Breach-response playbook: the first 72 hours

The hours after a breach is discovered decide how the rest of it goes. This playbook covers what to do first, who does it, and the reporting deadlines that are already running before you have finished investigating.

> **The clock starts on awareness, not on certainty.** Reporting deadlines run from the moment your organisation becomes aware of an incident — not from the moment you finish investigating it and confirm the full impact. Treat the discovery itself as the trigger and start the clock immediately. Waiting for a complete picture is the most common way teams miss a deadline.

Reporting deadlines at a glance

Which of these apply depends on the data involved, where the affected people are, and your contracts. Confirm the specifics for your situation — but assume the clock is running on all that could apply.

REGIME	DEADLINE	WHO YOU NOTIFY
India — CERT-In Directions 2022	**Within 6 hours of noticing a covered incident**	The Indian Computer Emergency Response Team (CERT-In).
EU / UK — GDPR Article 33	**Within 72 hours**	The relevant supervisory authority.
India — DPDP Act	**On becoming aware**	The Data Protection Board of India and each affected data principal.
US — HIPAA Breach Notification Rule	**Affected individuals without unreasonable delay, and no later than 60 days**	Affected individuals; the regulator and, for larger breaches, the media per the rule.
Card data — PCI DSS / card brands	**Promptly, per your acquirer contract**	Your acquiring bank and the relevant card brands.

This table is a planning aid, not legal advice. Exact triggers, thresholds and content requirements vary by regime and by the facts of the incident. Confirm your obligations with counsel.

First-hour actions

Move on these in parallel, not in sequence. The aim of the first hour is to stop the bleeding and preserve the truth — not to assign blame or write the press release.

- [ ] **Contain.** Isolate affected systems and accounts to stop the incident spreading — but do it in a way that preserves evidence rather than destroying it.
- [ ] **Preserve logs and evidence.** Capture and protect relevant logs, snapshots and artefacts before they roll over or are overwritten. Note times in a single time zone.
- [ ] **Assemble the response team.** Activate your incident roster — security, legal, leadership, communications and the relevant system owners — through a known, out-of-band channel.
- [ ] **Start the assessment.** Begin establishing what happened, what data and systems are involved, and who is affected, recording facts and timestamps as you go.
- [ ] **Open the incident record.** Start a single, timestamped log of decisions and actions from the first minute — it becomes your evidence and your timeline.

Who does what

Assign these roles to named people now, while it is calm. In the moment, ambiguity costs hours you do not have.

SEVERITY

Who assesses severity. One named owner classifies the incident, sizes the scope and confirms whether a reportable threshold is met.

DECISION

Who decides to report. A named decision-maker (with legal input) makes the call on each notification and owns the deadline.

DRAFTING

Who drafts the notification. One owner prepares the regulator and individual notices against pre-agreed templates.

COMMUNICATIONS

Who communicates. A single voice handles customers, staff and the public so messages stay consistent and accurate.

Decide in advance

The deadlines above are effectively unwinnable if you improvise. Six hours is not enough time to first locate your CERT-In contact, agree who has authority to report, and draft a notice from a blank page. The work that wins these deadlines is done before the incident, not during it.

Settle these while it is calm

- [ ] Name the people who hold each role above, with named backups, and keep the roster reachable out-of-band.
- [ ] Pre-write notification templates for each regime that could apply to you.
- [ ] Know exactly where and how you report to each authority — and have the contacts saved.
- [ ] Agree your severity thresholds in advance, so classification is a quick decision, not a debate.
- [ ] Run a tabletop exercise so the team has walked the path at least once before it is real.

Build the plan before you need it.

Tranquility Cybersecurity helps teams stand up incident-response plans, notification templates and tabletop exercises that hold up under a real deadline. Start at **tcsa.in**.