

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

The Missing Six Hours: CERT-In Incident Reporting, Digital Evidence, and India's Cyber Forensics Gap

ANWESH BHOWMICK*, DHURUV GANDHI**, AND SREEKAR POTARAJU***

ABSTRACT

Cyberattacks are often discovered after a delay. A company may first notice an unusual login, a suspicious transaction, an encrypted server, or a customer complaint. At that stage, the organisation may not know whether it has suffered a minor technical fault or a major cyber incident. India's Computer Emergency Response Team (CERT-In) Directions of 2022 require service providers, intermediaries, data centres, body corporates, and government organisations to report specified cyber incidents within six hours of noticing them or being brought to notice of them. This paper examines a narrow but important cyber-law issue: the gap between rapid incident reporting and reliable digital forensics. The six-hour rule is intended to make India's cyber response faster. It allows CERT-In to understand threats, issue warnings, coordinate response, and reduce harm. However, a rushed report may be incomplete or inaccurate, and a rushed response may unintentionally destroy evidence. At the same time, the 180-day log-retention rule may be insufficient for cyber incidents that are discovered months after an attacker first entered a system. The problem becomes more serious where data is stored across cloud services, outsourced vendors, foreign servers, and multiple internal systems. This paper argues that India needs a more structured cyber-incident evidence framework. The law should distinguish between an initial alert and a complete forensic report. It should require preservation of evidence immediately after notice of a suspected incident, standardise the minimum contents of a six-hour report, extend retention for high-risk sectors, clarify the duties of cloud and managed-security vendors, and protect good-faith early reporting from being treated as an admission of legal liability. These reforms would preserve the speed of CERT-In reporting while improving the quality of cyber investigation, victim protection, and criminal prosecution.

Keywords: CERT-In, cyber incident reporting, digital forensics, log retention

I. INTRODUCTION

A cyberattack does not always begin with an obvious warning. An attacker may enter a system through a stolen password, an insecure application, a phishing email, a cloud misconfiguration,

* Author is a Student at National Law Institute University, Bhopal, Madhya Pradesh, India.

** Author is a Student at National Law Institute University, Bhopal, Madhya Pradesh, India.

*** Author is a Student at National Law Institute University, Bhopal, Madhya Pradesh, India.

or a compromised vendor account. The attacker may remain hidden for days or months. During this period, the intruder may copy data, move within the network, change access permissions, install malicious software, or prepare for ransomware.

When an organisation finally discovers suspicious activity, time becomes extremely important. It must stop the attack, protect systems, preserve evidence, notify customers where needed, contact law-enforcement agencies, and comply with regulatory reporting duties. These duties can be difficult to reconcile. An organisation that disconnects a server too quickly may destroy volatile evidence. An organisation that waits too long to verify every fact may fail to report an incident within the required time.

India's CERT-In Directions, issued under section 70B(6) of the Information Technology Act, 2000, seek to address the need for fast reporting. The Directions require service providers, intermediaries, data centres, body corporates, and government organisations to report specified cyber incidents to CERT-In within six hours of noticing the incident or being brought to notice of it.¹ They also require these entities to enable logs of all their information and communication technology (ICT) systems and to retain them securely for a rolling period of 180 days within Indian jurisdiction.²

The purpose of the six-hour rule is understandable. CERT-In is India's national agency for responding to computer-security incidents. Rapid reporting can help the Government identify patterns, warn other organisations, coordinate technical responses, and reduce the spread of a cyberattack. A delayed report may allow the same attacker or malware to harm many more victims.

However, cyber incident reporting is not only a compliance formality. The first few hours after discovery may determine whether investigators can identify the attacker, establish the time of intrusion, recover stolen data, trace a money trail, and prove a criminal offence. This makes digital forensics central to cyber law.

This paper identifies a niche issue: the missing six hours. The phrase does not suggest that the reporting rule should be removed. It highlights the absence of a detailed legal method for preserving digital evidence while organisations report quickly. The present rule states when to

¹ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 70B(6) (India); INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT-IN), MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, *Directions under Sub-section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet*, No. 20(3)/2022-CERT-In, cl. (ii) (Apr. 28, 2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf [hereinafter CERT-In Directions].

² CERT-In Directions, *supra* note 1, cl. (iv).

report, but it does not fully explain what an organisation must preserve, how it should preserve it, what preliminary information is sufficient, how third-party cloud vendors should cooperate, or how early uncertainty should be recorded.

The central argument is that India should adopt a two-stage reporting model. An organisation should send an initial alert within six hours, based on reasonably available information. It should then submit a fuller forensic report after technical investigation. At the same time, it should immediately preserve relevant logs, devices, cloud records, communications, and access data. Such a model would make the law both faster and more reliable.

II. CERT-IN AND THE 2022 DIRECTIONS

A. CERT-In's statutory role

CERT-In is the agency appointed by the Central Government under section 70B(1) of the Information Technology Act, 2000, and it serves as the national agency for performing functions in the area of cyber security. Its functions include the collection, analysis, and dissemination of information on cyber incidents; forecasts and alerts of cyber-security incidents; emergency measures for handling such incidents; coordination of response activities; the issue of guidelines, advisories, vulnerability notes, and white papers on information-security practices and the reporting of cyber incidents; and such other functions relating to cyber security as may be prescribed.³

Cybersecurity is a collective problem. A phishing campaign, ransomware group, software vulnerability, or botnet may attack many organisations at the same time. If one organisation discovers the threat but does not report it, other organisations may remain exposed. CERT-In is intended to act as a central point for information sharing and national response.⁴

Section 70B(6) permits CERT-In to call for information and give directions to service providers, intermediaries, data centres, body corporate, and any other person. Failure to provide the information called for, or to comply with a direction issued under section 70B(6), is punishable under section 70B(7).⁵ The legal power behind the 2022 Directions is therefore significant.

³ Information Technology Act, 2000, § 70B(1), (4).

⁴ Press Release, MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, *CERT-In Issues Directions Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet* (Apr. 28, 2022), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1820904>.

⁵ Information Technology Act, 2000, § 70B(6)–(7).

B. The six-hour reporting obligation

The Directions state that covered entities must report the cyber incidents listed in Annexure I within six hours of noticing the incident or being brought to notice about it. The report may be made through the methods notified by CERT-In.⁶

The reportable incidents include targeted scanning or probing of critical networks or systems, compromise of critical systems or information, unauthorised access to IT systems or data, defacement of or intrusion into websites, malicious-code attacks including ransomware, attacks on critical infrastructure and operational-technology systems, identity theft, spoofing and phishing attacks, data breaches and data leaks, attacks through malicious mobile applications, attacks affecting cloud computing systems, and other specified categories.⁷

The phrase “noticing such incidents or being brought to notice” is deliberately broad. It does not require an organisation to wait until every technical fact is confirmed. This approach is useful because cyberattacks develop quickly. A requirement of complete certainty could encourage organisations to delay reporting.

Yet the phrase also creates uncertainty. A company may receive a customer complaint about fraud, an automated security alert, a claim by a ransomware group, or a media report about leaked data. It may not know whether the claim is true. If every unverified alert is treated as a confirmed incident, organisations may flood CERT-In with incomplete reports. If organisations wait for confirmation, they may breach the six-hour rule.

C. Log-retention obligation

The Directions require covered entities to enable logs of all their ICT systems and to maintain them securely for a rolling period of 180 days within Indian jurisdiction. The logs must be provided to CERT-In along with the report of an incident or whenever CERT-In so directs.⁸

Logs are digital records created by systems, applications, networks, and security tools. They can show who accessed a system, when an account logged in, which IP address was used, what files were accessed, whether an administrator changed permissions, and whether unusual traffic occurred.

Logs are often the foundation of cyber investigation. Without them, an organisation may know that an incident occurred but may not be able to establish how it happened or what data was

⁶ CERT-In Directions, *supra* note 1, cl. (ii).

⁷ *Id.* annex I; *see also* The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, r. 12(1)(a), G.S.R. 20(E) (Jan. 16, 2014) (India).

⁸ CERT-In Directions, *supra* note 1, cl. (iv).

affected. Log retention is therefore not merely a technical compliance requirement. It is a form of evidence preservation.

The Directions also create specific customer-record obligations for data centres, virtual private server providers, cloud-service providers, and virtual private network service providers. These entities must register specified customer information and maintain it for five years, or for any longer period mandated by law, after any cancellation or withdrawal of the registration.⁹ This information can help investigators connect online activity to a subscriber or account.

III. WHY DIGITAL FORENSICS MATTERS

Digital forensics is the process of collecting, preserving, examining, and presenting electronic evidence. In a cyber incident, it may involve system logs, firewall records, server images, email headers, endpoint data, cloud audit trails, access credentials, mobile-device information, payment records, malware samples, and backup files.

Forensics serves several purposes. First, it helps stop the incident. Investigators may identify the compromised account, vulnerable system, or malicious software. Second, it helps determine the scope of harm. An organisation may need to know whether attackers accessed customer data, source code, financial records, or internal communications. Third, it supports legal action. Law-enforcement agencies may need reliable evidence to identify and prosecute offenders. Fourth, it helps the organisation improve future security.

The first hours after discovery are often the most valuable. Some evidence is volatile. Memory contents may disappear when a machine is restarted. Network connections may end. Temporary cloud logs may be overwritten. Attackers may delete files or clear logs after detecting that they have been discovered. An organisation responding to an incident must therefore preserve evidence before making major changes to the affected system.

This does not mean that organisations should keep infected systems running. They may need to isolate a device quickly to stop further harm. But isolation should be carried out in a way that records what was done, when it was done, and by whom. A forensic image or snapshot should be created where reasonably possible. The principle is simple: contain the incident, but do not unnecessarily destroy the evidence needed to understand it.

Indian law recognises the importance of electronic records. The Bharatiya Sakshya Adhiniyam, 2023 contains rules on electronic and digital records and their evidentiary use.¹⁰ A digital record

⁹ *Id.* cl. (v).

¹⁰ The Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023, §§ 57–63 (India).

may be relevant, but its value depends on authenticity, integrity, and the ability to explain how it was collected. Poor preservation can make electronic evidence difficult to use in court.

IV. THE GAP BETWEEN REPORTING AND EVIDENCE PRESERVATION

A. Initial notice is not a final conclusion

The six-hour rule is designed for early notice. It should not be treated as a requirement to produce a complete forensic conclusion within six hours. In many incidents, the organisation will not know the full facts at the beginning. It may know only that a ransomware note has appeared, a database is behaving strangely, a customer account has been misused, or a security tool has flagged unauthorised access.

A legal framework should expressly distinguish an initial report from a final incident report. The initial report should state the facts then known, the date and time of discovery, the systems potentially affected, immediate containment measures, and a contact point. It should also say clearly that investigation is ongoing.

A later report should include the probable cause, the scope of systems affected, the data categories involved, attacker indicators, forensic findings, remediation measures, and information about any affected persons or public harm. This later report can be more accurate because it is based on investigation rather than immediate suspicion.

Without this distinction, organisations may take one of two harmful approaches. They may rush to make definite statements that later prove false. Or they may delay reporting until they have complete information. Both outcomes weaken cyber response.

B. The 180-day retention problem

The requirement to retain logs for 180 days is an important baseline. However, many sophisticated intrusions are discovered after more than six months. An attacker may obtain access through a stolen credential, remain inactive, and later use the access for data theft or ransomware. If the original entry occurred before the 180-day period, critical evidence may no longer exist.

The answer is not necessarily to require every small organisation to retain all logs indefinitely. That would be expensive and may create additional privacy and security risks. But high-risk sectors should retain important security logs for longer periods. Banks, payment systems, telecommunications providers, health-data systems, government platforms, critical infrastructure, large cloud providers, and major online marketplaces may need a longer period because the impact of an incident can be much greater.

The law should also distinguish between ordinary application logs and security-critical logs. Authentication records, administrator actions, cloud audit logs, data-exfiltration alerts, access-control changes, security-event records, and backup logs may be especially valuable. A risk-based retention rule would be more practical than one uniform period for every type of log.¹¹

C. Cloud and vendor dependence

Many organisations do not operate all their systems themselves. They use cloud storage, software-as-a-service tools, external payment processors, managed security providers, email platforms, customer-support systems, and outsourced IT vendors. A cyber incident may involve records held by several entities in different countries.

The organisation that discovers an incident may not directly control the most useful evidence. A cloud provider may hold access logs. A managed-security vendor may hold detection alerts. An email provider may hold message headers. A payment processor may hold transaction data. If contracts do not require timely assistance, the organisation may be unable to meet the reporting duty or to investigate properly.

The 2022 Directions cover data centres, cloud providers, and other service providers in specified ways.¹² However, the legal framework should more clearly require cooperation in evidence preservation. A service agreement should state who controls logs, how quickly evidence must be preserved, whether forensic snapshots can be taken, and how the customer can obtain incident data.

D. Reporting and self-incrimination concerns

An organisation may fear that an early report will be treated as an admission that it failed to maintain adequate security. This fear can encourage under-reporting or delayed reporting. The law should encourage truthful early alerts without making every preliminary statement conclusive proof of civil, regulatory, or criminal liability.

A good-faith initial report should be treated as a security notification, not as a final legal admission. This does not protect organisations that knowingly conceal information or make false statements. It simply recognises that the first hours of an incident involve uncertainty. Regulators should reward prompt cooperation and accurate updating, rather than punish an organisation merely because its first technical assessment changes after forensic investigation.

¹¹ Neeti Biyani, Andrei Robachevsky & Prateek Waghre, INTERNET SOCIETY, *Internet Impact Brief: India CERT-In Cybersecurity Directions 2022*, at 5–6 (June 1, 2022), <https://www.internetsociety.org/wp-content/uploads/2022/06/IIB-India-CERT-In-Directions-2022.pdf>.

¹² CERT-In Directions, *supra* note 1, cls. (iv)–(v).

V. THE RELATIONSHIP WITH DATA-PROTECTION LAW

Cyber incidents often involve personal data. If an attacker accesses names, phone numbers, passwords, financial information, health records, or identity documents, the incident may also become a data-protection breach.

The Digital Personal Data Protection Act, 2023 requires a Data Fiduciary to take reasonable security safeguards to prevent personal-data breaches. It also requires intimation of a personal-data breach to the Data Protection Board and to each affected Data Principal in the prescribed form and manner.¹³ The Digital Personal Data Protection Rules, 2025 provide further rules on reasonable security safeguards and breach intimation: Rule 6 includes a duty to retain logs for one year, and Rule 7 requires a description of the breach to be sent to the Board without delay, followed within seventy-two hours (or such longer period as the Board allows) by detailed information. These rules, and section 8 of the Act itself, form part of a phased commencement and come into force eighteen months after notification in November 2025.¹⁴

This creates multiple compliance obligations. A covered organisation may need to report a cyber incident to CERT-In within six hours. It may also need to notify the Data Protection Board and affected individuals under the data-protection framework. In addition, banks, insurers, listed companies, telecom companies, or other regulated entities may have sector-specific reporting duties.

Multiple reporting duties can improve accountability, but they can also create confusion. Different regulators may require different information, different timelines, and different definitions of an incident. An organisation dealing with a live attack may spend valuable time completing separate forms instead of containing the breach.

India needs a coordinated reporting architecture. CERT-In should remain the national technical-response body. The Data Protection Board should focus on the personal-data consequences and the affected Data Principals' rights. Sectoral regulators should focus on sector-specific safety and financial stability. These authorities should share relevant information through a structured system so that organisations do not have to repeat identical technical facts unnecessarily.

¹³ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, § 8(5)–(6) (India).

¹⁴ The Digital Personal Data Protection Rules, 2025, rr. 1(4), 6–7, G.S.R. 846(E) (Nov. 13, 2025) (India); MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, Notification G.S.R. 843(E), cl. (c) (Nov. 13, 2025) (India), <https://www.meity.gov.in/static/uploads/2025/11/c56ceae6c383460ca69577428d36828b.pdf>; see also PRESS INFORMATION BUREAU, *DPDP Rules, 2025 Notified: A Citizen-Centric Framework for Privacy Protection and Responsible Data Use* (Nov. 17, 2025), <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf>.

VI. A TWO-STAGE CYBER INCIDENT MODEL

India should retain the six-hour reporting rule but clarify its operation. The first stage should be an initial incident alert. It should be submitted within six hours of noticing or being informed of a reportable incident. The alert should contain only information reasonably available at that time.

The initial alert should include the organisation's identity, contact officer, time of discovery, nature of the suspected incident, affected systems if known, immediate containment steps, and whether personal data, critical services, financial systems, or public safety may be affected. The organisation should be allowed to state that the information is preliminary and subject to forensic investigation.

The second stage should be a forensic update report. The deadline can depend on the severity of the incident, but the report should generally follow after the organisation has conducted a reasonable investigation. It should include the likely attack method, confirmed systems affected, data involved, duration of unauthorised access, attacker indicators, remedial steps, and updates given to affected persons and other regulators.

This model would preserve the value of rapid notification while avoiding the unrealistic expectation that all facts can be known within six hours. It would also create a clear record of how the organisation's understanding developed over time.

The law should add an explicit preservation duty. On noticing a reportable incident, an organisation should take reasonable steps to preserve relevant evidence. These steps may include securing logs, taking snapshots of affected cloud systems, preserving endpoint images, retaining relevant communications, recording the chain of custody, and preventing automatic deletion or overwriting of evidence.

The preservation duty should be proportionate. A small business may not have the same forensic capacity as a large bank or cloud provider. But every organisation can be required to avoid intentional deletion, keep available logs secure, and seek professional support where the incident is serious.

VII. REFORM PROPOSALS

The first reform should be a CERT-In standard form for six-hour alerts. The form should be short and practical. It should distinguish confirmed facts from suspected facts. It should allow the reporter to classify the incident by urgency and to identify whether external assistance is needed.

The second reform should be mandatory evidence-preservation guidance. CERT-In should publish a simple incident-response protocol explaining how to isolate systems, preserve logs, retain cloud records, take forensic images, document actions, and communicate with law enforcement. The protocol should be adapted for small entities, large enterprises, critical infrastructure, and cloud providers.

The third reform should be risk-based log retention. The 180-day rule should remain the minimum baseline, but high-risk sectors should retain specified security logs for longer periods. This may include authentication logs, administrator records, cloud audit trails, data-exfiltration alerts, and critical-system event logs. Longer retention should be accompanied by encryption, access control, and retention limits to protect privacy.

The fourth reform should require cyber-evidence clauses in important service contracts. Cloud providers, data centres, managed-security service providers, software-as-a-service platforms, and payment vendors should be contractually required to preserve and provide relevant incident records quickly. An organisation cannot meet its legal duties if its suppliers refuse or delay access to essential evidence.

The fifth reform should coordinate reporting between CERT-In and the data-protection framework. A single technical incident number could be issued by CERT-In. The organisation could then use that number in its Data Protection Board and sectoral notifications. This would reduce duplication and improve the Government's understanding of major incidents.

The sixth reform should protect good-faith preliminary reporting. An early report should not be treated as a final admission of negligence solely because later forensic analysis changes some facts. The organisation should remain liable for concealment, false reporting, or unreasonable security failures. But the law should not create a disincentive to immediate cooperation.

VIII. CONCLUSION

India's six-hour CERT-In reporting obligation is an important cybersecurity measure. It recognises that cyber incidents can spread rapidly and that national response requires early information. The 180-day log-retention rule is also valuable because digital logs are essential for identifying attackers, understanding the extent of harm, and improving future security.¹⁵

However, the existing framework leaves an important gap between urgent reporting and reliable forensic investigation. An organisation may not know the full facts within six hours. It may depend on cloud providers and external vendors for evidence. It may lose critical logs before

¹⁵ CERT-In Directions, *supra* note 1, cls. (ii), (iv).

discovering a long-running intrusion. It may also face multiple overlapping reporting duties under cybersecurity, data-protection, and sector-specific law.

The answer is not to weaken rapid reporting. The answer is to make it more realistic and more useful. India should adopt a two-stage model: an initial alert within six hours and a fuller forensic report after reasonable investigation. It should add a clear duty to preserve evidence, establish risk-based log retention, require vendor cooperation, coordinate regulatory reporting, and protect good-faith preliminary disclosure.

The larger lesson is simple. Cybersecurity law should not treat reporting as a box-ticking exercise. A report is valuable only if it helps stop the attack, preserve the evidence, protect victims, and support a lawful investigation. In cyber incidents, the first six hours should not become the six hours in which the most important evidence disappears.
