City of Fredericton

• 600+ employees spread out at a variety of locations

• Centralized IT

• Several major IT programs and initiatives to enable digital transformation and security

• Public Safety key priority

• Start Up Community of the Year (2016)

Challenges

• Launching city-wide security awareness program for first time

• Building a process for reporting suspected phishes

• Need to gather meaningful insights and measures for new multi-year security roadmap

Key Decision Factors

• Highly **automated** deployment and management

• Insightful analytics and key **metrics** to benchmark program effectiveness

• Detailed dashboards and **automated reporting**

• Simplified **risk assessments**

• Canadian company (with **data hosted in Canada**)

• **Multiple authentication methods** for departments including support for single sign on (SSO)

• Ability to create **custom courses** and deploy within platform

Protecting the Smart City

Cities, towns and villages across North America are embracing digital technology to improve services to citizens, increase efficiency and reduce cost. At the same time, they face a growing global threat from criminals who seek to steal data and extort officials, causing financial losses and reputational damage. Dozens of municipal entities – from large cities, to small towns – have been the victims of international cybercrime in the past two years.

Teams of sophisticated and dedicated criminals have launched a virtual crime wave that has locked access to financial payment systems for transit and utility services, crippled municipal emergency services, and stolen citizen information.

Municipalities under threat

Cyber criminals, hactivists and thrill seekers have been causing havoc for dozens of cities and towns in Canada and the United States. There have been a steady stream of headlines about cyber attacks and cities in the past year. From the nearly week-long outage at the City of Atlanta that cost more than $10 million to clean-up and months to fully recover, to attacks on small towns that wiped out citizen and tax information in Alberta, Canada.

Launching the first city-wide cyber awareness program

The Innovation, Improvement and Technology Team at the City of Fredericton was acutely aware of the increasing number of attacks on municipalities yet still needed to find a way to pursue an ambitious agenda of digital transformation for the city.

The first priority was to improve the City's ability to educate and engage all of its employees about cybersecurity.

The team needed an easy-to-manage tool that would help them raise awareness and generate meaningful insights and metrics to help with on-going awareness program management. With Beauceron's unique personal cyber risk score, employees have been able to see the connection between their good security behaviours and keeping the organization safe.

Protecting those who Serve and Protect

Among the key objectives of the city's first campaign was to provide awareness and education to its 100+ member police service. After receiving a briefing from Beauceron on cyber risks and incidents involving police forces across North America, the police leadership team made completing the core awareness training mandatory, achieving 75% completion in the first 30 days and 100% completionwithin six months.

"We looked to several companies to help with cyber awareness training but there was nothing like the comprehensive program that Beauceron has available. The personalized risk score really caught everyone's attention by providing context. For IT managers it helps us to zero in on the high-risk individuals and high-risk groups and follow up with more focused interventions.

It's relatively hands-free to manage and the implementation was lightweight. We probably spent more time putting up the catchy posters in the lunch room than we did configuring our systems to be ready."

Adam Bell, Assistant Director
Finance, Innovation, and Technology
City of Fredericton
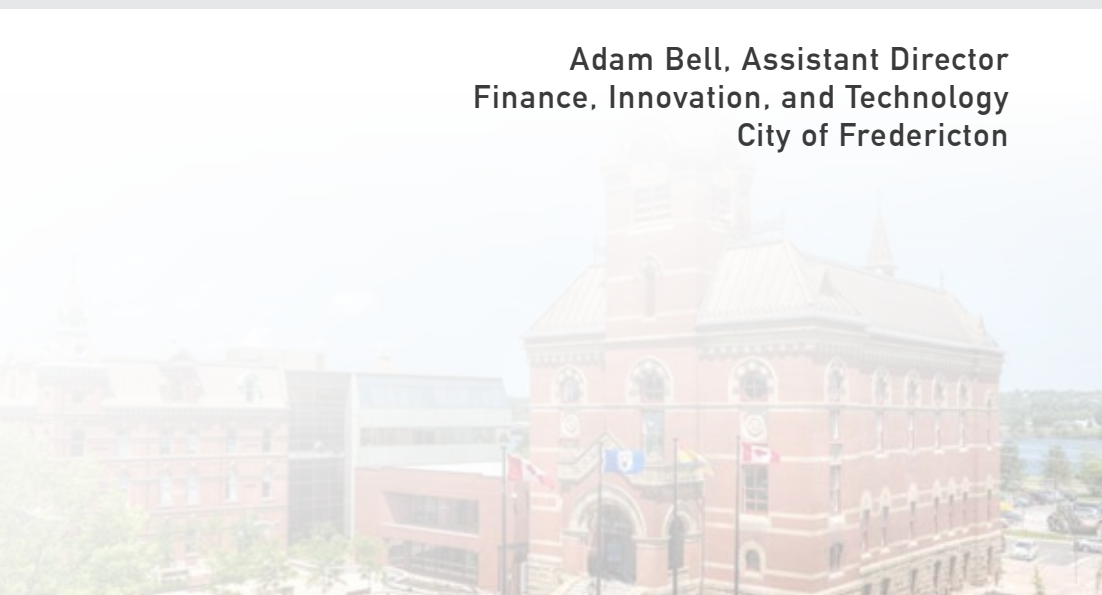
Key Features Deployed

• Individualized dashboard for employees highlighting their personal risk score, surveys, online education courses and learning management system, exposure report

• Custom Course Creation with Third-Party SCORM 1.2 support

• Automated phishing campaigns with auto-assigned remedial education

• Phishing reporting feature with automated reward messages for catching simulated phishes

• Risk Self Assessments with NIST Maturity and Technology Gap Reports as well as Risk Advisor Dashboard

• Incident Reporting Tool

Results

• Successfully delivered first citywide cybersecurity awareness program.

• Over 90% staff reported feeling they knew more about cybersecurity from this experience

• 100% of police force completed training in their mandatory program

• Benchmarking data and insights via the NIST CSF maturity report

• 3.25 phishes caught and reported by employees for every one clicked.