INCIDENT RESPONSE RUNBOOKS · FREE EXTRACT

The first hour

What to do in the sixty minutes after you realise something has gone wrong — and which Canadian clocks start running the moment you do.

FREE · SHARE IT FREELY INSIDE YOUR ORGANISATION

Three rules before you touch anything

- **One person coordinates.** Name them out loud. Everything else goes wrong when four people are independently phoning the same supplier.
- **Do not destroy evidence.** Isolate machines, do not wipe them. Do not delete the phishing email. Logs you overwrite today are the logs your insurer and the regulator will ask for.
- **Promise nothing yet.** Not to customers, not to staff, not on social media. You do not know the scope in the first hour, and a correction later costs more trust than an hour of silence.

The first sixty minutes

0 – 15 MIN

Stop the bleeding

1. Name the coordinator and open a written log. Time-stamp every entry from now on.
2. Isolate affected systems from the network. Disconnect, do not power off — memory holds evidence.
3. Disable or reset the credentials you believe were used, including any session tokens.
4. Check whether backups are reachable and, critically, whether they are also affected.
5. Tell your cyber insurer's hotline if you hold a policy. Many policies require notice before you engage anyone.

15 – 30 MIN

Work out what you are dealing with

1. What exactly happened, in one sentence you would be comfortable reading back in six months.
2. Which systems, which accounts, which data. Write down what you know and what you are guessing.
3. Was personal information involved, or might it have been? This is the question that starts the legal clocks.
4. Is it still happening? An incident that is contained and one that is live need different next moves.
5. Does a supplier or customer need to know because their systems are exposed through yours?

30 – 60 MIN

Decide and notify

1. Work through the notification decision tree overleaf. Decide, and record why you decided it.
2. Start the record that the law requires whether or not you end up notifying anyone.
3. Brief one person to handle all external questions. Everyone else refers to them.
4. Tell the board or owner. A short factual note now is worth more than a polished one tomorrow.
5. Book the post-incident review before you finish the call. It will not happen otherwise.

What to write down

This record is not paperwork. It is the evidence that you handled the incident competently, and it is the first thing anyone will ask for.

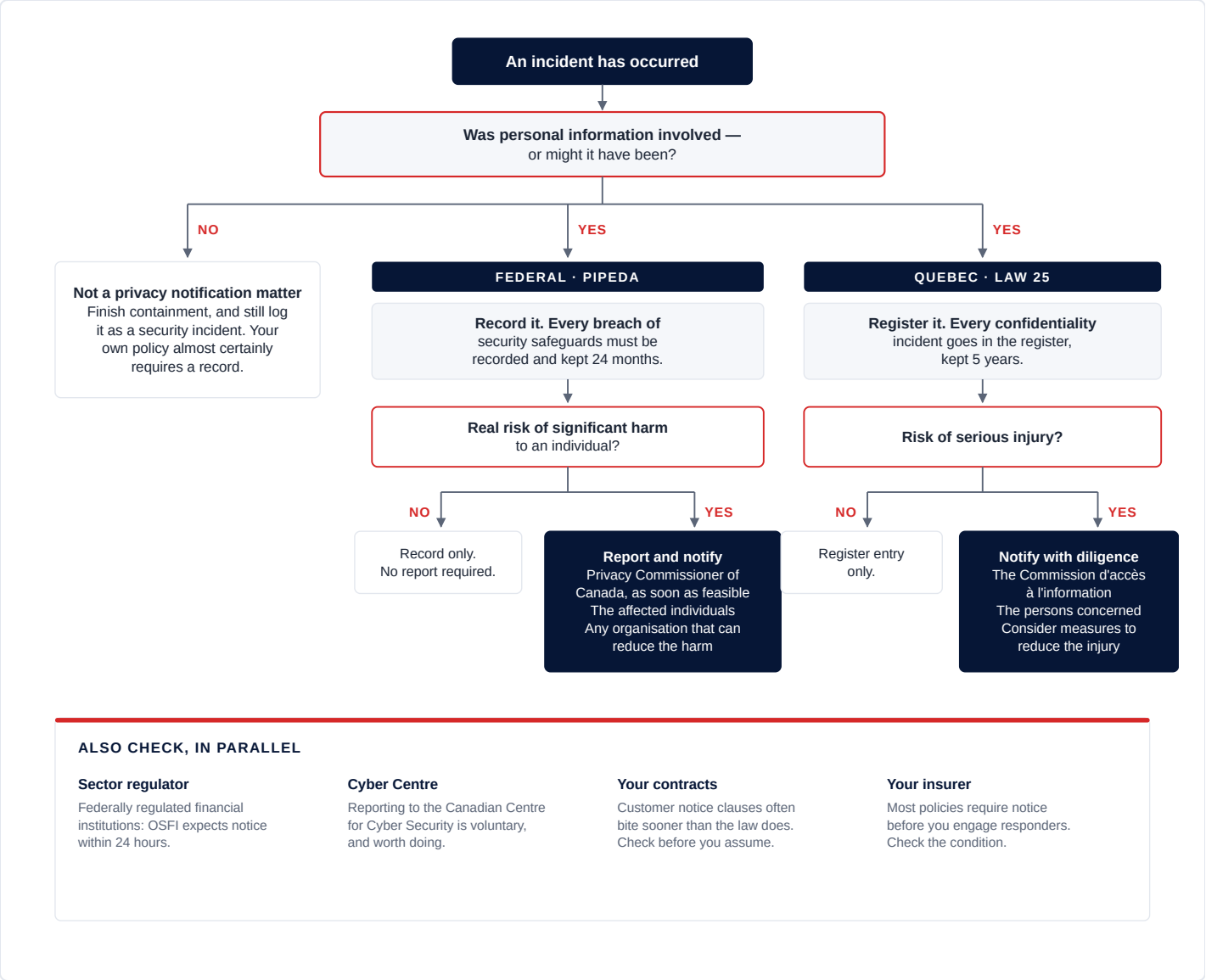
FIELD	WHY IT MATTERS
When you became aware	Both retention clocks run from a date you must be able to state.
What happened	In plain words. Regulators read these; so do customers, eventually.
Personal information involved	Categories and approximate number of people. Say 'unknown' if it is unknown.
Harm assessment	Your reasoning, not just your conclusion. The reasoning is what gets tested.
Who was notified, and when	Regulator, individuals, other organisations, insurer, customers.
What you changed	The control you fixed. This is what turns an incident into an improvement.

What not to do

- ✕ Do not pay a ransom before taking advice. It may be a sanctions offence, and it rarely restores everything.
- ✕ Do not email about the incident using the system you think is compromised.
- ✕ Do not tell anyone the incident is closed until you know how the attacker got in.
- ✕ Do not let 'we are still investigating' become the reason you miss a notification deadline. The clock does not pause.
- ✕ Do not skip the record because you decided not to notify. The record is required either way.

The notification decision tree

Two regimes can apply at once. Federal law and Quebec law ask different questions, use different thresholds and keep records for different lengths of time. Work through both — not one or the other.



This tree covers private-sector organisations. Federally regulated sectors, public bodies and health information custodians carry additional obligations. It is a starting point for your own legal advice, not a substitute for it.