INVEST TALENT

High Tech Case Study:

Cybersecurity Workforce Development

Cybersecurity Invest Talent Pilot

Invest Vancouver focuses on growing export-oriented industries that generate high-quality jobs and strengthen the regional economy. Because these firms compete globally and can choose where to locate, workforce availability and job readiness increasingly influence investment decisions, particularly in sectors where trust, security, and regulatory compliance are critical.

In this context, and with the support of the Future Skills Centre, Invest Vancouver launched the High Tech - Cybersecurity Invest Talent pilot to address workforce challenges in Metro Vancouver's rapidly expanding cybersecurity sector. The pilot was informed by global investment trends, national and provincial labour market intelligence, and extensive employer engagement, ensuring alignment with real-time industry demand and investment priorities.

Unlike the MedTech Invest Talent pilot, which tested short-cycle training delivery, the cybersecurity work intentionally focused on employer engagement, demand validation, and ecosystem coordination. Given the breadth of roles, rapidly evolving skill requirements, and diversity of employers in cybersecurity, Invest Vancouver prioritized building shared understanding and system readiness as a necessary first step before launching role-specific training pilots.

Global and Economic Context

Cybersecurity is a high-growth, globally mobile industry driven by digital transformation, cloud adoption, AI-enabled threats, and expanding regulatory requirements. Between 2019 and 2024, global cybersecurity foreign direct investment projects increased from 184 to 288 annually, while associated job creation rose from approximately 14,000 to more than 37,000 jobs.

Global investment data shows that access to skilled talent is the single most important factor influencing cybersecurity investment decisions, cited in nearly 45% of projects, followed closely by proximity to customers. As a result, regions that can demonstrate workforce readiness and coordinated talent systems are better positioned to attract and retain cybersecurity investment.

> "The challenge isn't just finding people - it's finding people who can operate effectively in our environment. Even strong candidates often need months of mentoring before they're fully productive, and that has real cost and risk implications for the business."
>
> - Chief Information Officer, TelCom

The Economic Development Challenge

Cybersecurity is an export-oriented, high-growth sector in Metro Vancouver. Since 2019, employment in software and IT has grown by more than 50%, with cybersecurity-specific roles increasing by over 120%. The sector supports a wide range of industries, including financial services, healthcare, transportation, energy, and the public sector.

Despite strong growth, approximately 80% of cybersecurity employers that were interviewed via Invest Talent consistently indicated severe difficulty filling key roles, particularly at the intermediate and senior levels. The most difficult-to-fill positions include:

- Security Analysts (Blue Team / SOC)
- Cloud Security and Identity & Access Management Engineers
- Security Architects with responsibility for risk, compliance, and enterprise alignment

Employers also identified persistent gaps in applied, business-critical skills, such as communicating risk to executives, operating in regulated environments, and making decisions under incident pressure, highlighting a disconnect between traditional training pathways and job readiness.

Employer Engagement and Demand Validation

The Cybersecurity Invest Talent pilot engaged a broad cross-section of employers spanning financial services, technology, critical infrastructure, healthcare, professional services, and the public sector. Participants included global cybersecurity firms, large enterprises with in-house security teams, managed security service providers, and fast-growing technology companies.

This breadth of employer involvement revealed a highly fragmented demand profile, with significant variation in:

- Role definitions and seniority expectations
- Tool stacks and cloud environments
- Regulatory and compliance requirements
- Security clearance and trust obligations

Rather than centring on a single anchor employer, Invest Vancouver intentionally tested how Invest Talent could function as a neutral convenor, aggregating demand across multiple employers to identify shared priorities, common gaps, and system-level constraints.

Despite the diversity of roles and contexts, employers consistently emphasized a need for:

- Stronger alignment between training and enterprise environments
- Greater emphasis on defensive ("Blue Team") capabilities
- Improved pathways for career switchers and internationally trained professionals
- Coordinated approaches that reduce duplication and hiring friction across the ecosystem

Key Workforce Development Challenges Identified

Employer engagement surfaced several structural challenges shaping cybersecurity workforce development in Metro Vancouver:

- Breadth and complexity of roles. Cybersecurity demand spans a wide range of functions, making one-size-fits-all training models ineffective.
- Rapidly evolving skill requirements. Cloud security, identity management, automation, and enterprise tools evolve faster than traditional curriculum cycles.
- Shortages at intermediate and senior levels. Entry-level interest is strong, but employers face acute shortages in roles requiring experience, judgment, and leadership.
- Gaps in applied and contextual skills. Many candidates lack experience operating in regulated environments or translating technical risk into business decisions.
- Barriers to inclusion and mobility. Credential recognition, security clearance requirements, and access to Canadian work experience limit participation for newcomers and internationally trained professionals.

These challenges reinforced the need for system-level coordination before launching training interventions.

What This Phase Tested: Ecosystem Readiness and Alignment

Rather than delivering training, the Cybersecurity Invest Talent pilot focused on building the conditions necessary for effective employer-led pilots.

Key activities included:

- Structured employer interviews to build relationships, validate demand and role priorities
- Skills Needs Forums to translate employer demand into shared signals for education, workforce, and community partners
- Cross-sector dialogue to identify misalignment across training, hiring, and policy
- Early pathway mapping for potential role-specific pilots

This approach reduced fragmentation across the ecosystem and established a common foundation for coordinated action.

Why the Metro Vancouver Region?

Metro Vancouver is emerging as a strong cybersecurity hub, anchored by a growing cluster of product companies, managed security providers, and global firms, alongside deep research and talent capabilities.

The region benefits from:

- One of Canada's largest concentrations of technology talent
- Strong post-secondary and applied research capacity
- Adjacent strengths in AI, quantum technologies, and advanced analytics
- A stable, trusted regulatory environment supporting secure digital infrastructure

Between 2019 and 2025, Metro Vancouver attracted seven cybersecurity foreign direct investment projects, representing more than US$550 million in capital investment and over 1,000 jobs created. While competing with larger hubs such as Toronto and Montréal, the region performs strongly against peer cities and offers significant room for growth.

For cybersecurity firms operating in regulated or risk-sensitive environments, Metro Vancouver provides a compelling alternative to U.S. hubs - combining talent depth, policy alignment, and institutional trust.

Looking Ahead: From Ecosystem Alignment to Employer-Led Pilots

The Cybersecurity Invest Talent pilot established a clear proof point: effective workforce development in cybersecurity must begin with coordinated employer demand and ecosystem alignment.

Drawing on lessons from the MedTech Invest Talent pilot, Invest Vancouver is now positioned to move into a next phase of employer-driven cybersecurity pilots, focused on:

- Clearly defined, high-demand roles such as Security Analysts and Cloud Security Specialists
- Short-cycle, applied training aligned to enterprise tools and environments
- Modular and stackable pathways for career switchers and internationally trained professionals
- Continued employer leadership and cross-sector co-design

By sequencing ecosystem alignment first and training delivery second, Invest Vancouver is building a resilient, scalable talent accelerator model that reflects the complexity of cybersecurity while maintaining the speed and relevance required by globally competitive firms.

Connecting employers, learners, and partners

Contact us at investtalent@investvancouver.ca

Invest Vancouver

INVEST TALENT