BreachReady
BY DFI FORENSICS

A GUIDE FOR BUSINESS LEADERS

Preparing for ransomware

Beyond the backup



NOVEMBER 2026

dfiforensics.ca

01 / THE BUSINESS RISK

Prepare for the disruption as well as the encryption

Backups are essential, but they do not decide which service returns first, establish whether an attacker still has access or resolve the theft of confidential information. Ransomware preparation has to connect technical recovery with business continuity, investigation and leadership decisions.

BreachReady arranges DFI incident-response specialists before a crisis, with priority support 24/7 from day one of an active annual agreement. DFI guides practical ransomware mitigation and response preparation alongside your team and IT provider. The agreed engagement defines support and scope; it is not a guarantee of prevention or recovery. [1, 2]

RECOVERY HAS MORE THAN ONE DIMENSION

Availability

Can essential services operate again?

Trust

Are systems and accounts safe to use?

Confidentiality

Was information accessed or taken?

Data theft can outlast the outage

Attackers may steal information as well as encrypt systems, or use theft alone to extort the organization. Restoring data does not remove copies held by an attacker. A recovery plan therefore needs a way to investigate possible exposure and support decisions about affected people, contracts and communications. [3]

Put business ownership beside technical responsibility

Your IT provider implements agreed safeguards and restoration. DFI adds specialist response and forensic guidance. Leadership defines service priorities and accepts business risk, with counsel advising on legal duties. A shared plan helps these responsibilities work together rather than leaving restoration decisions entirely to whoever can bring a server online.

The question behind the backup report

Could we restore a trusted, usable business service after losing our normal systems and accounts? A successful backup job does not answer that on its own.

02 / REDUCING EXPOSURE

Make entry harder and limit the reach of an attack

A useful mitigation discussion follows the ways an attacker could gain access, obtain more privilege and reach critical systems. The aim is not to buy every available product. It is to establish a maintained set of safeguards with clear ownership and evidence that they work.

Protect access	Use strong authentication, including phishing-resistant MFA where supported, for email, remote access and administrative accounts. Remove unnecessary access and separate privileged accounts from ordinary daily work. [3, 4]
Reduce exposed weaknesses	Keep supported systems updated, prioritize exploitable internet-facing weaknesses and remove unnecessary exposed services. Know who owns remote-access tools and how third-party access is approved and withdrawn. [3, 4]
Limit movement	Separate critical systems and backup administration where appropriate. Restrict permissions and connectivity so one compromised user or device does not automatically reach every important resource. Have your IT provider validate the design. [3]
Detect and act	Maintain supported endpoint and other security tools, relevant logs and an alert-handling process. Confirm who investigates warnings and who can isolate a device or account, including outside normal working hours. [6]

Turn assessment findings into completed changes

A network vulnerability assessment helps identify and prioritize technical concerns. It does not reduce the risk by itself. Assign remediation, confirm completion and test important changes. BreachReady's specialist guidance can help your team and IT provider connect that work to common ransomware paths and business impact. Scope and technical testing must be agreed. [1, 2]

Avoid a false sense of coverage

Retained response expertise is not the same as continuous monitoring or a managed security operations centre. Confirm separately who watches alerts and what each provider is engaged to do.

03 / RECOVERABLE BACKUPS

Protect the recovery route from the same compromise

A backup can exist and still be unusable when it is needed. It may be incomplete, too old, reachable by the same compromised administrator or dependent on an unavailable service. Treat backup resilience as a recovery capability that must be demonstrated, not just a successful status indicator. [3, 4]

Separate access and preserve a usable copy

Have your provider design appropriate barriers between production systems and backups. Depending on the environment, this may include offline or immutable copies, separate administrative credentials, MFA and restricted management access. Verify who can change retention or delete copies, and whether the organization could recover if its normal identity systems were unavailable.

Define tolerable loss and interruption

For each critical service, leadership should agree the maximum tolerable interruption and the amount of recent data the business could lose. Recovery time and recovery point objectives translate these needs into targets. They are planning objectives, not evidence of achieved performance. Compare them with restore-test results and fix the gap. [5]

TEST A SERVICE, NOT ONLY A FILE

Recover the data

A usable copy from an appropriate point.

Rebuild dependencies

Identity, network, applications and access.

Prove business use

A responsible owner completes a real task.

Make the test reflect the incident you fear

A meaningful exercise might assume the backup administrator's normal laptop and primary credentials are unavailable. In a controlled environment, recover a representative service, record elapsed time and identify missing licences, keys, configuration, people or vendor assistance. Do not expose live data or disrupt production just to make the test realistic.

Choose the restore point deliberately

The newest backup may contain compromised files or configuration. Technical responders need to assess integrity and the incident timeline before selecting what to restore. [3, 6]

04 / BUSINESS CONTINUITY

Restore the work not merely the servers

Start recovery planning with the business activities people rely on. Payroll, client service, production and regulatory reporting have different deadlines and dependencies. A system's technical importance does not always match the order in which the organization needs its services back. [5, 7]

Map a critical service from end to end

For one priority service, identify its people, applications, data, identity access, network connections and outside providers. Determine what minimum service looks like during an outage and who can authorize it. A restored application may still be unusable if staff cannot sign in, a shared file store is missing or an external integration is not available.

The server is back, but the business is not

ILLUSTRATIVE SCENARIO / NOT A DFI CLIENT INCIDENT

A team restores its order-management server. Staff still cannot process orders because account access, shipping connections and current stock records are unavailable. The service owner and technical lead must coordinate the dependencies, validate data and approve a controlled return to use. The backup restored a component; the recovery plan restores the service.

Plan temporary work without creating a second problem

Agree how essential activity could continue through approved manual or alternate processes. Keep those processes proportionate to safety, confidentiality and fraud risks. Uncontrolled personal email accounts, improvised file sharing or bypassed payment approvals may create new exposure during the outage. Record transactions that must later be reconciled.

Set evidence for return to service

Decide in advance who must sign off on technical readiness and business usability. The decision should consider containment, identity security, restored data integrity, essential functions and the remaining risks. Some services may return in stages. Record any temporary controls and the point at which they must be reviewed or removed.

A practical leadership conversation

Which service must work first, what does it depend on, and who can demonstrate that it is ready for people to use?

05 / RESPONSE AND RECOVERY DECISIONS

Contain the incident then recover with evidence

If ransomware or suspected data extortion is discovered, activate your response arrangements immediately. Use a verified communication route that does not depend on affected accounts. Bring together the response lead, IT, retained specialists and legal or privacy advisers. Address immediate safety risks first. [3, 6]

Coordinate containment and preservation

Authorized technical responders should reduce ongoing access and spread while preserving relevant logs, alerts, affected-system evidence and ransom communications as practicable. Avoid indiscriminate wiping or restoration that destroys the information needed to understand the attack. Evidence work must not delay urgent protection. Record response changes and their timing.

Do not let the ransom deadline set the whole strategy

A demand is an attacker's claim, not proof that payment will restore systems or prevent disclosure. Payment carries legal, financial and operational risks and does not guarantee recovery. Obtain specialist legal advice, involve relevant authorities and the insurer, and follow applicable requirements. Do not make commitments or conduct negotiations informally. [3, 4]

Investigate exposure while rebuilding trusted operations

Restore in a controlled sequence with appropriate identity and access remediation. Validate backups and systems before returning them to use. Continue assessing possible data theft and notification duties even when operations improve. Where PIPEDA applies, reporting and notification depend on the risk of harm, and records of all breaches must be kept. Other laws and contracts may apply. [6, 8]

Rehearse the recovery decisions before the event

Use a scenario in which a critical service is unavailable and the attacker claims to have copied client data. Have leaders explain their service priorities, contact routes, decision authority and communication approach. Have the technical team demonstrate a separate controlled restore test. Resolve the gaps with named owners and retest what changed.

Keep recovery and closure separate

Bringing services back is a milestone. Closing the incident also requires a supported account of impact, outstanding duties and corrective work.

06 / SPECIALIST HELP AND REFERENCES

Build confidence in the recovery you can perform

BreachReady helps turn preparation into arrangements your team can use: retained specialists, response plans and playbooks, rehearsed decisions and guidance on ransomware and business email compromise mitigation. DFI works with your IT provider on agreed safeguards and helps leadership connect response choices to business priorities. [1, 2]

Bring your essential services, backup and restore arrangements, existing IT support and any recent test findings. We can discuss the preparation and specialist support that would add the most value for your organization.

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] Canadian Centre for Cyber Security | Ransomware playbook
Ransomware, data extortion, preparation and response, ITSM.00.099.

[4] Canadian Centre for Cyber Security | Ransomware prevention and recovery
Protective measures, backups and the risks of payment, ITSAP.00.099.

[5] Canadian Centre for Cyber Security | IT recovery planning
Recovery dependencies, responsibilities and testing, ITSAP.40.004.

[6] Microsoft | Incident Response ransomware approach
Identity, evidence and coordinated restoration considerations.

[7] Canadian Centre for Cyber Security | Business continuity planning
Continuing essential operations during disruption, ITSAP.10.005.

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