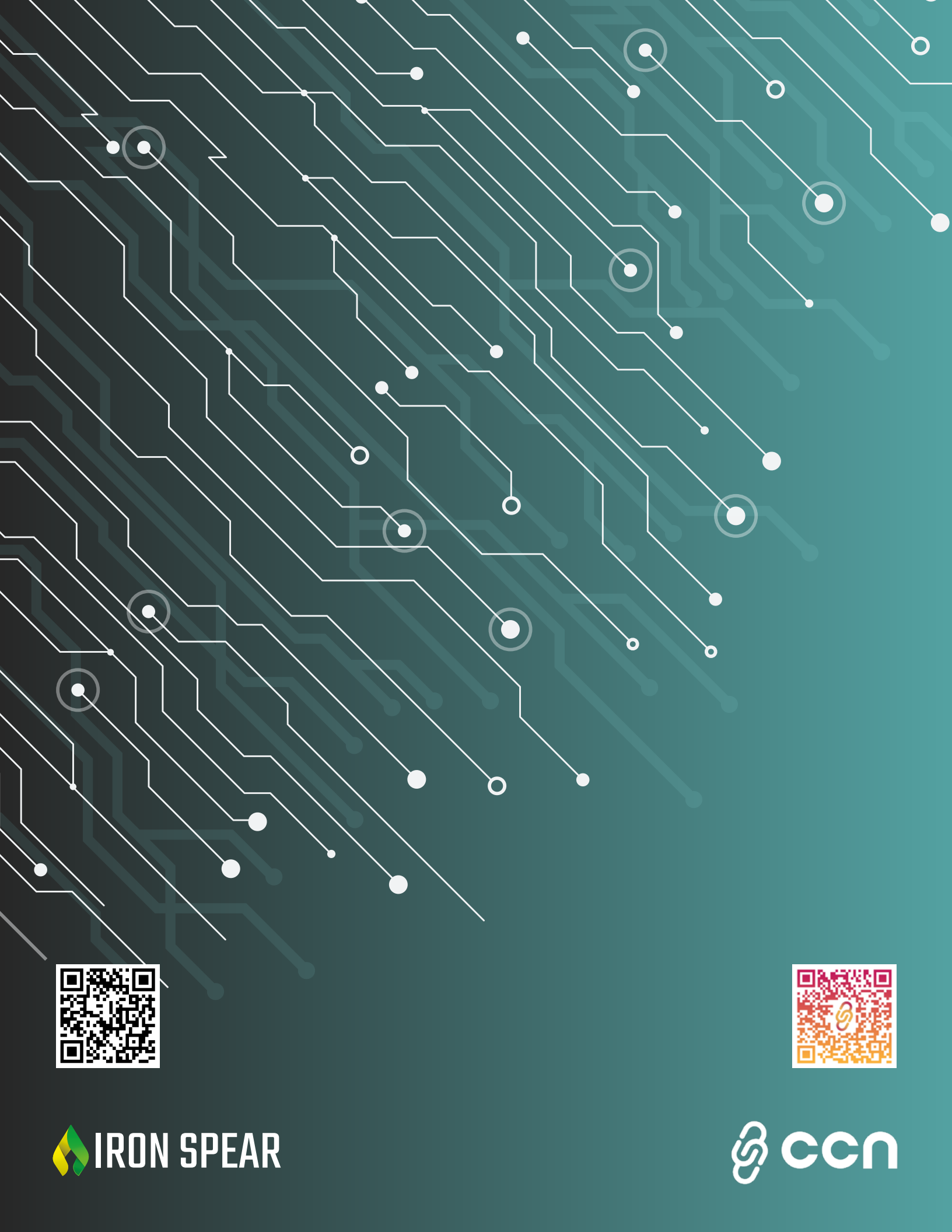
[6] https://glitchsecure.com/about/ accessed April 12, 2025.

[7] https://en.wikipedia.org/wiki/Red_River_Floodway (accessed March 27, 2025)

[8] For technical details see the Bridge Replacement paper presented by Norman Ulyatt at the 2007 Annual Conference of the Transportation Association of Canada (accessed April 18, 2025):

[9] https://www.candorail.com/cemr/ (accessed March 27, 2025)




IRON SPEAR
ccn