KRYNTHNODE



Cybersecurity and digital risk | Report

The six-hour clock

Building an incident response playbook for CERT-In reporting

Published 15 September 2026
Krynthnode Research and Advisory LLP | krynthnode.com

Research that shows its working.

Executive summary

Since April 2022, organisations covered by CERT-In's directions have had to report specified cyber security incidents within six hours of noticing them, or of being informed about them. Six hours is very little time. It is often not enough to understand what has happened, let alone to convene the people who should decide whether and how to report.

This report sets out a playbook that makes the six-hour clock manageable. The central idea is simple: decide in advance who decides, what is reportable, and what information will be sent, so that the hours after detection are spent on facts rather than on process. The same playbook can serve breach notification under the DPDP Act and sector regulators' reporting requirements.

Key findings	Confidence
The six-hour window starts when an incident is noticed or reported, not when it is fully understood. Organisations should plan to report on initial information and update later.	High confidence
Pre-agreed decision rights are the single most important factor in meeting short reporting windows; assembling a decision group after detection routinely consumes most of the available time.	Moderate confidence
The log retention and clock synchronisation requirements are prerequisites for effective investigation, not just compliance obligations.	High confidence
A single, joined-up playbook covering CERT-In, DPDP and sector regulators reduces the risk of inconsistent or late notifications.	Moderate confidence

Each finding is graded in the Krynthnode confidence ledger. See the methodology at the end of this report.

What we recommend

1. Name a primary and a deputy person authorised to decide whether an incident is reportable, available at all hours.
2. Pre-draft the report template with the information CERT-In requests, so that only incident facts need adding.
3. Confirm that logs are kept for a rolling 180 days within India and that system clocks are synchronised as specified.
4. Rehearse the full reporting path at least twice a year, including outside business hours.

© 2026 Krynthnode Research and Advisory LLP. All rights reserved.

What the directions require

CERT-In issued the directions under sub-section (6) of section 70B of the Information Technology Act, 2000. They apply broadly, to service providers, intermediaries, data centres, body corporates and government organisations. The main requirements are:

- Report the types of cyber incidents listed in the directions within six hours of noticing them or being informed about them.
- Designate a point of contact to interface with CERT-In, and share their details.
- Connect to and synchronise ICT system clocks with the Network Time Protocol servers of the National Informatics Centre or the National Physical Laboratory, or with servers traceable to them.
- Enable logs of all ICT systems and maintain them securely for a rolling period of 180 days within Indian jurisdiction, providing them to CERT-In when required.
- Additional record-keeping obligations apply to data centres, virtual private server and cloud providers, VPN service providers, and virtual asset service providers.

The list of reportable incidents is wide. It includes targeted scanning of critical networks, compromise of critical systems or information, unauthorised access to IT systems and data, defacement, malicious code attacks including ransomware, attacks on servers, identity theft and phishing, data breaches and data leaks, and attacks on internet of things devices, among others.

Why six hours is hard

In the first hours of an incident, facts are incomplete and change quickly. Security teams are focused on containment. Legal, communications and executive stakeholders need to be informed. In many organisations, nobody is explicitly authorised to decide that an incident is reportable, so the decision waits for a meeting that takes hours to arrange.

CERT-In's published frequently asked questions acknowledge that initial information may be limited, and that organisations can report what is known and provide further details later. The practical implication is that the playbook should aim for a timely initial report, not a complete one.

The playbook

Time from detection	Activity	Owner
0 to 30 minutes	Triage: is this a potential incident of a reportable type? Open an incident record and start the clock.	Security operations
30 to 90 minutes	Decision: the authorised decision-maker confirms reportability on current facts.	Named decision-maker
90 minutes to 4 hours	Prepare the initial report from the pre-drafted template; legal review focused on accuracy.	Incident lead, legal

© 2026 Krynthnode Research and Advisory LLP. All rights reserved.

Time from detection	Activity	Owner
Within 6 hours	Submit the initial report to CERT-In; record the time and reference.	Point of contact
Following days	Provide updates; assess DPDP breach notification and sector reporting; preserve evidence.	Incident lead, privacy, legal

The durations leave a margin. The aim is to submit well within the window, because late detection of the incident's scope, overnight timing or holiday staffing can all compress the available time.

Connecting CERT-In, DPDP and sector reporting

A single incident can trigger several obligations. A ransomware attack that exposes customer records may require a CERT-In report within six hours, notification of the Data Protection Board and affected individuals under the DPDP Act, and reports to a sector regulator. Regulated entities in the securities market, for example, must also follow SEBI's Cybersecurity and Cyber Resilience Framework.

Rather than maintaining separate procedures, build one playbook with a decision table that shows, for each incident type, which notifications apply, to whom, and by when. Assign one person to coordinate all external notifications so that the facts reported are consistent.

Preparing before the incident

- Confirm log coverage and 180-day retention for all ICT systems, including cloud services and outsourced operations.
- Verify clock synchronisation, since inconsistent timestamps can make investigations unreliable.
- Agree with managed security providers and cloud providers how quickly they will inform you of incidents in your environment.
- Keep an up-to-date contact list for CERT-In, regulators, legal counsel, insurers and forensic support.
- Run tabletop exercises that include the reporting decision, not just technical containment.

© 2026 Krynthnode Research and Advisory LLP. All rights reserved.

Methodology and the confidence ledger

This report is based on CERT-In's directions and published frequently asked questions, the Digital Personal Data Protection Act, NIST incident response guidance and established practice. It is not legal advice; confirm the obligations that apply to your organisation with counsel.

Grade	What it means	How to use it
High confidence	Consistent across several independent sources and established practice.	Suitable for committing budget.
Moderate confidence	Supported, with some gaps or variation between contexts.	Suitable for a pilot with a review date.
Emerging evidence	Limited or recent evidence.	Worth monitoring before acting.

References

1. Indian Computer Emergency Response Team (CERT-In). Directions under sub-section (6) of section 70B of the Information Technology Act, 2000. 28 April 2022.
2. Indian Computer Emergency Response Team (CERT-In). Frequently Asked Questions on Cyber Security Directions of 28 April 2022. May 2022.
3. Government of India. The Digital Personal Data Protection Act, 2023.
4. National Institute of Standards and Technology. SP 800-61 Revision 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management. April 2025.
5. Securities and Exchange Board of India. Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities. August 2024.

About Krynthnode

Krynthnode Research and Advisory LLP is an independent technology and cybersecurity research and advisory firm. We help leaders make decisions they can defend: every finding we publish carries its evidence, its sources and an honest rating of how sure we are. We do not sell technology, take referral fees or accept payment for ratings.

To discuss this research with the analyst team, visit krynthnode.com/contact or email hello@krynthnode.com.

This publication reflects the views of Krynthnode analysts based on the sources available at the time of writing. It is provided for information and is not legal, regulatory, financial or investment advice. Mention of any organisation, product or standard is not an endorsement. Trademarks belong to their respective owners. No part of this publication may be reproduced or redistributed without written permission, except for short quotations with attribution.