

How Bulletproof Helped the City of Saint John Overcome a Ransomware Attack

When a crippling ransomware attack hit the City of Saint John in 2020—amid the height of a global pandemic—the municipality refused to pay the ransom.

Instead, the City partnered with Bulletproof to rapidly rebuild systems and strengthen its cybersecurity posture.

Thanks to fast action, a tightly integrated team, and the power of Microsoft Security solutions, Saint John **restored critical services in just six weeks**—avoiding what could have been years of recovery.

THE CITY OF SAINT JOHN

Founded in 1785, Saint John, New Brunswick is Canada's oldest incorporated city with a population of 70,000.

The City of Saint John is a 15-person IT team that supports 900+ users across vital city services—from water to emergency response.

"After we understood that we were indeed attacked we had Bulletproof on site and ready to support us in containment. When Bulletproof came on site, it was like they were part of the team: instant connection, working with them side by side."

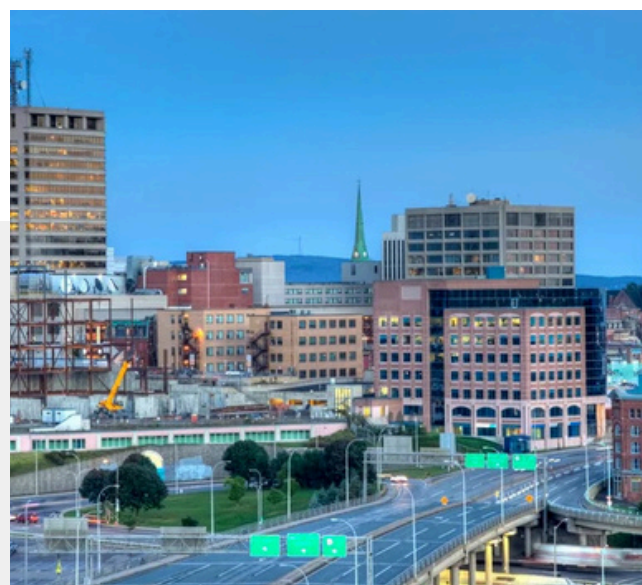
Stephanie Rackley-Roach
Chief Information Officer, City of Saint John



THE CHALLENGE: LIMITED RESOURCES, RISING THREATS

Despite proactively assessing its security posture and beginning to implement SIEM/SOC solutions with Bulletproof, the City of Saint John faced ongoing challenges. The IT team had plans to expand monitoring across more servers and endpoints, but—like many municipalities—struggled to get consistent budget approvals for cybersecurity.

In late 2020, those limitations were tested when the City was hit with a ransomware attack demanding \$12–14 million in Bitcoin. The attack struck late on a Friday night—forcing the IT team into immediate crisis mode.



JUMPING INTO ACTION

Upon arriving in Saint John, the Bulletproof team met with Rackley-Roach and her IT Team to be briefed on the crisis, develop a plan of action, and bring City leadership onboard.

While Rackley-Roach worked with the City's executive leadership team to enact emergency procurement procedures and ensure crucial resources and services could be revived without delay, the Bulletproof team jumped into action.

Thanks to an active incident response contract, Bulletproof was onsite before 9:00 AM the next morning.

“Any IT executive confronted with a ransomware incident must balance urgent containment actions and communications internally with outside demands, like dealing with media, insurance, and City Council.”

Chris Johnston, Former CEO, Bulletproof



ASSESSING THE DAMAGE

An immediate priority was determining the source of the breach. “That initial response is a very complicated operation with a lot of moving parts,” explains Bulletproof's former COO Jeff Shaw. “We had to deal with the complex technical issues of forensic analysis and sever partner connections in addition to the internet. For the CIO, it means navigating operational impact while also working with law enforcement, insurance, external counsel, partner organizations, and other stakeholders.” Bulletproof worked with the City's IT to develop a detailed path forward, laying out the recovery steps.

Working as a single integrated team, the City of Saint John's IT team and Bulletproof began to rebuild the City of Saint John operating environment, layering in security with the end-to-end Microsoft Security solutions stack. It deployed the Bulletproof 365 Enterprise system, which seamlessly merges Microsoft Sentinel with Microsoft 365 to deliver comprehensive intelligent security.

“We deployed Microsoft Sentinel to fix the ‘blind spot’ that happens with traditional log-based SIEMs,” explains Shaw. “The visibility and capability we get with Microsoft Sentinel far exceeds that of the previous SIEM.”

We brought the signal into our security operations center with Microsoft Sentinel for a real-time overview of the entire estate. It was critical to spot any threat that could delay reinstating the network and operating systems to fully restore IT functions.”

Implementing the Microsoft Security stack was already on the City of Saint John's roadmap, so the Bulletproof team was able to swiftly rollout Microsoft Defender for Endpoint to secure the City's servers and other endpoints, Microsoft 365 Defender, and Microsoft Defender for Cloud. “In this situation, where we needed ultimate confidence to ensure that everything brought back online was highly secure, the Microsoft Defender suite was critical,” says Johnston. “Defender for Endpoint is invaluable in alleviating the fear of residual malware in on-premises servers as systems come back online.”

THE RESULT: RAPID RECOVERY & LONG-TERM RESILIENCE

The City's goal: restore core IT operations in six weeks—a target most thought impossible. With long hours from both teams, the City was back online on schedule. Within 18 months, the full environment was rebuilt and modernized with stronger security and visibility.

"The silver lining of our ransomware attack is that I go home at night feeling good about the state of our network," she says.



"Now, we work from an assume-breached mentality. Thanks to Microsoft Sentinel, we know that this is the case.

The difference is that now we know that we can manage whatever happens through enhanced visibility and response capabilities."

Stephanie Rackley-Roach, CIO, City of Saint John



"Bulletproof was our primary partner for containment and restoration. The attack impacted nearly every system."

Stephanie Rackley-Roach
Chief Information Officer, City of Saint John

STAYING VIGILANT

Today, with Bulletproof 365 Enterprise and Microsoft Sentinel, the City benefits from 24/7 threat monitoring and intelligence, with monthly review sessions to stay ahead.; because after all, cybercrime never sleeps.

"We've all lived in a multi-vendor world with limited visibility into security," states Chris Johnson, Former Bulletproof CEO. "That was the best we could hope for until the Microsoft Security solution stack was available, giving us a way to protect customers. We protect our own business with it."

WHY BULLETPROOF

At Bulletproof, we help organizations solve complex challenges with confidence—whether it's strengthening cybersecurity, modernizing IT infrastructure, or driving more value from Microsoft technologies.

Backed by deep industry expertise, a people-first approach, and our trusted partnership with Microsoft, we deliver practical, scalable solutions that make a measurable impact.

From municipalities to enterprises, our clients choose Bulletproof for our commitment to excellence, our collaborative mindset, and our ability to turn goals into results.

