Ransomware Recovery Playbook for Canadian SMBs

A practical reference for Canadian SMBs (10-150 employees).

By Mike Pearlstein, CISSP
Founder & CEO, Fusion Computing | CISSP-led, founded 2012
Named in Canada's 50 Best Managed IT Companies 2024 & 2025
Published 2026-05-19

fusioncomputing.ca | contact@fusioncomputing.ca | (416) 566-2845
100 King St W, Suite 5700, Toronto, ON M5X 1C7

Ransomware Recovery Playbook for Canadian SMBs

A 12-page operating playbook from a CISSP-led MSP that has actually run a Friday-to-Monday ransomware recovery.

By Mike Pearlstein, CISSP -- Founder & CEO, Fusion Computing Date: 2026-05-19 Toronto . Hamilton . Greater Toronto Area . Metro Vancouver

Named in Canada's 50 Best Managed IT Companies 2024 & 2025. CISSP-led incident response. Founded 2012.

Cover note

This playbook is built from a real Fusion Computing engagement. A 45-employee Canadian industrial supplier was hit with ransomware on a Friday evening. By Monday morning, every employee walked back to a working desk. Zero ransom paid. Zero data lost.

The reason that outcome was possible is the same reason most ransomware recoveries fail -- the difference between Monday morning and three weeks of downtime is not a tool, a vendor, or luck. It is the playbook the IT partner runs in the first sixty minutes, and the readiness work done in the ninety days before.

This document is the playbook. Twelve pages, five phases, ten pre-incident questions, three case-study sidebars, and the pitfalls that turn a recoverable incident into a six-figure event. Use it as a board memo, a tabletop exercise prompt, or a benchmark to ask your current IT provider the right questions.

It is not legal advice. It is not a substitute for the Office of the Privacy Commissioner's PIPEDA materials, your cyber-insurance carrier's policy wording, or qualified incident-response counsel during an active event. It is the operational pattern Fusion's CISSP-led team uses when the call comes in.

Page 2 -- When ransomware lands at 4 PM on a Friday

The call comes in at 4:47 PM on a Friday in late March. A 45-employee industrial supplier in Mississauga has just lost every workstation, file share, and server to a ransom note. The CEO has been off the phone with her bank for ninety seconds. The finance team is staring at the same encrypted screen. Payroll runs Monday at 9 AM and the ERP system that prints the customer shipping labels is unreachable.

What the CEO does not yet know is that her endpoint-detection system has already isolated two devices, the lateral-movement attempt was contained at six o'clock, and the scope is bounded to local drives -- not the servers. She does not know it because nobody has had time to tell her. She just knows the screens are red.

Within forty minutes, a Fusion on-call engineer has the affected segment cut from the network, the two compromised credentials disabled, and the attack perimeter mapped. Saturday is spent confirming the initial access path -- a phished credential into an administrative account -- and validating the immutable offsite backup checksums. Sunday is rebuild: identity tenant first, then endpoints, then the file shares, then the line-of-business application. Sunday night the finance team validates the ERP from home. Monday at 8 AM everyone walks in, sits down, and works.

That outcome was not magic. Fusion's pre-engagement cybersecurity assessment had already flagged the recovery posture as weak. Backups were inconsistent. Restore testing was weak. The runbook was an idea, not a document. The client had three months of remediation work between the assessment and the incident.

Without that remediation, the call on Friday becomes a call to the cyber-insurance carrier on Monday about a six-figure ransom payment.

The difference between Monday morning and weeks of downtime is the playbook the IT partner runs.

Page 3 -- The 5-phase recovery model

Every recoverable ransomware incident follows the same five phases. Skip a phase and the next phase fails. Compress a phase to save time and a hidden re-infection vector survives into rebuild. Sequence matters.

Phase 1 -- Contain (first 4 hours)

Stop the spread. Isolate the affected segment, disable the compromised credentials, snapshot the forensic state before anything is unplugged, and notify the cyber-insurance carrier. The goal is not yet to rebuild. The goal is to prevent the blast radius from doubling while the rest of the playbook runs.

Phase 2 -- Triage (hours 4 to 12)

Scope it. What was encrypted, what was exfiltrated, what is backed up, what is not, and what was the initial access vector. Build the decision tree on rebuild-versus-decrypt with cyber-insurance counsel in the room before any restore actions are taken.

Phase 3 -- Restore (hours 12 to 72)

Rebuild clean, in order: identity tenant first (Microsoft 365 / Entra ID), then endpoints from gold image, then file data from validated backups, then applications. Validate each layer before bringing the next one online. Return-to-service criteria documented before users get credentials back.

Phase 4 -- Harden (week 1 to 2)

The week after the lights come back on is the only window in the year when partners and finance will sign off on every control that was deferred. MFA enforcement, conditional access, EDR everywhere, immutable backups, privileged access management. The remediation list from the post-incident review is the prioritized work plan.

Phase 5 -- Report (week 2 to 4)

The cyber-insurance carrier evidence package. The board memo. The PIPEDA breach-of-security-safeguards notification decision. The customer communication. The lessons-learned document. The next tabletop exercise scheduled. A ransomware incident that ends at Phase 4 with no formal report is an incident that will repeat.

The next five pages walk each phase line by line. Each phase has a *what to do*, a *what not to do*, and a *what to document*.

Page 4 -- Phase 1: Contain (first 4 hours)

The first four hours decide whether the incident is bounded or unbounded. Almost every catastrophic ransomware case Fusion has seen in the wild had a containment failure in the first ninety minutes -- not a backup failure later.

What to do

Isolate the affected segment, do not pull the plug. Network-level isolation through the firewall or switch port preserves the running state of the compromised host. Pulling the power cable destroys the memory image a forensic investigator will need to identify the strain, the initial access vector, and any exfiltration channel still open.

Disable the compromised credentials, do not delete them. Suspend the user account, force-revoke active tokens at the identity provider (Microsoft 365 / Entra ID), and rotate the password. Do not delete the account -- the audit trail of what the credential did is the evidence package for cyber insurance and for the OPC notification calculus.

Snapshot the forensic state. Capture memory images, disk images, and the EDR event timeline before any reboot, reimage, or shutdown. If your EDR is connected, the timeline is already captured server-side. If it is not, the snapshot is a one-shot operation.

Notify the cyber-insurance carrier. Most carriers require notification within 24 to 72 hours and many will void coverage on actions taken without their panel counsel's awareness. Notification is a phone call to the carrier's incident hotline, not a portal submission. Fusion treats this call as a Phase 1 step, not a Phase 5 step.

Identify the initial access vector. Was it a phished credential, an unpatched VPN appliance, an exposed RDP endpoint, an MSP supply-chain compromise, or a compromised remote-management tool? The initial access vector determines whether other tenants, other endpoints, or other credentials are also at risk.

Stand up the incident bridge. A 24/7 conference bridge with the CEO, the IT lead, Fusion's CISSP on-call, the cyber-insurance carrier's panel counsel, and (where applicable) external forensic counsel. Decisions are logged. The bridge does not close until Phase 3 is complete.

What not to do

Do not communicate over the compromised email tenant -- assume the attacker is reading. Do not pay the ransom in the first four hours under any circumstance -- the rebuild path has not yet been ruled out. Do not announce externally until Phase 2 has confirmed scope.

What to document

Time of detection. Time of containment. Affected endpoints, credentials, segments. Insurance carrier ticket number. Counsel contact name. Decision log. This document becomes the spine of the Phase 5 report.

Page 5 -- Phase 2: Triage (hours 4 to 12)

Once the bleeding has stopped, Phase 2 is the diagnostic sprint. The team that confused Phase 1 and Phase 2 is the team that started rebuilding from a backup that turned out to be infected.

What to do

Map the blast radius. Every endpoint, every server, every cloud tenant, every SaaS application, every backup target. The map is a spreadsheet with five columns: asset, status (clean / encrypted / exfiltrated / unknown), backup availability (immutable / online / none), criticality (tier 1 / 2 / 3), and rebuild owner.

Identify what was exfiltrated, not just what was encrypted. Modern ransomware is double-extortion. Encryption is the leverage. Exfiltration is the threat. Pull the firewall logs, the egress logs, the EDR network telemetry, and the cloud-tenant audit logs covering the seventy-two hours before detection. The exfiltration

finding drives the PIPEDA breach-of-security-safeguards calculus in Phase 5 and the cyber-insurance reserve in Phase 1.

Validate the backup chain before you trust it. Three checks, in order. First, are the backups immutable (cannot be modified or deleted by the production credentials)? Second, when was the last successful restore test, and was it a full restore or a file-level restore? Third, mount the backup in an isolated forensic environment and scan it with current EDR signatures before any production restore. A backup that has been quietly encrypting since week two is a worse outcome than no backup at all.

Build the rebuild-versus-decrypt decision tree. With panel counsel in the room. The decision factors are: backup integrity (proven good or unverified), exfiltration confirmed (yes / no), decryptor availability for the strain (yes / no), business recovery timeline (hours / days / weeks), regulatory exposure (PIPEDA / Law 25 / sector-specific), and insurance position. The decision is logged. The decision is signed.

Set the return-to-service criteria. Before any restore action runs, write down what "back online" means. Endpoints rejoin the domain after a clean image. File shares are accessible after data validation. Email flows after tenant rebuild. The line-of-business application is functional after database integrity check. No user gets credentials back until their endpoint is on the post-incident gold image.

What not to do

Do not start restoring before you know the initial access vector -- you will restore the back door. Do not negotiate with the threat actor without panel counsel approving the channel. Do not promise the board a timeline before Phase 2 is complete.

What to document

Blast-radius spreadsheet. Backup validation log. Decision tree with signatures. Return-to-service criteria. Exfiltration finding.

Page 6 -- Phase 3: Restore (hours 12 to 72)

The rebuild is methodical, sequenced, and validated layer by layer. Speed comes from sequencing, not from skipping.

Clean-rebuild order

1. Identity first. Microsoft 365 / Entra ID is rebuilt before anything else. Reset every administrative credential. Revoke every active token. Rotate every service-account secret. Re-enrol MFA from a clean device. Audit every consent grant for OAuth applications added in the past ninety days -- attackers commonly persist via OAuth app consent, not just credentials. Identity is the trust anchor for every later step.

2. Endpoints second. Every affected endpoint is reimaged from a gold image -- not "cleaned." Reimaging is faster, more reliable, and forensically defensible. The gold image includes the post-incident EDR agent, the new conditional-access policy, and the hardened local-admin configuration. Endpoints rejoin the domain after the image is validated.

3. Data third. File shares, SharePoint libraries, OneDrive, and the application database are restored from the validated immutable backup. Each restored share is mounted read-only and scanned with current EDR signatures before users get write access. If the data is restored from a backup older than the access-vector date, validate file-level integrity for the affected window.

4. Applications fourth. The line-of-business application (ERP, practice management, CRM, EHR) is restored last because it depends on the previous three layers. Application restore includes database integrity check, integration token rotation, and a functional smoke test before users get access.

Validate each layer before the next

Identity is validated by attempting an administrative sign-in on a known-clean device with MFA. Endpoints are validated by EDR baseline scan and a network-policy check. Data is validated by checksum against pre-incident backups and by current-signature scan. Applications are validated by smoke test of the three highest-volume daily transactions.

Return-to-service criteria

Endpoints rejoin only after gold-image deployment. Users get credentials back only after the endpoint is verified. External-facing services come back last, behind the new web application firewall ruleset. The criteria are checked off in the incident bridge before each layer goes live.

What to document

Restore-by-restore log with timestamps. Validation result per layer. Backup mount-and-scan log. EDR baseline scan results. Application smoke-test pass.

Page 7 -- Phase 4: Harden (week 1 to 2)

The week after operations come back is the only week in the calendar year when every control that was previously deferred will be approved by partners and finance without argument. Use it.

The post-incident hardening checklist

Multi-factor authentication enforced on every user account. Including service accounts, including shared mailboxes, including the CEO. Number-matching MFA, not SMS. Conditional access policies block sign-in from unmanaged devices and from outside the geographies where the business actually operates.

Endpoint Detection and Response (EDR) on every managed device. Active monitoring through a 24/7 SOC. No exceptions for "the partner's personal laptop" or "the legacy machine in shipping." If the device touches firm data, it has EDR.

Privileged access management. Local administrator rights removed from end-user accounts. Domain administrator accounts used only for administrative work, never for email or web browsing. Just-in-time elevation for sensitive operations. Documented and audited.

Immutable backup architecture. The backup target is immutable -- neither the production credentials nor a domain administrator can modify, encrypt, or delete the backup chain. The 3-2-1 rule applied: three copies of data, two media types, one offsite and immutable. Documented restore test scheduled quarterly.

KeeperSec (or equivalent) password manager. Rolled out company-wide with shared-vault structure for departments. Eliminates the post-incident credential-rotation problem of "we don't know which fifty SaaS apps that employee was logged into." Fusion's standard rollout is part of the post-incident hardening package.

Email and identity hardening. DMARC, DKIM, SPF on the production domain enforced at p=reject. Legacy authentication protocols (POP3, IMAP, basic SMTP) disabled at the tenant. Out-of-band callback verification policy for any banking-detail change.

Documented incident response runbook signed by the named partner. With on-call contact, decision tree, counsel contacts, carrier contacts, and the post-incident report template prepared ahead of time -- not built mid-incident.

Tabletop exercise scheduled. Within ninety days of the incident, before the muscle memory fades. The exercise is run by the CISSP-led team with all stakeholders in the room, including the cyber-insurance carrier where the policy allows.

Frameworks that map to the hardening list

CIS Controls v8.1 (the Center for Internet Security's prioritized control set), NIST Cybersecurity Framework 2.0, and the cyber-insurance baseline questionnaire that your carrier has already shared with you. These are not competing standards. The hardening list is the intersection.

What to document

Hardening status report by control. Owner. Completion date. Evidence (screenshot, policy export, audit log). The same evidence packet feeds the Phase 5 report and the next insurance renewal.

Page 8 -- Phase 5: Report (week 2 to 4)

The phase most often skipped. The phase that determines whether the next ransomware incident is a recurrence or a different incident.

The cyber-insurance carrier evidence package

Most carriers require a formal post-incident report within thirty days. The package contains:

- Incident summary (one page, dates, scope, outcome)
- Timeline log (Phase 1 through Phase 4, timestamped)
- Initial access vector with root-cause analysis
- Blast-radius finding (encrypted, exfiltrated, restored)
- Backup integrity finding
- Hardening actions completed (Phase 4 list)
- Outstanding remediation with dates
- Vendor / tooling changes
- Next tabletop exercise date

Carriers use this package to set the next renewal premium and the next-year baseline-controls questionnaire. A complete package is the difference between a renewal and a non-renewal.

The board memo template

One page. Five sections. *What happened. What we did. What it cost. What we changed. What is still open.* The memo is read in a closed board session, archived in the corporate record, and re-read at the next AGM. The CEO signs. The IT lead signs. The named director with cyber oversight signs.

Regulatory notification -- PIPEDA Schedule 4

Under the Personal Information Protection and Electronic Documents Act, an organization that experiences a breach of security safeguards involving personal information must notify the Office of the Privacy Commissioner of Canada and affected individuals if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. The record-keeping obligation runs for twenty-four months whether or not notification is required.

The decision is not the IT team's. It is the privacy officer's, with counsel. Phase 5 surfaces the finding. Schedule 4 is the federal framework; provincial frameworks (Quebec Law 25, Alberta PIPA, British Columbia

PIPA) impose additional or parallel obligations where the affected individuals are in those provinces. PHIPA (Ontario health), MFIPPA (Ontario municipal), and FIPPA (Ontario broader public sector) impose sector-specific rules. The sector and the data class determine the path. Fusion does not provide legal advice -- this is the playbook for surfacing the question to counsel, not answering it.

Customer and partner communication

Drafted by counsel, sent by leadership. Internal communications first, then customers whose data may have been affected, then suppliers, then public statement if required. The communications calendar is itself part of the report.

Lessons-learned document

Closed-door, full team, two weeks after operational recovery. Five questions. *What worked. What did not. What would we change in the runbook. What would we change in the controls. What is the next tabletop exercise focus.* Documented. Filed. Re-read before the next incident.

What to document

The full report. The board memo. The notification calculus log. The lessons-learned document. The next tabletop date.

Page 9 -- Pre-incident readiness: the 10 questions every Canadian SMB should be able to answer

These ten questions are the difference between a Monday-morning recovery and a multi-week event. If your leadership team and your IT provider cannot answer all ten with a documented control, an owner name, and a date, the playbook above will not run as written -- and the gap is the work plan.

1. Are our backups immutable? Can the production credentials, including a domain administrator, modify, encrypt, or delete the backup chain? If the answer is "I think so," the answer is no. Immutable means the backup target enforces write-once or object-lock at the storage layer, not at the application layer.

2. When was the last full restore test, with a documented result? File-level restore is not a full restore. The test must include a representative server, a file share, and a sample of the line-of-business application database. Quarterly minimum.

3. Is MFA enforced on every user account, including service accounts and shared mailboxes? Number-matching MFA, not SMS. Including the CEO. Including the partner who travels and "doesn't like the prompt." Conditional access blocks sign-in without MFA, not just prompts for it.

4. Do we have EDR on every managed device, monitored 24/7? Not antivirus. EDR -- behavioural detection, response, and rollback. Monitored by a SOC, not by an inbox. Coverage report exported monthly.

5. Who do we call at 5:47 PM on a Friday? A named on-call number that reaches a human in under fifteen minutes, with a documented escalation tree to a CISSP-led incident-response capability. The cyber-insurance carrier's incident hotline is taped to the same document.

6. Do we know what we own? An asset inventory: every endpoint, every server, every cloud tenant, every SaaS application, every domain, every certificate. Updated monthly. The blast-radius map in Phase 2 starts here.

7. Is our cyber-insurance policy current, and have we answered the baseline-controls questionnaire

honestly? Misrepresentation on the application is the most common reason a claim is denied. The answered questionnaire matches the actual controls. Re-confirmed at each renewal.

8. Do we have a written incident-response runbook signed by a named partner or director? Decision tree. Contact list. Counsel name. Carrier name. Forensic vendor name. Customer-communication template. PR template. The runbook is on paper and on a phone, not just in SharePoint that may be unreachable during the incident.

9. Have we run a tabletop exercise in the last twelve months? With leadership in the room. Not a fire drill. A scenario walk-through with named decisions logged. After-action notes filed. Findings tracked to closure.

10. Do we know which staff member can be reached on which device after 6 PM on a Friday? The contact list is current. The IT lead, the CEO, the privacy officer, the named board director, the counsel, the carrier. Reachable. Tested in the tabletop. Not assumed.

If the answer to any of ten is uncertain, that uncertainty is the most expensive line item on next year's risk register. Fusion's Cybersecurity Assessment closes the ten in ninety days.

Page 10 -- Three case-study sidebars

Three real Fusion engagements, anonymized. The pattern is the same. The specifics -- the industry, the entry vector, the regulatory path -- vary, and the variance is the point.

Sidebar 1 -- Industrial supplier, 45 employees, Mississauga (the lead case)

Friday 4:47 PM. Phished administrative credential. Two endpoints encrypted before lateral movement was contained by EDR. Servers and file shares unaffected. Saturday and Sunday spent on identity rebuild, endpoint reimaging from gold image, and immutable-backup restore validation. Monday 8 AM: full production, zero data loss, zero ransom paid. Post-incident hardening: MFA enforced firm-wide, conditional access deployed, EDR everywhere, the previously-deferred privileged access management rolled out. Cyber-insurance renewal completed with no premium increase.

Why it worked: the pre-engagement cybersecurity assessment ninety days earlier had already flagged the recovery posture and remediated the backup architecture before the incident. Phase 0 -- readiness -- is where this case was actually won.

Reference: /case-study-ransomware-recovery-back-online-by-monday-morning/

Sidebar 2 -- Marketing agency, cyber crisis turned recovery success

A Canadian marketing agency experienced a cyber incident that threatened both client deliverables and the agency's reputation in a relationship-driven sector. Fusion led the containment, restored the affected systems, and worked with leadership to convert the recovery into a measurable security uplift. The agency emerged with a documented incident-response runbook, an EDR-monitored fleet, and a client-communication template that made the post-incident conversations with clients shorter and more confident than the pre-incident security posture would have allowed.

Lesson: a well-run recovery is a marketing asset, not a liability -- but only if Phase 5 is actually executed, not skipped.

Reference: /case-study-how-one-marketing-agency-turned-a-cyber-crisis-into-a-recovery-success/

Sidebar 3 -- Cannabis retail, securing growth in a regulated sector

A Canadian cannabis retailer growing across multiple provinces needed a security posture that could survive both the operational reality of multi-site retail and the regulatory scrutiny of a federally regulated sector. Fusion's engagement was not a post-incident recovery -- it was the readiness work that prevents the Friday call. The result was a security posture that satisfied provincial regulators, payment processors, and the company's own board cyber oversight.

Lesson: in regulated sectors, the cybersecurity posture is also the licensing posture. The same control that satisfies the carrier satisfies the regulator. Phase 0 readiness compounds.

Reference: /case-study-securing-growth-in-the-cannabis-retail-sector/

The three cases differ in industry and entry vector. They share the operating pattern: containment first, validated rebuild second, documented hardening third, formal report fourth. The pattern works.

Page 11 -- Common pitfalls and what not to do

The playbook above is the recoverable path. These are the moves that turn a recoverable incident into a six-figure event. Every one of them is something Fusion has seen another party do on a real engagement.

Do not pay the ransom without panel counsel. Payment may violate sanctions regulations depending on the threat-actor attribution, may void the insurance claim depending on the carrier, may not produce a working decryptor, and may set a precedent the threat actor sells to the next gang. The decision is counsel's, after exfiltration, attribution, and decryptor reliability have been assessed. Not an IT decision. Not a panicked-Friday decision.

Do not unplug the endpoint from the network before the forensic snapshot. Pulling the cable destroys the memory image, eliminates the evidence package, and may erase the indicators-of-compromise that prove the scope is bounded. Network-level isolation through the firewall or switch port preserves the running state. Pulling cables is reflex. The discipline is to isolate, not to disconnect.

Do not restore from a backup that has not been validated. Mount the backup in an isolated environment first. Scan with current EDR signatures. Verify the backup pre-dates the initial access vector window. The most common second-incident pattern is: restore, get hit again ninety minutes later from the same back door.

Do not communicate over the compromised email tenant. Assume the attacker is reading the email thread, including the thread to counsel, the carrier, and the board. Use an out-of-band channel -- a fresh tenant, a managed Signal group, or a conference bridge -- until identity rebuild is complete.

Do not rebuild on the same gold image that produced the incident. If the initial access vector was an unpatched service or a configuration weakness, the same weakness is on the gold image. Update the image, harden it, and validate before reimaging the fleet.

Do not skip the carrier notification. Carriers have voided coverage on policies where the insured took remediation action -- including paying a vendor -- before notifying the carrier. The notification call is Phase 1, not Phase 5.

Do not promise the board a timeline before Phase 2 is complete. Premature timelines force premature restore actions and premature restore actions skip validation. The bridge runs the bridge. The bridge tells the board the timeline when the bridge knows the timeline.

Do not let the cyber-insurance carrier or the threat actor set the operational tempo. The carrier has interests. The threat actor has leverage. The decisions are the insured's -- informed by counsel, supported

by the IT partner. The CEO does not delegate the rebuild-versus-decrypt decision to the carrier's chat support agent.

Do not skip Phase 5. A ransomware incident without a formal report is an incident that will repeat. The lessons-learned document is the most expensive document the organization will ever fail to write.

Do not assume the IT provider's "we're fine" is an answer. If the provider cannot walk leadership through each of the ten pre-incident questions on page 9 with a date, a name, and a piece of evidence, the answer to all ten is "uncertain," and the playbook above will not run as written.

Page 12 -- Next steps + how Fusion engages

If this playbook is more detailed than what your current IT partner has documented, that itself is the finding. The fix is not to wait for the Friday call. It is to close the readiness gap in ninety days.

Two paths forward

Path 1 -- Use this playbook as the audit. Hand the ten questions on page 9 to your IT lead and your current provider. Ask for the documented control, the owner, and the date for each. The gaps are the prioritized work plan. The cost of the gaps is the cost of the next incident.

Path 2 -- Engage Fusion for a Cybersecurity Assessment. A two-week, CISSP-led engagement that produces the same evidence-by-control answer the ten questions on page 9 require, plus a remediation roadmap mapped to CIS Controls v8.1 and your cyber-insurance carrier's baseline questionnaire. The assessment is the same engagement that prevented Sandra's Friday call from becoming a Monday shutdown.

What Fusion's incident-response engagement includes

- 24/7 CISSP-led on-call response
- EDR-monitored fleet with SOC integration
- Immutable backup architecture with quarterly restore tests
- Written incident-response runbook signed by your named partner or director
- Cyber-insurance carrier liaison during active incidents
- Phase 5 report package delivered within 30 days of an incident
- Annual tabletop exercise included

What we don't do

We do not negotiate with threat actors -- that is panel counsel's job, with attribution support from a specialist forensic vendor. We do not provide legal advice -- that is your privacy counsel. We do not file your PIPEDA notifications -- that is your privacy officer with counsel. We run the operational playbook. The rest of the ecosystem stays in its own lane and we make sure the lanes coordinate.

Talk to us before the Friday call

The clients whose names appear in case-study sidebars are not the clients who got lucky. They are the clients who did the readiness work in the ninety days before. The conversation that prevents the Monday shutdown happens on a Wednesday morning, not on a Friday evening.

Book a 30-minute Ransomware Readiness Walk-through ->

Mike Pearlstein, CISSP -- Founder & CEO, Fusion Computing Toronto . Hamilton . Greater Toronto Area . Metro Vancouver Named in Canada's 50 Best Managed IT Companies 2024 & 2025 Founded 2012

This document is operational guidance from a CISSP-led MSP. It is not legal advice, not a substitute for cyber-insurance policy wording, and not a regulatory determination under PIPEDA, Quebec Law 25, Alberta PIPA, British Columbia PIPA, PHIPA, MFIPPA, FIPPA, or sector-specific regimes. For Canadian SMBs in federally regulated critical sectors, note that Bill C-8 (the Critical Cyber Systems Protection Act framework) passed third reading in the House of Commons on 2026-03-26 and is not yet in force for general SMB scope; the Office of the Privacy Commissioner of Canada and your sectoral regulator remain the authoritative sources. Sources: priv.gc.ca (PIPEDA Schedule 4 breach reporting), cisecurity.org (CIS Controls v8.1), nist.gov (NIST CSF 2.0), parl.ca (Bill C-8 status).