GUIDE · INCIDENT RESPONSE

PRIVATEER CYBERSECURITY

Cyber incident first-hour card

What to do, who to call and what not to touch in the first hour of ransomware, email fraud or a lost laptop. Printable.

Printable PDF | 8-minute read | Updated October 2026

Print it. Tape one copy by the server closet and one in the office manager's desk. Fill in the contacts section today, not during the incident.

PART 1: WHAT TO DO IN THE FIRST HOUR

If money left by wire or EFT in the last 72 hours: call your bank's fraud line now, then come back here.

Before anything else (2 minutes)

1. **Name one incident lead.** One person decides; everyone else reports to them. When two people give IT different instructions, you lose time.

2. **Start a paper log.** Write the time, what you saw, and who did what. Use paper or a phone that is not on the company network. Your insurer, your lawyer and the regulator will all ask for this timeline, and "promptly" is judged against it.

3. **Stop using company email and Teams/Slack to talk about it.** In many ransomware and email-fraud cases, the attacker can read the mailbox. Use phone calls, or a Signal/WhatsApp group on personal phones.

What are you looking at?

YOU SEE…	IT IS PROBABLY…	GO TO
Files renamed with a strange extension, a ransom note, servers or shared drives suddenly unreachable	**Ransomware**	A
A client or supplier says they got an email from you with new banking details; a payment went to the wrong account; strange inbox rules; MFA prompts nobody asked for	**Email account takeover / payment fraud (BEC)**	B
A laptop, phone or USB drive is lost or stolen	**Lost device**	C

YOU SEE…	IT IS PROBABLY…	GO TO
An odd login alert, an antivirus pop-up, “something feels off”	**Treat it as B** until someone proves otherwise	B

A. Ransomware

Do

- ✓ **Unplug the network cable and turn off Wi-Fi on affected machines. Leave them powered on.** Memory holds evidence (running processes, sometimes keys) that is lost on shutdown. *Exception:* if a file server is visibly encrypting and you cannot cut its network, powering it off is the lesser evil. Write down that you did it and when.
- ✓ **Disconnect backups now.** Unplug USB/NAS backup drives. Change the backup console password and MFA from a clean device (a phone, a home computer), never from a machine on the affected network. Attackers go after backups early.
- ✓ **Call your insurer’s breach line before you hire anyone or spend money.** Many policies require the insurer’s prior consent and its panel vendors, and costs you commit to first may not be reimbursed. Don’t wait for the callback to contain the attack: isolating machines is always allowed.
- ✓ **For IT:** export firewall, VPN and EDR logs to offline storage before anyone “cleans up.” Note which logs roll over and when.

Don't

- ✗ **Don’t open the ransom note link or contact the attackers.** Contact tells them you have found them and can speed up a data leak. Paying does not guarantee you get your data back, and it may be unlawful under terrorism, money-laundering or sanctions laws (Canadian Centre for Cyber Security). Any negotiation is a specialist job coordinated with your insurer and counsel.
- ✗ **Don’t restore into the same network yet.** If you restore before the way in is closed, you restore into a network the attacker still controls, and you overwrite evidence of what they took. The entry point is usually a VPN or firewall without MFA, exposed remote desktop, or a stolen password. Restore once that is fixed, or into an isolated, rebuilt environment, with your incident response firm.
- ✗ **Don’t reimage, wipe or run “cleaner” tools.** That destroys the evidence your insurer, your lawyer and the privacy regulator will ask for.
- ✗ **Don’t assume “they only encrypted, they didn’t steal.”** Most ransomware groups now copy data before encrypting. Until forensics shows otherwise, plan as if personal information was taken.

B. Email takeover / payment fraud (BEC)

Do

Don't

- ✓ **If money left: call your bank's fraud line within the hour and ask for a wire recall.** Recovery odds drop by the hour as funds are moved on. Then file a police report; the bank and insurer will ask for the file number.
- ✓ **Lock the account, then kill the sessions.** A password reset does not log out an attacker who already holds a session token. In Microsoft 365: Entra admin center → Users → the user → *Revoke sessions*. Also block sign-in while you investigate, because tokens already issued can keep working for up to about an hour. Then remove and re-register MFA methods (attackers often add their own authenticator app). In Google Workspace: reset sign-in cookies and review 2-Step Verification devices.
- ✓ **Photograph before removing anything:** inbox rules (forwarding, auto-delete, rules moving mail to "RSS Feeds" or "Archive"), mailbox forwarding, apps granted access (OAuth consents), newly registered MFA devices.
- ✓ **Export the logs today.** Microsoft Entra sign-in and audit logs are kept **7 days** on the free tier and **30 days** with Entra ID P1/P2. The Microsoft 365 unified audit log (Audit Standard) keeps 180 days. Logs you don't export may be gone before forensics starts.
- ✓ **Phone your top clients and suppliers** (use numbers from your own records, not from the email) and tell them that any banking change "from us" is fraudulent. The attacker has often emailed your whole address book.

- ✗ **Don't delete the phishing email or the malicious rules.** They show what the attacker read. That decides whether personal information was accessed, which decides your Law 25 / PIPEDA obligations.
- ✗ **Don't reply to the fraudulent thread** to "warn" the other party. The attacker controls the thread.

C. Lost or stolen device

Do

- ✓ **Establish one fact first: was it encrypted (BitLocker/FileVault/phone passcode) and locked?** This largely decides whether you face a reportable privacy incident. Ask IT for proof, such as the MDM compliance report or the escrowed BitLocker recovery key. "I think so" is not proof.

Don't

- ✗ **Don't skip the register because it was encrypted.** Under Law 25, every confidentiality incident goes in the register, including the loss of a device holding personal information. Record it and write down why you judged the risk low (encryption, locked, wiped at 14:32).

- **Remote lock or wipe through MDM** (Intune, Jamf, Google endpoint management). Record the time and the confirmation.
- **Revoke that user's sessions and change any passwords saved in the browser** (email, banking, line-of-business apps).
- **File a police report if it was stolen.** The insurer and regulators will ask for the number.

Call in this order

1. **Bank fraud line first** if money moved in the last 72 hours.
2. **Internal incident lead** (decides; one voice).
3. **Insurer breach line**, *before* you hire vendors or spend money. Insurers usually assign a breach coach (a lawyer) and a forensics firm. **No insurance?** Call an incident response firm and a lawyer directly.
4. **Breach coach / lawyer.** Running the investigation through counsel may help protect privilege. Ask them; don't assume.
5. **IT provider / MSP.** Tell them: contain, don't wipe. If their remote management tool could be how the attacker got in, they are part of the investigation, not just the fix.
6. **Police and the Canadian Anti-Fraud Centre** for fraud or extortion: 1-888-495-8501, reportcyberandfraud.canada.ca. The **Canadian Centre for Cyber Security** also takes reports: 1-833-CYBER-88 (1-833-292-3788), My Cyber Portal.
7. **Privacy regulators:** once you have facts, with counsel (see the clocks below).
8. **Staff, clients, partners:** once, from a script. Don't let rumours go out first.

Evidence to keep (don't delete, don't "tidy up")

- Your paper log (time-stamped).
- Photos of ransom notes, error screens and suspicious emails (whole screen, with the clock visible).
- The suspicious emails themselves, exported with full headers (.eml/.msg), not forwarded.
- Firewall, VPN, EDR/antivirus, and Microsoft 365/Google Workspace sign-in and audit logs, exported to offline storage.
- Affected machines: powered on and unplugged, or powered off and labelled with who touched them and when.
- Bank confirmations, wire details, the fraudulent invoice.
- A list of every person who touched an affected system, with times.

Regulatory clocks

Privacy law in Canada has **no fixed hour count** like Europe's 72 hours. "Promptly" and "as soon as feasible" are judged after the fact, and your log is how you defend them. Regulated sectors are different (see the table).

IF YOU…	OBLIGATION	CLOCK
Operate in **Quebec** (Law 25, private sector act)	Record **every** confidentiality incident in your register, serious or not. Keep each entry at least **5 years** after you became aware of the incident. Take reasonable measures to reduce the risk of injury and prevent new incidents.	Register: now.
	Assess the risk **with your person in charge of protection of personal information**. If there is a **risk of serious injury**, notify the **Commission d'accès à l'information** (form *Déclaration d'un incident de confidentialité*) **and** the people concerned. Risk factors: sensitivity of the information, likely consequences of its use, likelihood of misuse. Notice to individuals may wait while it would hamper an investigation. You may also notify anyone who can reduce the risk, sharing only what is needed.	**Promptly** ("avec diligence").
Are subject to **PIPEDA** (federal; often applies alongside Law 25 when information crosses provincial or national borders)	If a breach creates a **real risk of significant harm**: report to the **OPC** (online breach form), notify affected individuals, and notify organizations that can reduce the harm (e.g., banks). Keep a record of **every** breach for **24 months**.	**As soon as feasible** after you determine a breach occurred.
Operate in **Alberta**	PIPA requires a separate report to the Alberta OIPC where a reasonable person would consider there is a real risk of significant harm.	Without unreasonable delay.
Are a **regulated financial institution** (AMF in Quebec, OSFI federally)	Report information security incidents to your regulator. AMF: updates every 3 days, final report within 30 days of resolution.	**Within 24 hours** (AMF regulation in force since April 2025; OSFI advisory).
Have **cyber insurance**	Notice clause in your policy. Late notice is a classic reason for disputed claims.	Per your policy: write it below.
Have **client contracts / DPAs**	Many contracts require notifying the client within a fixed window (often 24-72 hours).	Per contract: write the strictest one below.

This card is not legal advice. Your breach coach decides what gets reported and when.

Fill this in today

ROLE	NAME	PHONE (24/7)	BACKUP CONTACT
Incident lead			

ROLE	NAME	PHONE (24/7)	BACKUP CONTACT
Deputy (if lead unreachable)			
IT provider / MSP			
Insurer breach line			
Policy number		Notice deadline in policy:	
Breach coach / lawyer			
Bank fraud line		Account manager:	
Incident response firm (if no insurance, or once your insurer approves it)			
Person in charge of the protection of personal information (Law 25)			
Strictest client notification clause	Client:	Hours:	

If you are insured, ask your insurer now which incident response firms it approves, so there is no dispute on the day.

Where the offline copies live: backup admin credentials: ____ · break-glass admin account: ____ · this card (digital copy, outside company systems): ____

Last reviewed: __ / __ / __ by: ____

Get a second pair of eyes.
Talk directly to the expert who would lead the work.

PRIVATEER CYBERSECURITY
privateer.ca · info@privateer.ca