RISK
INSIGHTS

RANSOMWARE– CURRENT LANDSCAPE

Multi-extortion threats to Canadian businesses

Ransomware remains the most common cyber threat facing Canadian organizations, and attackers now use multi-extortion tactics—encrypting data, stealing sensitive information, and threatening leaks or regulatory reporting to maximize pressure. This overview highlights current trends and practical steps organizations can take to better prepare for and respond to these attacks.

Northbridge® Insurance

MULTI-EXTORTION IS NOW THE NORM

Ransomware tactics have changed. Today, attackers may not only disrupt systems but also copy sensitive data and use the threat of disclosure or regulatory scrutiny to apply pressure. The Canadian Centre for Cyber Security (CCCS) calls ransomware the **most common cyber threat Canadians face**, and it continues to rise in frequency and impact.

Why this matters

Even with strong backup strategies, organizations can still be vulnerable to data theft and potential leak scenarios, which may lead to regulatory notifications, privacy-related expenses, reputational impacts, as well as unexpected operational downtime.

The CCCS reports that the number of ransomware incidents they track has increased, on average, by **26%** every year since 2021, reinforcing that ransomware is continuing to grow and evolve in Canada. (1)

Why Canadian organizations are being impacted

- Ransomware incidents today often involve the supply chain. In many cases, attackers gain access through a trusted vendor rather than directly targeting the organization. This means an organization's overall risk is influenced not only by its own controls, but also by those of its partners.
- Cross-sector disruption: Transportation & logistics, healthcare (clinics, long-term care, ancillary providers), technology companies, utilities, and manufacturers have all faced operational shutdowns and costly recovery in recent years. The CCCS assesses ransomware against Canada will **continue to target enterprises and critical infrastructure of all sizes**.
- Preparedness gap in small business: **47%** of small businesses are more concerned about ransomware than pre-pandemic, but only **24%** say they have cyber insurance—indicating under-preparedness for adverse events. (2)
- True costs are under-reported: The CCCS assesses that a majority of ransomware attacks against Canadian victims may be unreported to authorities, which means the public view of incident volume and costs is likely lower than reality. (3)

WHAT TYPICALLY BREAKS (WHERE DEFENSES FAIL)

Initial access: Attackers often gain their first foothold through phishing emails, stolen or reused login credentials, or by exploiting external systems that haven't been patched—such as when an employee clicks a convincing email or a publicly exposed service is left vulnerable.

Spreading inside: Many organizations focus on protecting their network perimeter and assume internal systems are safe. But if attackers breach those defenses, they can move through the internal network—especially when user accounts have more access than they need and systems aren't properly separated—allowing a single incident to quickly escalate into a much larger compromise.

Backup compromise: If attackers can access backups on the same network, they will often target and disable or encrypt them first—turning a recoverable incident into a much more serious disruption.

Exfiltration & extortion: Attackers often steal and extort data by staging it on high-privilege systems, such as administrative workstations, and exploiting gaps in endpoint detection and response (EDR) and weak data loss prevention (DLP) controls—allowing sensitive information to leave the organization undetected.

CONSIDER THIS

If a set of your customer data appeared online tomorrow, how would you explain it to customers and regulators? What steps would you have to take to remove it? Would you need to notify your customers?

PRACTICAL STEPS

The following advice can help you prioritize what security controls you should work on first.

Access controls

- **Strong authentication (MFA):** Enable multi-factor authentication for email, remote access (VPN), and all privileged or high-access accounts. While no control is foolproof, MFA significantly reduces the risk of attackers gaining access using stolen credentials.
- **Least-privilege access:** Provide employees and third party users with only the access required to perform their jobs. Limiting the number of high-access accounts reduces how far attackers can move within your systems if a breach occurs.

Resilience

- **Backups you can rely on:** Maintain multiple backup copies across environments—including read-only or write-protected backups and offline replicas—to support both redundancy and recoverability. Often called *immutable backups*, these copies cannot be altered or deleted by attackers or accidental actions, while regular testing of redundant copies helps ensure fast, reliable recovery after an incident.
- **Identify your critical suppliers:** Secure at least one backup for each, and keep a simple shared record (lead times, pricing, ordering authority) to reduce disruption risk without complex tools or big budgets.
- **Patch internet-facing systems quickly:** Many cyberattacks begin by exploiting known vulnerabilities in systems exposed to the internet. Prioritize applying security updates to these systems as soon as fixes become available.

Human factors

- **Employees as the first line of defense:** Many ransomware attacks begin with a convincing phishing email. Short, regular awareness training and periodic phishing simulations can help employees recognize suspicious messages and track improvement over time. Attackers increasingly use AI to create more realistic phishing emails at scale, making vigilance even more important.

Response capabilities

- **Plan and test your response:** Develop a clear incident response plan outlining roles and responsibilities in the first hours of an attack. Regularly run a simple "*what if ransomware hit today?*" exercise, also called tabletop exercise, with IT, privacy/legal, and communications teams to ensure everyone understands their role and can respond quickly and effectively.

Simple ways to gauge readiness

- **Backup recovery:** Have you successfully restored a critical system from a secure backup within the last 90 days?
- **MFA coverage:** Is multi-factor authentication enabled for email, remote access, and privileged accounts?
- **Patch speed:** How quickly are critical, internet-facing vulnerabilities identified and fixed?
- **Incident preparedness:** If you don't have an incident response plan, now is a great time to build one. If you have one, have you run a tabletop exercise on this plan?

CONSIDER THIS

If email and file shares were down for 3 days, which teams are most critical—and what's your manual workaround?

NORTHBRIDGE INSURANCE CYBER COVERAGE

Your safety net

Even strong controls cannot eliminate risk entirely—which is where risk transfer plays a safety net role. Northbridge offers **comprehensive cyber coverage** (first and third-party; optional cyber-crime) and **Cyber Assist services** (vulnerability scan, self-assessment, incident simulation for eligible customers) to support risk management programs.

For more information on making your business safer, contact our Risk Services team at **1.833.692.4111** or visit us at **www.northbridgeinsurance.ca**.

[1] Ransomware Threat Outlook 2025-2027, Canadian Centre For Cybersecurity, 2025.
[2] Léger Small Business Cyber Security Survey for Insurance Bureau of Canada, 2021.
[3] Ransomware Playbook, Canadian Centre for Cybersecurity, 2026. [5066-001-ed04E | 05.2026]