BreachReady
BY DFI FORENSICS

A GUIDE FOR BUSINESS LEADERS

Avoiding delay in a cyber crisis

A leadership guide



NOVEMBER 2026

dfiforensics.ca

01 / PREPARED LEADERSHIP

Arrange expertise before the pressure starts

A cyber incident can leave leadership with urgent decisions and incomplete facts. Which services should stop? Who can authorize containment? What should clients be told? Finding the right specialists, agreeing terms and establishing decision authority at that moment can add avoidable delay.

BreachReady brings retained DFI incident-response specialists into your preparations before a crisis. From day one of an active annual agreement, you have priority access to support 24/7 under the agreed terms. DFI works with your leadership and IT provider on preparation and risk reduction, including business email compromise and ransomware. [1, 2]

READINESS THAT SUPPORTS ACTION

Specialists arranged

A known contact route and agreed engagement.

Decisions practised

Named roles and realistic incident scenarios.

Recovery directed

Business priorities linked to technical work.

Your IT provider and DFI have complementary roles

Your IT team or managed service provider runs day-to-day technology and implements agreed technical changes and restoration. DFI adds specialist incident response, forensic investigation and readiness guidance. Leadership retains business decisions; counsel advises on legal obligations. These responsibilities should meet in one response plan, rather than compete during an incident.

The leadership objective

Make the next safe decision with the right people and enough reliable information. A plan is useful when the team can actually use it.

This guide explains the arrangements, decisions and communication habits that help. It is preparation guidance, not a substitute for your organization-specific response plan. If an incident is underway, use your agreed response route now; do not wait to finish this guide.

02 / AUTHORITY AND ACCESS

Make decisions possible when normal systems fail

An incident-response plan should explain who can act, who must be consulted and who takes over if the usual decision-maker is unavailable. A name in a document is not enough if that person cannot approve the work or cannot be reached outside office hours. [3, 4]

Business leadership	Choose the response lead and deputy. Set authority for emergency spending, service interruption, customer commitments and accepting residual risk. Give technical responders a clear route to a decision.
Technical response	Identify who can isolate devices, restrict accounts and protect backups. Agree the boundaries of pre-authorized containment and how actions will be recorded. Technical choices need to reflect safety and business dependencies.
Legal and privacy	Arrange access to counsel and a privacy lead. They assess applicable duties and oversee sensitive communications. Do not assume that involving counsel automatically makes every record privileged.
Finance and insurance	Know the insurer or broker notification route, relevant policy conditions and bank fraud contact. Confirm consent or provider requirements before a crisis, rather than assuming any engagement or cost is covered.

Build a route around unavailable or untrusted email

Keep an accessible offline copy of essential contacts and the plan. Establish an alternate communication channel that does not depend on the affected accounts. Decide how participants will verify one another and limit access to incident information. Test this route with deputies and external advisers.

A useful leadership question

If our email and primary administrator account were unavailable tonight, could the response lead reach the right people and authorize the first protective actions?

03 / THE EARLY RESPONSE

Stabilize the incident without losing the evidence

The first objective is to reduce ongoing harm while building a reliable picture of what happened. Containment, investigation, business continuity and legal assessment often proceed together. Their order depends on the incident; a rigid minute-by-minute timetable can create false confidence. [3]

Activate the team and define the immediate risk

Acknowledge the report, open an incident record and bring in the response lead, IT and retained specialists. Separate observed facts from suspicions. Record the affected service, the time noticed, what users are seeing and any action already taken. Prioritize threats to people, continued unauthorized access, fraudulent payments and spreading disruption.

Coordinate containment with evidence preservation

Authorized responders may need to isolate devices or restrict accounts promptly. They should preserve relevant logs, messages, alerts and other evidence as practicable, without delaying urgent protection. Avoid indiscriminate deletion, wiping or restoration. Record who changed what and when so later analysis can distinguish attacker activity from response activity.

PARALLEL WORK THAT NEEDS ONE COORDINATOR

Contain harm

Reduce ongoing access and exposure.

Establish facts

Preserve and examine relevant records.

Keep service moving

Use approved continuity arrangements.

Make staged decisions as the picture develops

Ask the technical lead what is known, what remains uncertain and which decision cannot wait. A reversible restriction may be appropriate before the full scope is known. A broad return to service needs more evidence. Agree the next review point and make one person responsible for confirming whether each action happened.

Do not confuse activity with control

A password reset, a clean scan or a restored server is an action. The team still needs to assess whether unauthorized access remains and what information or services were affected.

04 / COMMUNICATIONS AND OBLIGATIONS

Give people reliable information and a clear next step

A cyber incident creates an information problem as well as a technical one. Staff need instructions, clients may need protection and leaders need a basis for decisions. A calm update should distinguish confirmed facts, the current impact, protective action and the next update. Avoid confident claims that the evidence does not support.

Inside the organization	Tell staff which channels and systems to use, what to stop doing and how to report new signs. Keep unnecessary personal information out of broad updates. Give the response team a single place to maintain the current position.
Clients and partners	Coordinate notices with legal, privacy and communications advisers. Explain relevant impact and useful protective steps without speculating. Target practical warnings when a fraudulent message or payment request may still cause harm.
Authorities and insurer	Evaluate applicable reporting, notification and contractual duties promptly. Requirements differ by jurisdiction, sector, information and agreement. Record the basis for decisions, including why further facts are needed.

Do not treat confidential information as a secondary issue

An incident can affect information confidentiality even when systems keep working. Where PIPEDA applies, organizations must report qualifying breaches that create a real risk of significant harm, notify affected individuals and keep records of all breaches. Other laws and contracts may also apply. Counsel should assess the actual circumstances and deadlines. [5]

Maintain a decision record that can be understood later

Capture the decision, decision-maker, time, facts relied on, alternatives and follow-up. Preserve original evidence separately from working summaries. Correct earlier statements when new information changes them. The aim is a defensible account of the response, not a polished story that conceals uncertainty. [3]

05 / REHEARSAL AND CONTINUING READINESS

Practise the difficult choices before they become urgent

A tabletop exercise is a structured conversation about an incident, not a test of who can guess the technical answer. It should expose hand-offs, missing authority and unrealistic assumptions. Use the actual people, contact routes and business priorities in your plan. [3, 4]

A supplier warning changes the picture

ILLUSTRATIVE SCENARIO / NOT A DFI CLIENT INCIDENT

A supplier says it received unusual payment instructions from your finance mailbox. Email still works. The finance lead is travelling and the IT provider has found an unfamiliar forwarding rule.

At the first decision point, discuss who can hold pending payments, activate specialists and restrict the account. Then introduce a second fact: the mailbox contains confidential client correspondence. The team must now consider information exposure alongside fraud.

Finally, suppose the mailbox can be restored, but the access history is incomplete. Decide who authorizes normal use, how clients will be protected and what uncertainty must remain in the leadership update.

Turn findings into owned improvements

End the exercise with a short set of prioritized changes, each assigned to a person with a due date. Retest the weak hand-off or recovery assumption after the change. A completed exercise has limited value if everyone leaves expecting someone else to resolve the gaps.

Keep preparation connected to the business

Review the plan when key staff, vendors, systems or services change, and after incidents or exercises. Ask your team to demonstrate important capabilities: an alternate contact route that works, a restore test that supports a business service, and a payment-verification process that survives a senior executive's urgent request.

Ask what your team can do today

Confidence should come from arrangements that exist and actions the team can carry out, not from an intention to complete them later.

06 / SPECIALIST HELP AND REFERENCES

Put specialist guidance behind your response

BreachReady helps your organization prepare an expert-led response, reduce exposure to common cyber threats and keep readiness current. DFI guides the planning and rehearsal with your team; your IT provider implements agreed technical safeguards and restoration. Retained support helps you avoid starting those arrangements in the middle of a crisis. [1, 2]

A useful first conversation starts with your existing IT and security support, critical business services and current response arrangements. We can discuss where specialist support would add value and what preparation would involve for your team.

Talk through your current arrangements

dfiforensics.ca/contact | 778-742-5621 | info@dfiforensics.ca

If an incident is underway, existing BreachReady clients should use their agreed response arrangements. Others can visit dfiforensics.ca/incident-help. An inquiry does not create an engagement or guarantee a response time. Do not send passwords or confidential evidence with an initial inquiry.

Sources and further reading

Primary sources checked 9 November 2026. General preparation guidance, not legal advice or an assessment of your organization. Apply current service documentation, law and agreed engagement terms. Sources do not imply endorsement of DFI.

[1] DFI Forensics | BreachReady
Annual preparedness and response program; specialist and IT-provider roles.

[2] DFI Forensics | What BreachReady includes
Response planning, playbooks, exercises and continuing readiness support.

[3] NIST | SP 800-61 Rev. 3
Incident response within cybersecurity risk management, April 2025.

[4] Canadian Centre for Cyber Security | Incident response planning
Roles, response arrangements and plan maintenance, ITSAP.40.003.

[5] Office of the Privacy Commissioner of Canada | Breach reporting
PIPEDA reporting, notification and record-keeping obligations.

[6] DFI Forensics | Urgent cyber incident help
Incident contact route and existing-client response arrangements.