Cyber claims in Canada: A race to respond

In Canada's cyber environment, the first hours of a claim often shape the outcome

Crawford®

$6.98M

AVERAGE DATA BREACH COST IN CANADA IN 2025.

IBM

86.5%

OF THE TOTAL CANADIAN ORGANIZATION LANDSCAPE EXPERIENCED A CYBER INCIDENT IN 2024

CDW CANADA'S 2025 CANADIAN CYBERSECURITY STUDY

Cyber claims in Canada at a glance

Cyber risk is now part of day to day business in Canada. Recent data shows that 73% of Canadian small businesses have already experienced a cybersecurity incident.

Phishing leads the list at 61%, followed by ransomware at 12%. Even with that level of exposure, only 47% of Canadian small medium enterprises (SME) say they are prepared for a cyber attack or data breach. Insurance uptake is still limited. Just 22% carry cyber insurance, and only 12% have a dedicated stand alone policy.

The pressure is building in places that are harder to manage. 72% of Canadian SMEs say AI and new technology are making cyber risk harder to handle, yet only 45% say they have policies and training in place to help staff spot AI generated scams. On the claims side, 60% of 2024 cyber claims came from business email compromise and funds transfer fraud incidents, with 29% of BEC events escalating into fraudulent transfer.

Severity still turns on interruption. At SMEs, claims with a business interruption component are more than 650% more expensive than claims without one. Most of those BI losses are tied to ransomware. Third party dependency is also carrying more weight. In 2024, 32% of the breach matters supported by Experian involved third or fourth party exposure. Even where response plans exist, execution is uneven. 96% of organizations say they have a cyber response plan, yet 71% still experienced at least one incident that stopped critical business functions.

That is the current market. Canadian businesses are exposed, many are underprepared, and losses widen quickly once operations are affected.

A market that moves fast

Cyber claims move quickly because the facts move quickly. Logs get overwritten. Systems are restored before anyone preserves the right evidence. Payment instructions are acted on before the fraud path is clear. Privacy timelines begin running from discovery, not from first notice to the insurer.

Canada adds its own complexity. Privacy obligations sit across federal and provincial regimes. Many insureds rely on US based vendors, cloud platforms, and outsourced service providers. Shared technology creates concentration risk. One provider failure can affect multiple insureds at once.

That is why these files benefit from structure early. Someone needs to keep the response moving, make sure the right specialists are engaged, and keep the facts from getting lost in the noise. When that happens early, the file tends to stay narrower and easier to manage.

The claims driving the market

The current claims picture still turns on two themes, fraud and extortion.

Business email compromise, funds transfer fraud, and ransomware continue to drive a large share of both claim count and claim spend. The difference now is how these losses develop. They pull in identity controls, communications channels, shared vendors, customer disruption, and regulatory pressure much earlier in the life of the claim.

A file may start with a mailbox compromise, a weak remote access point, or a vendor issue, then turn into an interruption problem, a privacy review, and a coverage discussion within days. Once that happens, the cost curve usually moves quickly.

> “Cyber claims develop incredibly fast, and the early response has to match that pace to contain loss, preserve evidence, and protect recovery opportunities. Decisive action at the outset is what keeps the loss controlled rather than compounded.”
>
> Brendan Leon, cyber specialist

> In cyber claims, the loss rarely stops at the point of intrusion. What drives the outcome is how quickly the response turns chaos into structure."
>
> Mike de Maria, claims adjuster, Global Technical Services

Business email compromise

Business email compromise remains one of the most common cyber losses affecting Canadian businesses. The pattern is familiar. An attacker gets into an email account or convincingly imitates one, inserts a payment request into a real conversation, and leans on urgency and familiarity to get the money moving.

What has changed is the reliability of the signals people use to decide whether something is real. Voice, video, caller ID, and writing style all carry less weight than they once did. Deepfakes and AI enabled impersonation have pushed that even further. Help desks and service desks have become attractive targets because they sit close to identity, passwords, and device enrollment.

That changes what matters early in the file. The useful questions go beyond whether the email was fake. How were payment changes verified? Who approved the transfer? Was a second channel used? Had the mailbox already been compromised? Were any identity controls bypassed in the days leading up to the loss?

Recovery remains difficult once the funds are gone. Speed still matters. So does knowing what to secure immediately, including the wire details, bank notifications, account access history, and the internal approval trail.

Ransomware

Ransomware remains the most disruptive cyber loss for many insureds because it puts pressure on operations, legal review, communications, and leadership all at once.

In Canadian claims data, ransomware remains the leading cause of loss. The model has also changed. Encryption is still common, though more events now include data theft, extortion, or threats of public disclosure. That shift changes what drives severity. In many files, the biggest issue is not the ransom demand. It is the interruption period, the scope of data review, the customer fallout, and the time it takes to restore operations.

The route in is rarely surprising. Weak remote access controls, poor identity hygiene, vulnerable public facing systems, and help desk manipulation continue to appear in serious files. Once inside, threat actors move quickly. They disable tools, expand access, and go straight to the systems that will create the most pressure.

Shared platforms raise the stakes. A vendor or managed service provider compromise can create the same operational consequences as a direct attack on the insured's own environment while affecting several policyholders at once.

Recovery capability remains one of the clearest dividing lines between manageable files and expensive ones. Some organizations restore critical operations within days. Others remain unstable for weeks because dependencies, credentials, infrastructure, and communications were never fully planned.

Why these files get complicated quickly

Canada adds complexity early. Privacy obligations are spread across federal and provincial laws, and one incident can trigger more than one notification path. Many insureds also depend on US based vendors, cloud providers, and service partners, which can complicate evidence handling, legal coordination, and the practical flow of the response.

Third party concentration now plays a bigger role in claims severity. Many organizations rely on a small number of core providers for cloud infrastructure, communications, payments, and managed IT. When one of those providers fails or is compromised, the problem reaches farther and lasts longer.

Data governance also matters more than many insureds realize. Excessive retention widens the review, prolongs legal work, and increases response spending. Poor data discipline changes the economics of the file.

Late notice remains a recurring challenge. Some insureds start remediation before anyone has preserved logs, isolated the right systems, or sorted through who did what. That makes the technical story harder to reconstruct and narrows the path for recovery later.

> For every insurer writing cyber risk in Canada, the speed and quality of the claims response is what the policy ultimately delivers."
>
> Brendan Leon, cyber specialist

Where severity builds

The largest cyber losses are usually built through interruption. Once operations are affected, the file changes shape. Revenue is touched. Staff time is diverted. Customers leave. Suppliers wait. Leadership attention shifts out of normal business activity and into crisis management.

Contingent business interruption now matters as much as direct interruption in many files. A cloud provider outage, SaaS failure, payment processor incident, or managed service provider compromise can produce the same commercial damage as a direct attack on the insured's own systems.

That is why BI and contingent BI function as claim multipliers. They expand what might have been a contained technical incident into a broader operational loss.

The relationship between interruption and extortion is practical. The decision around a ransom often sits beside the question of how long the business can stay impaired. That decision depends on the quality of backups, the pace of restoration, the credibility of the threat actor, and how quickly the response lines up with the commercial reality of the loss.

What changes the outcome

Serious cyber claims attract a crowd quickly. Forensics, counsel, communications, internal IT, leadership, banks, and vendors all arrive, or are about to. That kind of response needs shape early.

The files that settle into a manageable rhythm usually have a few things in common. The facts are gathered quickly. The response stays organized. The work being done stays tied to the actual loss.

Preparation plays a large role here. Pre-established response vendors matter. Clear internal authority matters. Out of band communications matter. Practical tabletop work matters. The strongest files usually come from organizations that had already worked through who decides what, how communications continue if core systems are unavailable, and which outside partners can actually respond when called.

The same is true for cost control. The first 24 to 48 hours influence the size of the notification review, the quality of the forensic findings, the pace of restoration, and whether recovery opportunities are preserved. Good files tend to have one thing in common. The process stays tight.

Coverage and market realities

Coverage issues often surface early in cyber files, especially where control representations, application answers, or operational reality do not line up neatly. Those issues matter, and they need to be handled carefully. The main point is simple. Early visibility helps. It gives the insurer a clearer view of how the file is developing and where the real pressure points are likely to sit.

The market is shifting as well. Cyber insurance is influencing baseline resilience more directly than it used to. Underwriting expectations around MFA, endpoint controls, and tested response planning are setting practical standards across the market. At the same time, a meaningful share of cyber loss still sits outside indemnity, especially where interruption is prolonged, governance is weak, or operational change continues after the immediate response is over.

Claim response study

► ADJUSTER ACTION ♦ DECISION POINT ⚑ COVERAGE CONCERN

HOUR 0 DISCOVERY	HOURS 1-12 CONTAINMENT	DAYS 1-2 COMPILATION	DAYS 3-7 NEGOTIATION & RECOVERY	WEEK 2+ RESOLUTION
► 6PM Friday - loss reported. Immediate triage. Systems down; potential data exposure identified.	► DFIR and breach counsel engaged immediately. Privilege established on first call.	► Backups encrypted and not isolated. Restoration not viable. Ransom negotiator engaged.	♦ Ransom path confirmed with insurer and counsel. Sanctions reviewed; negotiations advance.	► Forensic work concludes. Root cause confirmed. Operations restored.
► Vendor response requirements defined on first call.	► Hourly insurer updates begin. Policy reviewed for initial coverage position.	⚑ Backup controls inconsistent with application. Potential misrepresentation identified.	♦ Forensics vs restoration managed. Evidence preserved before system rebuild.	⚑ Misrepresentation confirmed post-forensics. Coverage position finalized.
	♦ Regulatory notification obligations and timelines assessed.	♦ Critical path letter issued within 48 hours. Rights reserved as response continues.	► BI impact assessed. Reserves updated as scope expands.	► BI period quantified and closed. Subrogation potential assessed.

Closing

Cyber claims in Canada are getting more layered, more operational, and more dependent on what happens in the first days of the response.

The files that go well usually have a few things in common. The facts are gathered early, the response stays organized, the right specialists are in place, and the commercial reality of the loss stays visible throughout.

That is where outcomes are shaped. It affects containment, downtime, evidence quality, reserve stability, recovery options, and the path to resolution. It also affects what happens after the file closes, including regulatory follow through, recovery efforts, and the insured's ability to steady itself for the next event.

Cyber exposure will keep growing, and the claims will keep getting more layered. The files that are handled well will keep standing out for the same reason. The response stayed focused, the facts stayed clear, and the loss was managed before it had the chance to spread.

The statistics cited in this report are drawn from third party industry and government sources and reflect published estimates available at the time of writing. Figures may vary based on incident type, organization size, reporting methodology and scope.

For further discussion on cyber response strategies, visit crawco.ca.

About Crawford & Company®

For over 80 years, Crawford has led the industry through a relentless focus on people and the innovative tools that empower them.

10K employees | **50K** field resources | **70** countries | **$18B** claims managed annually

Crawford®

Learn more at
www.crawco.ca

CRAW-CYBER-CANADA-0426