THE GLOBE AND MAIL

Report on Business

Canada faces massive shortage of cybersecurity workers

By ALEXANDRA POSADZKI
Staff

1,227 words
2 September 2019
The Globe and Mail
GLOB
Ontario
B2
English

Lack of candidates who are able to prevent data breaches means agencies, businesses and customers are left vulnerable to attacks

A lana Staszczyszyn never predicted she would be speaking about cyberwarfare at conferences, or getting paid to hack into networks.

The Toronto resident attended an art-focused high school and had planned to become an artist and a musician. But she also enjoyed math and science, so when a family friend in the technology industry told her that a career in cybersecurity could be lucrative and stable, she was intrigued.

“He said, ‘You're never going to not have a job,' " says Ms. Staszczyszyn, now 23. "That was the most attractive thing to me."

Shortly after completing Sheridan College's four-year bachelor's program in cybersecurity, Ms.Staszczyszyn has already landed a gig at Security Compass, a Toronto-based firm that specializes in penetration testing – the practice of intentionally hacking into a system in order to identify its weaknesses.

The demand for skills such as hers is huge and growing rapidly.

Canada faces a massive shortage of cybersecurity talent, an issue that leaves government agencies, businesses and customers vulnerable to attacks. The situation is so urgent that Ryerson University – with financing from Rogers Communications, the Royal Bank of Canada, the federal government and the City of Brampton – is preparing to launch a bootcampstyle program that will ready workers for entry-level roles in the cybersecurity sector in just 20 weeks.

“One of the challenges that we have with the existing programs in universities is that they take five years [to complete]," says Laurie Pezzente, senior vice-president of global cybersecurity at the Royal Bank of Canada. “We don't have five years to wait."

A study published last year by non-profit IT security organization (ISC)2 pegged the number of unfilled cybersecurity positions globally at 2.93 million. In Canada, organizations will be looking to fill roughly 8,000 such roles between 2016 and 2021, according to a 2018 report by Deloitte and Toronto Financial Services Alliance (now Toronto Finance International), an organization aimed at promoting and developing Toronto's financial-services sector.

By some estimates, the numbers are even higher. Recruitment firm Randstad, which tracks job openings, says Canadian organizations posted 5,100 new cybersecurity positions in 2017 and another 5,700 in 2018.

“Almost every major Canadian organization has postings that they can't fill," says Ryan Wilson, a partner in EY's Canadian cybersecurity practice. “Employers are paying a premium for experienced professionals."

Many sectors of the economy face a dearth of talent these days, but Jennifer Reynolds, president and chief executive of Toronto Finance International, says that addressing the shortage in cybersecurity should be “at the front of the line."

“Cybersecurity is critical to the economy and it can pose huge economic threats," Ms. Reynolds says. “This isn't like, ‘Oh we can delay building something.' We have to have this talent." The issue has become top of mind for corporate boards as well, as the increasing prevalence of cyberbreaches highlights the significant costs and reputational damage associated with such attacks.

EY pegs the average cost of a data breach globally at US$3.62million, a figure that includes patching up security issues, paying for credit monitoring for affected users and managing public relations.

“Not a week goes by without some company coming forward, recognizing that there's been some breach and then having to manage that," says Rahul Bhardwaj, president and chief executive of the Institute of Corporate Directors, Canada's national association for boards and directors.

Among the more recent incidents was a breach at Capital One that affected six million Canadians and roughly 100 million U.S.

customers – and left the financial institution facing potential classaction lawsuits on both sides of the border.

Part of the issue, says Ali-Akbar Ghorbani, the Canada Research Chair in Cybersecurity, is that academia has been slow to respond.

“We were not quick to recognize that cybersecurity should be a priority," says Mr. Ghorbani, who is also a computer-science professor at the University of New Brunswick.

It's become challenging to find qualified instructors to teach courses, as cybersecurity professionals are in high demand and can earn considerably more working in the private sector.

It's “almost too late" to fix the problem, says Nish Bhalla, CEO and founder of Security Compass.

“We should have done it back when the problem started. Right now, there's a war on for talent and everyone – both our customers, as well as ourselves – are losing it."

Mr. Bhalla believes that the solution lies in corporations partnering with colleges and universities to build educational programs – much like the Rogers Cybersecure Catalyst program being launched by Ryerson in February.

The accelerated 20-week program, which will be free for students, aims to have 640 industryready professionals graduate over five years. It will look to take many people who already have work experience and technology skills but whose roles have been made redundant because of technology/automation, and it will give special consideration to women and newcomers to Canada.

“Our purpose here is to move quickly to try to address part of this challenge," says the program's executive director, Charles Finlay.

Ryerson's program is not the only public-and-private partnership striving to remedy the talent shortage. Bell is currently completing plans for a new master's program in cybersecurity that will be offered at the University of New Brunswick in the fall.

The telecommunications company is offering to pay students' tuition fees and guarantee them a job upon graduation. It hopes 70 students will graduate within the first three years.

“When I was in university, if I could have had my tuition fees paid and a guaranteed job coming out, I would have thought that's a pretty sweet deal," says Marc Duchesne, vice-president of corporate security and responsibility at Bell.

Mr. Wilson, from EY, says it's also important that companies use automation to reduce the need for certain roles, and that they hire people outside of major cities and allow them to work remotely.

Retaining existing employees is equally critical. That means providing them with interesting and challenging problems to solve, RBC's Ms. Pezzente says.

“Cybersecurity professionals want to work on the latest and greatest, using cool techniques and new tools and that sort of thing," Ms. Pezzente says. “So if they find that you're in the dark ages and you're working on things that were worked on 15-20 years ago, that's not terribly interesting to them."

Another key to retention is managing burnout.

“The shortage has caused a huge burnout culture, in that people keep working and working and taking on too many projects," Ms. Staszczyszyn says.

She believes that the key to expanding the cybersecurity work force is to focus on diversity – that is, finding ways to lure women, LGBTQ individuals and other candidates from underrepresented groups in the industry.

Many creatively oriented people may not be aware of how rewarding a role in cybersecurity can be, Ms. Staszczyszyn says.

What she's discovered is that hacking is as much an art as it is a science.

“It's like a puzzle. … You have to constantly think outside the box."

Document GLOB000020190902ef920000n