Making Headway

Reporting on the Financial and Consumer Services Commission's Fullsail Capital Markets Initiative

SPECIAL EDITION

Cybersecurity in New Brunswick

FINANCIAL AND
CONSUMER SERVICES
COMMISSION

March 2018

Cybersecurity – not just a problem, but also an opportunity

A few years ago, I attended an Information Systems Audit and Control Association (ISACA) cybersecurity conference where Mike Rogers was the keynote speaker. Rogers, who at that time had just completed his term as the Chairman of the United States Permanent Select Committee on Intelligence, spoke about the increasing importance of cybersecurity in today's technology-driven business environment. He gave numerous examples of how cybersecurity risks were permeating previously untouched business infrastructure areas and impressed on the attendees the importance of adopting a broad holistic approach to cybersecurity-risk management. He concluded by saying that in today's world "managing cybersecurity risks is no longer a cost of doing business; it is now and will remain for the foreseeable future, a cost of *staying* in business." A few years later, these words continue to ring true. There is not a week that we do not hear about some new breach or new threat. There is little doubt that we all need to take cybersecurity seriously.

But it is not all bad news. We are getting better at managing cybersecurity risks through the adoption of best practices standards, frameworks and new tools. Here in New Brunswick, we are moving the needle on cybersecurity by supporting and encouraging projects that hold promise in helping businesses better manage cybersecurity risks. There are real opportunities for researchers and entrepreneurs to provide new and innovative solutions not just to big business, but also small and medium enterprises, which appear to be a growing target for cybercriminals.

Our government and academic institutions are on the same page in looking to make New Brunswick a centre of excellence for cybersecurity innovation. This issue of *Making Headway* hopes to play a small part in supporting that effort.

JAKE VAN DER LAAN

Jake is the Chief Information Officer and Director of Enforcement at the Financial and Consumer Services Commission. Since 2015, he has overseen the development and execution of the Commission's holistic Cybersecurity Strategy and Plan, based on the National Institute of Standards and Technology Framework.

FCNB

WE WANT TO HEAR FROM YOU

Tell us what you'd like to read in the next edition of Making Headway. You can submit your story or send us an email telling us about something great that is happening in New Brunswick's capital markets.

FINANCIAL AND CONSUMER SERVICES COMMISSION
85 Charlotte Street, Suite 300
Saint John, NB
E2L 2J2

Toll Free: 1 866 933-2222
Email: info@fcnb.ca
Website: FCNB.ca

NEVER MISS AN UPDATE

Subscribe Online

Connect with us to stay up-to-date on what we're doing to foster New Brunswick's capital markets, as well as for updates on regulatory and enforcement matters, and our education and outreach programs.

FCNB.CA

@FCNB_

FCNB CA

FCNB.CA

FCNB.CA/subscribe

FEATURE

Highway Robbery on the Information Superhighway

In David Shipley's words, no one talked about highway robbery on the information superhighway, but unfortunately that is what's happening now.

"The internet was never designed to be secure, and in the cases of many technologies being developed today, cybersecurity is an afterthought," says the CEO of Beauceron Security Inc. "Despite these risks, many are still behaving as though better technology is the only solution to cybercrime. We're totally ignoring the human element."

A recent study from IBM concluded 95 per cent of successful cyberattacks are the result of human error – employees clicking on a link in a phishing email, for instance. These mistakes cost the victims dearly. A 2015 study by a British insurance company found that cybercrime costs businesses worldwide $400 billion a year.

The cultural problem standing in the way of cybersecure workplaces is what drives the effort at Beauceron. The business, now in its third year of operations, was named after the French sheepdog with the intention of replicating its behaviour and turning company employees into the protectors of the business' digital assets. This thinking is a radical shift in the way a company is usually protected, as most rely on their overworked team in the IT department.

"The internet was never designed to be secure."

Today, Beauceron offers cybersecurity training, online teaching, phishing simulations and a suite of other services with the aim of simplifying the learning curve and changing behaviours to reflect real business vulnerabilities.

Highway Robbery on the Information Superhighway – continued

David Shipley's Tips:

Three steps anyone can take to protect their devices from hackers

1. Get informed.

You don't have to be an expert, but you do need to pay attention. Ask yourself: What devices do I have in my household? Is my software up to date? (Fun fact – The Equifax breach was a result of the company neglecting to update its servers.) At the office, ask your IT manager if your computer is up-to-date. You can help spot problems.

2. Treat cybersafety just like physical safety.

It's easy to forget that something like a weak password can make you just as vulnerable as having a $100 bill hanging out of your pocket in a crowded place.

3. Report suspicious emails or other unusual activity to your IT team.

When you report that strange email, you protect others in your organization who might get the same message – all while helping the team better understand the attack.

Shipley's prediction for the future of cybersecurity? It's going to get worse before it gets better, particularly as it relates to what he calls a massive regulatory gap.

"The example I would use is the Titanic," he says. "It was the first major marine disaster to prompt the creation of stronger regulation for marine safety, including the required number of lifeboats aboard each ship.

"The *Digital Privacy Act* is going to need a similar upgrade," he continues. "Right now the maximum fine for a breach is $100,000, which is a blip on the radar compared to how much money hackers can steal."

What's more, the struggle to catch hackers in the act won't get any easier. In Canada, suspects are only ever identified in six per cent of police-reported cybercrimes.

> **"Right now the maximum fine for a breach is $100,000, which is a blip on the radar compared to how much money hackers can steal."**

Shipley stresses that not all hope is lost. Cybersecurity is in the hands of people who can take concrete steps to protect themselves and their workplaces.

"When individuals are given the right tools and education, empowered to understand their role in protecting an organization and encouraged to do so, they're energized by the idea of playing their part," Shipley says.

Protecting New Brunswick from the World Wild West

If you ask Dr. Ali Ghorbani what it takes to coordinate a strong cybersecurity effort in New Brunswick, it becomes clear he's given it a lot of thought.

"For cybersecurity efforts to work, you need all levels of government, academia and industry to work together," says the director of the Fredericton-based Canadian Institute for Cybersecurity (CIC). "Cybersecurity breaches impact us all, so it's crucial that we work together to prevent them."

Dr. Ghorbani's vision of a more cybersecure province took form in early 2007 with the creation of the Centre of Excellence in Cybersecurity on the Fredericton campus of the University of New Brunswick (UNB). "One aspect of cybersecurity that we realized needed to be addressed was its interdisciplinary nature," Ghorbani says. "It isn't just about computer science. It involves business, education, psychology, design – the list goes on."

In January 2017, UNB, the Atlantic Canada Opportunities Agency (ACOA) and the provincial government took it a step further with the creation of the CIC: a comprehensive multi-disciplinary training, research and development, and entrepreneurial unit that draws on the expertise of researchers in the social sciences, business, computer science, engineering, law and science.

The need to build a strong cybersecurity program is now a fact of life across all disciplines. Digital medical records are used to build health-care profiles; chemistry and life sciences store vast quantities of biomedical data; and the legal system generates an ever-increasing amount of sensitive information.

"Ultimately, it's people who are responsible for safeguarding the systems that contain vulnerable

World Wild West – continued

information," Ghorbani says. "It is crucial that we safeguard New Brunswick's critical infrastructure. For instance, if a breach managed to compromise our power grid, it would be very logistically and financially painful for us."

Making New Brunswick cybersafe comes with a unique set of challenges.

"The lack of awareness among New Brunswickers is our main challenge," Ghorbani says. "Many New Brunswickers do not have the fundamental knowledge of how to stay safe in cyberspace. To address this issue we in collaboration with CyberNB made a concerted effort to go into schools and provide workshops that shares this knowledge. I'm hopeful that we'll start providing this training to seniors as well."

So when asked how can we protect ourselves, Dr. Ghorbani stated the number one thing is to practice vigilance. "Don't be too trusting in cyberspace – it's still the Wild West," he says. "Be suspicious of things that are not known to you. Make sure your systems are up-to-date with the latest operating systems and patches."

Dr. Ghorbani notes the need to tread carefully will only become greater as the level of risk intensifies – particularly as artificial intelligence and automation become more prominent.

"We've just seen the tip of the iceberg with the Internet of Things," Ghorbani says. "Artificial intelligence and machine learning, helpful as they are, bring forth a whole new set of vulnerabilities that the bad guys can exploit."

> **"Don't be too trusting in cyberspace – it's still the Wild West. Be suspicious of things that are not known to you."**

It has become apparent that education plays a significant part in reducing cyberrisk. UNB Faculty of Computer Science just approved a one-year Master of Applied Cybersecurity program – this in addition to the undergraduate programs offered on campus.

"Education, education, education," Ghorbani concludes. "That's the way to fight cybercrime."

> **"Ultimately, it's people who are responsible for safeguarding the systems that contain vulnerable information. It is crucial that we safeguard New Brunswick's critical infrastructure."**

The **Internet of Things** refers to the concept of connecting any device with an on and off switch to the Internet (and/or to each other). This can include cellphones, coffee makers, washing machines, headphones, lamps, and wearable devices. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig.

FEATURE

Making New Brunswick a Cybersecurity Epicentre

As more lives are connected online, CyberNB is assuming a leadership role in Canada when it comes to cybersecurity.

"Imagine if New Brunswick experienced an attack and our Internet was shut down," says Allen Dillon, Vice President, CyberNB. "Everything from our gas pumps to our banking and our food supply, we rely on technology for all of it. So it's critical to ensure we have the safest system that we can."

Launched by the province in 2016, CyberNB is a special operating agency of Opportunities NB and focused on a five-pillar strategy to protect citizens and the economy from cybercrime.

According to Cybersecurity Ventures, the global cost of cybercrime will reach $6 trillion by 2021. At the same time, it predicts 3.5 million cybersecurity jobs will be unfilled by 2021.

"We were formed based on the realization that, as we become a more connected world, cybersecurity is part of everything we do," says Dillon. "Fundamental to protecting our citizens and our economy is having the right resources in place, whether that's policies for protecting our citizens and our critical infrastructure to creating the right opportunities for our labour force."

> "Imagine if New Brunswick experienced an attack and our Internet was shut down. Everything from our gas pumps to our banking and our food supply, we rely on technology for all of it."

Developed with input from industry, academia and government, the agency's five key strategies incorporate building the skills and workforce to deal with the growing need for cybersecurity professionals; protecting the province's critical infrastructure; supporting the development of new cybersecurity technologies; creating a world-class cybersecurity business park; and partnering with the Canadian Institute for Cybersecurity at UNB (See story ***Protecting New Brunswick from the World Wild West***).

"So it's a holistic and full approach through collaboration with industry, government and academia to making sure our economy and our citizens are protected with the right information and the right resources," Dillon says.

CYBERNB

A SPECIAL OPERATING AGENCY OF OPPORTUNITIES NB | UN ORGANISME DE SERVICE SPÉCIAL D'OPPORTUNITÉS NB

ONB Opportunities | OpportunitésNB

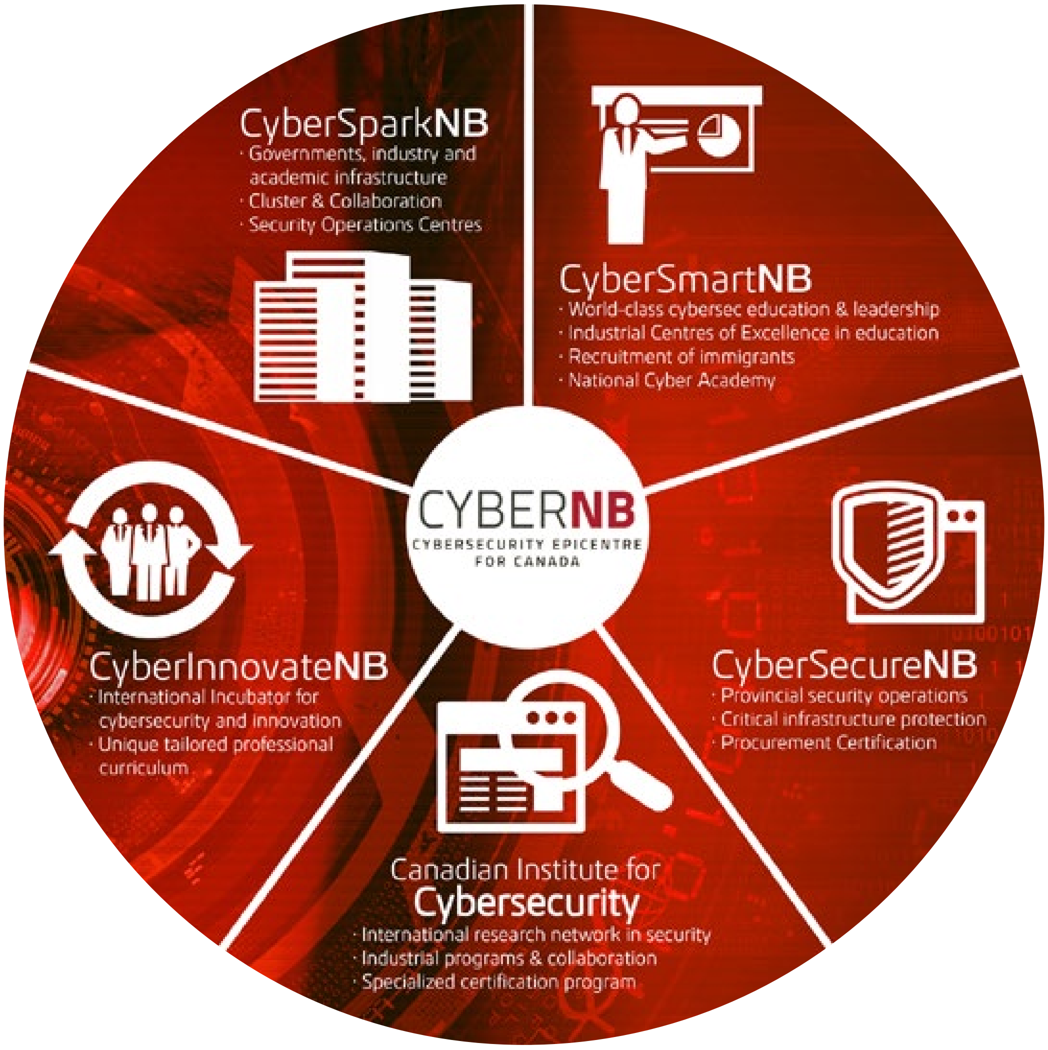
Cybersecurity Epicentre – continued

Since its launch, the agency introduced Cyber Essentials Canada, a cybersecurity standard and set of best practices that organizations can be assessed and certified against. Through collaboration with CyberNB, the New Brunswick Community College recently announced a one-year diploma program that will start in September at the Saint John campus. The program will focus on how to set up secure networks and learn to identify threats to the system.

In partnership with Blue Spurs, it also piloted an educational starter kit that includes both hardware and software to help elementary, middle and high school students understand the fundamentals of the Internet of Things (IoT). Now, it is working with the government to implement the kits in school curriculum across the province.

“We are a leader in many aspects of what we are doing,” he says. “We want to make New Brunswick an epicentre for cybersecurity in Canada.”

Learn more at cybernb.ca and check out its video[1].


CyberSparkNB
· Governments, industry and academic infrastructure
· Cluster & Collaboration
· Security Operations Centres
CyberSmartNB
· World-class cybersec education & leadership
· Industrial Centres of Excellence in education
· Recruitment of immigrants
· National Cyber Academy
CYBERNB
CYBERSECURITY EPICENTRE FOR CANADA
CyberInnovateNB
· International Incubator for cybersecurity and innovation
· Unique tailored professional curriculum
CyberSecureNB
· Provincial security operations
· Critical infrastructure protection
· Procurement Certification
Canadian Institute for Cybersecurity
· International research network in security
· Industrial programs & collaboration
· Specialized certification program

[1] https://youtu.be/hYRYlHLN5W8