Municipal Insurance
Association of British Columbia

200 - 429 West 2nd Ave.
Vancouver, BC V5Y 1E3
Phone: 604-683-6266
Email: AskUsAnything@miabc.org

miabc.org

MUNICIPAL INSURANCE ASSOCIATION OF BRITISH COLUMBIA

Cyber Incidents Have Changed

Reflections from a Real Municipal Cyber Incident

This Is No Longer a "What If"

Cyber incidents are no longer rare, abstract, or limited to large organizations. They are operational events that can disrupt services, decision-making, and community trust—often without warning. Most incidents do not begin dramatically. They start quietly, through everyday gaps that do not appear urgent on their own.

What the Fort St. John Incident Reinforces

Cyber incidents unfold quickly, often within hours. Attackers do not need sophisticated tools—one weak entry point is enough. Encryption is only part of the problem; data theft adds pressure, complexity, and reputational risk. Even well managed organizations can be affected. While technical details matter, the organizational response matters more.

Cyber Risk Is Not Just an IT Issue

A cyber incident affects leadership, operations, communications, legal and insurance considerations, staff, and public confidence. Cyber readiness is about governance, clarity, and preparedness—not just technology. The most important question is not "Could this happen to us?" but "How ready would we be if it did?"

Small Gaps Add Up

Many incidents begin with a phishing email, a reused password, a delayed system update, or a security exception that quietly became permanent. Individually, these issues do not feel urgent. Together, they create opportunity. Strong fundamentals reduce risk far more effectively than complex or expensive solutions.

Time Matters—Especially at the Start

Early detection and fast response can limit operational disruption, reduce data exposure, shorten recovery time, and ease pressure on staff and leadership. Knowing who to call, how to escalate, and what authority exists before an incident occurs makes a measurable difference.

Cyber Insurance Is a Response Tool

Cyber insurance is not just about reimbursement. It provides access to coordinated incident response, technical investigation, legal and communications support, and structure during a chaotic event. Insurance is most effective when it is understood before it is needed.

Readiness Is Ongoing—Not OneTime

Cyber readiness is a cycle: prepare, reduce risk, detect early, respond, and recover. No organization eliminates risk entirely, but resilient organizations recover faster and with fewer impacts. MIABC provides risk support and guidance for local governments, while coordinated cyber-insurance response resources—whether through the Victor Cyber Program or another insurer—play a critical role in helping organizations move through this cycle with greater confidence and less uncertainty.

A Moment to Reflect

If something suspicious happened tomorrow, would everyone know what to do next? That clarity—more than technology—is what builds resilience.