



The India CISO Incident Response Playbook

CERT-In And DPDP Ready In The First Six Hours

An Operational Framework For Indian Enterprises

Authored by: Proactive Data Systems, A Cisco Preferred Security Partner

Research Edition: February 2026

Audience: CISOs, CROs, Legal Counsel, and Security Operations Leaders

DISCLOSURE

- This white paper was authored by Proactive, a Cisco Preferred Security Partner.
- Research content, frameworks, and operational recommendations have been developed independently.
- Product information appears only in the clearly labelled appendix.
- Readers should evaluate recommendations in the context of their own enterprise risk profiles.

CERT-In And DPDP Ready In The First Six Hours

The India CISO Incident Response Playbook

Table of Contents

FRONT MATTER

Sponsorship Disclosure	
How To Use This Playbook	5

PART ONE — THE REGULATORY AND FINANCIAL CASE

Executive Context	6
Regulatory landscape: CERT-In and DPDP	
Key data: IBM and Verizon benchmarks	
Detection latency as a financial multiplier	

PART TWO — THE SIX-HOUR ASSURANCE MODEL

The Six-Hour Assurance Model	7
Dimension 1: Signal Integrity	8
Dimension 2: Classification Discipline	8
Dimension 3: Escalation Certainty	8
Dimension 4: Evidence Defensibility	8
Relationship to ISO 27035 and NIST CSF	9
Why Most Indian Enterprises Miss The Six-Hour Window	9
Illustrative scenario: A Mumbai NBFC	10
Failure Pattern 1: Identity logs incomplete or inaccessible	10
Failure Pattern 2: Severity classification is unclear	10
Failure Pattern 3: Reporting ownership is ambiguous	11
Failure Pattern 4: Evidence capture is informal	11

The First Six Hours Operating Model	11
Operating benchmarks (time targets by step)	12

PART THREE — REGULATORY AND DECISION FRAMEWORKS

Regulatory Requirements, Translated Into Operations	13
CERT-In: The six-hour reporting obligation	14
Regulatory ambiguity: Four grey areas to pre-interpret	14
DPDP Act, 2023: Personal data breach obligations	15
Decision Models And Evidence Standards	16
CERT-In reportability decision logic	16
Severity and regulatory linkage matrix	17
Evidence readiness standard	18
Financial impact model: The cost of detection delay	19

PART FOUR — SECTOR OVERLAYS AND GOVERNANCE

Sector Overlays	19
Banking, Financial Services, and Insurance (BFSI)	20
Manufacturing and Industrial	21
Information Technology and IT-Enabled Services (IT/ITeS)	22
Governance And Board Exposure	23
Three questions boards ask after an incident	23
Governance safeguards	23
Readiness scorecard: Four-level maturity model	24

PART FIVE — IMPLEMENTATION

90-Day Readiness Roadmap	25
Days 1–30: Foundation	26
Days 31–60: Build and rehearse	26
Days 61–90: Simulate, measure, present	26
Architecture-To-Outcome Mapping	27
Control domain prioritisation table	27
Adversary behaviour implications	28

REFERENCE MATERIAL

Glossary	29
Closing	31
Appendix: About The Sponsor	32
Sources	33

FIGURES AND INFOGRAPHICS

Figure 1: The Six-Hour Assurance Model

Figure 2: First Six Hours Operational Flow

Figure 3: Detection Delay Cost Escalation

Note on Page Numbers

Page references are approximate and reflect the document as typeset in Microsoft Word at standard zoom. Page counts may vary slightly depending on your viewing application, display settings, and font rendering. The Figures section at the end of this contents page cross-references the three embedded infographics.

How To Use This Playbook

This playbook is written for three primary reader groups. Knowing which group you are in will help you navigate it efficiently.

Reader	Primary Focus	Recommended Sections
CISO / Head of Security	Framework ownership, readiness posture, board reporting	All sections
Legal Counsel / Compliance	CERT-In and DPDP obligations, regulatory ambiguity, evidence chain	Executive Context, Regulatory Requirements, Governance
SOC Lead / IR Manager	Detection benchmarks, severity matrix, evidence protocols	Six-Hour Operating Model, Severity Matrix, Evidence Readiness

The playbook is structured in three parts. Part One (Executive Context) establishes the regulatory and financial case for readiness. Part Two (The Operating Model) is the operational core — the Six-Hour Assurance Model and its constituent elements. Part Three (Sector and Governance Lenses) applies the framework to specific industries and board-level considerations.

Terminology used in this playbook is defined in the Glossary at the end of the document. References appear in the Sources section.

Executive Context

The regulatory and financial imperative for six-hour readiness

India's regulatory posture has tightened materially. CERT-In's Directions of April 2022 mandate reporting of specified cyber incidents within six hours of detection or awareness. The Digital Personal Data Protection (DPDP) Act, 2023, introduces structured obligations for breach assessment and intimation where personal data is implicated. Taken together, these two frameworks create one of the most operationally demanding incident response environments in the Asia-Pacific region.

Industry data reinforces the urgency of readiness.

Data Point	Figure	Source
Average cost of a data breach in India, 2024	INR 195 million	IBM Cost of a Data Breach Report 2024, India segment
Average cost of a data breach in India, 2025	INR 220 million	IBM Cost of a Data Breach Report 2025, India segment
Year-on-year cost increase	INR 25 million (+13%)	IBM 2024–2025 comparative
Proportion of breaches involving the human element	~68% globally (India approximates global trend)	Verizon DBIR 2025
Third-party involvement in breaches	~30% of cases globally	Verizon DBIR 2025

***Note on Verizon figures:** India-specific breakdowns are not published separately in the DBIR. Global figures are cited as directional context. Organisations should validate against sector-specific experience.*

These numbers carry a direct operational implication. If the average breach cost is INR 220 million and containment delay increases forensic scope, customer notification scale, legal exposure, and downtime, even a 10–15% cost escalation linked to detection latency translates to INR 22–33 million in additional impact per incident. That figure is not a theoretical risk. It is a compounding financial multiplier with a measurable operational cause: delay.

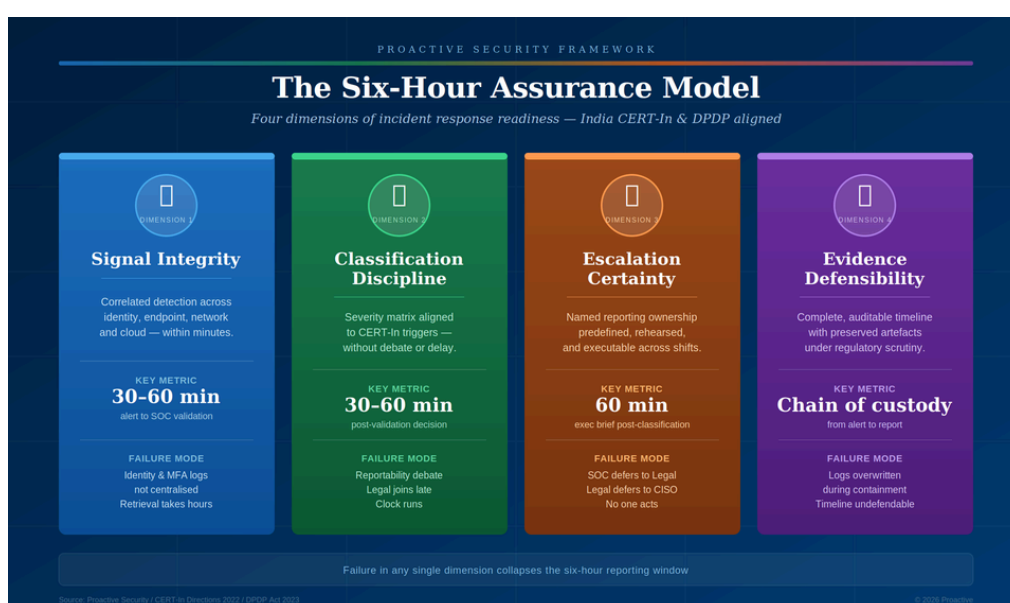
Speed, ownership, and evidence quality determine regulatory posture, financial exposure, and board confidence. This playbook is structured to make all three measurable.

The Six-Hour Assurance Model

A proprietary readiness lens for Indian enterprise incident response

Most Indian enterprises have incident response procedures. Fewer have tested whether those procedures can execute within the CERT-In six-hour window under real conditions. The gap between having a procedure and being able to execute it is the gap this model addresses.

The Six-Hour Assurance Model evaluates readiness across four dimensions. Failure in any single dimension is sufficient to collapse the reporting window.



Dimension 1: Signal Integrity

Can your organisation generate accurate, correlated detection signals across identity, endpoint, network, and cloud within minutes of an anomalous event? Signal integrity is the foundation of everything that follows. Without it, the remaining three dimensions are irrelevant because the incident is not yet known.

The most common failure here is not a lack of detection tools. It is fragmented telemetry. Identity logs stored separately from endpoint logs. MFA records not centralised. Cloud control plane events in a different system from on-premises SIEM. When retrieval requires multiple manual steps across multiple systems, the 30–60 minute validation target becomes unrealistic.

Dimension 2: Classification Discipline

Can your team apply a severity matrix aligned to CERT-In triggers without debate or delay? Classification discipline is operationally distinct from investigation. It answers one question: does this incident meet the threshold for regulatory reporting?

This question must be answerable within 30–60 minutes of validation. When classification requires legal debate or senior leadership approval at each incident, the process becomes dependent on availability, not on pre-established criteria. The severity matrix must pre-empt that dependency by making the classification criteria explicit and agreed in advance.

Dimension 3: Escalation Certainty

Is reporting ownership predefined, rehearsed, and executable across shifts? Escalation certainty is a governance construct. It means that at any hour, on any day, there is one named individual whose role it is to authorise and submit the CERT-In notification.

The failure mode here is structural ambiguity. The SOC assumes Legal will decide. Legal assumes the CISO will escalate. The CISO is not on call. In that structure, the six-hour window passes before a decision is made. Ownership must be documented, tested, and on a rotation schedule.

Dimension 4: Evidence Defensibility

Can your team produce a complete, auditable incident timeline with preserved artefacts under regulatory scrutiny? Evidence defensibility is the standard against which a CERT-In inspection or a post-incident legal challenge will be measured.

The requirement is not perfection of investigation. It is discipline of documentation. Every detection event, every log retrieval, every classification decision, every escalation action, and every reporting submission must carry a timestamp and an accountable name. Chain of custody must be maintained from the moment of detection.

Relationship to ISO 27035 and NIST Frameworks

The Six-Hour Assurance Model is operationally complementary to established frameworks rather than a replacement for them.

ISO 27035 (Information Security Incident Management) provides a five-phase process model (Plan, Detect, Assess, Respond, Learn). The Assurance Model maps most directly to the Detect and Assess phases, adding India-specific regulatory precision that ISO 27035 does not include.

NIST CSF 2.0 Respond and Recover functions address similar terrain at a higher level of abstraction. The Assurance Model provides the specific time targets and ownership structures that NIST does not prescribe.

Organisations already using ISO 27035 or NIST as their base framework can adopt the Six-Hour Assurance Model as a CERT-In compliance layer on top of their existing structure.

Why Most Indian Enterprises Miss The Six-Hour Window

Four structural failure patterns recur across sectors. They are not accidents. They are the predictable consequence of organisations that have invested in detection technology without investing equally in the process and governance infrastructure that converts a detection signal into a defensible regulatory response.

Illustrative Scenario: A Mumbai NBFC

Timestamped Walkthrough

08:40 AM - A privileged account logs in from an unfamiliar geography. The alert triggers in the SIEM but is one among several hundred that shift.

09:55 AM - The SOC validates the alert as a true positive but cannot immediately retrieve historical MFA logs. Log centralisation gaps delay confirmation by over an hour.

10:40 AM - Legal is informed. A debate begins over whether this incident qualifies as reportable under CERT-In's specified categories.

11:20 AM - Evidence of access to a customer data repository emerges, confirming personal data scope.

12:15 PM - Escalation to the CISO occurs. Reporting ownership is still being confirmed.

02:30 PM - An initial report is prepared. The six-hour window has been exhausted.

Assessment: The breach itself may have been limited in scope. The regulatory exposure arose from delay, ambiguity, and log retrieval gaps — not from the severity of the incident.

Failure Pattern 1: Identity Logs Are Incomplete Or Inaccessible

Critical identity and MFA logs are not centralised in a single, queryable repository. Retrieval requires manual intervention across multiple systems. The 15–30 minute log retrieval target becomes impossible. Signal integrity fails in the first hour, setting off a cascade of delays in every subsequent step.

Failure Pattern 2: Severity Classification Is Unclear

The severity matrix does not exist, is not rehearsed, or does not clearly map to CERT-In's specified incident categories. Teams spend time in classification debate rather than in classification execution. Legal involvement at this stage, which is appropriate for advice, becomes a blocker when it is used as a decision gate rather than a validation step.

Failure Pattern 3: Reporting Ownership Is Ambiguous

There is no single named reporting officer accountable for the CERT-In submission decision. The SOC assumes Legal will decide. Legal assumes the CISO will escalate. No pre-agreed rotation schedule exists for out-of-hours incidents. The ownership gap produces inaction, and inaction produces a missed window.

Failure Pattern 4: Evidence Capture Is Informal

Logs are overwritten during containment activity. Artefacts are not timestamped at capture. Investigation actions are not recorded in a centralised incident log. When regulatory scrutiny arrives, timeline reconstruction becomes defensive narration rather than factual documentation. This is the failure pattern that most directly undermines regulatory confidence.

These failures are structural, not accidental. They require structural remediation.

The First Six Hours Operating Model

The operating model translates the Six-Hour Assurance Model into a sequential, time-bound operational flow. Each step requires a named owner and a defined time target. Absence of either is an identified gap requiring remediation.

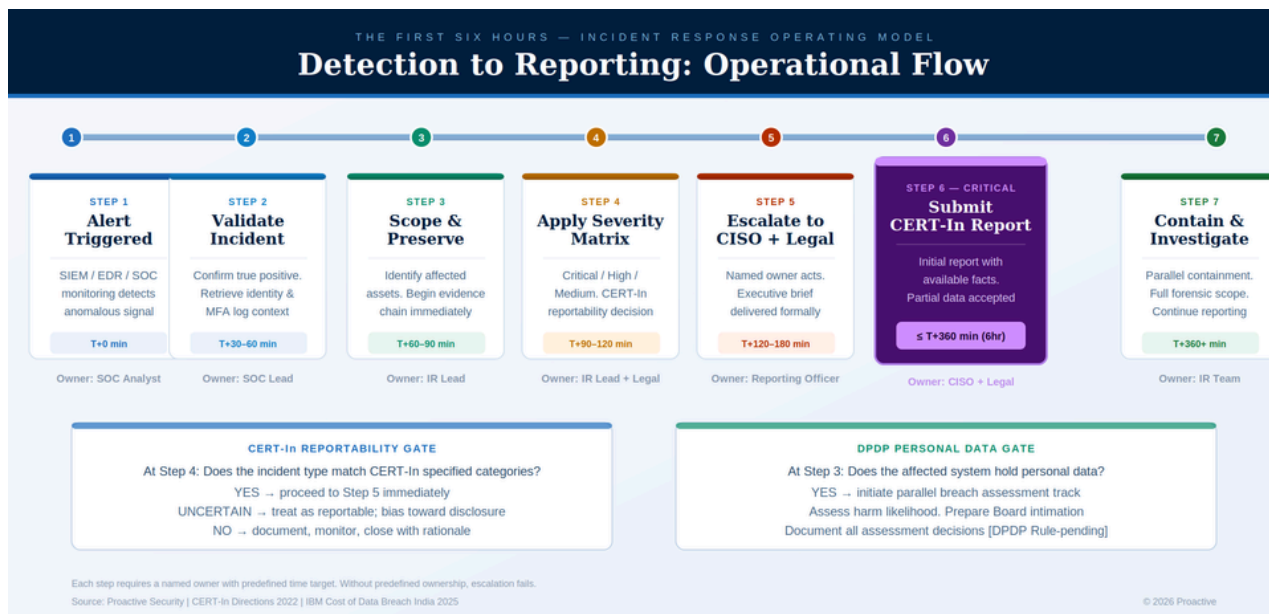


Figure 2: First Six Hours Operational Flow - Detection to Reporting with Regulatory Decision Gates

Operating Benchmarks

The following benchmarks are operational targets, not legal thresholds. They are derived from incident review practice and represent the minimum performance required to reliably meet the CERT-In six-hour deadline under normal enterprise conditions. Organisations operating in high-risk sectors or with complex log environments should target the lower end of each range.

Step	Target Time	Owner Role	Critical Dependency
Detection to SOC validation	30–60 minutes	SOC Analyst / Lead	Centralised identity & MFA logs
Log retrieval for critical systems	15–30 minutes	SOC Lead	SIEM configuration and retention policy
Severity and reportability decision	30–60 min post-validation	IR Lead + Legal	Pre-agreed severity matrix
Executive brief delivery	Within 60 min of classification	Reporting Officer	Named owner with out-of-hours access
CERT-In initial submission	Within 6 hours of detection	CISO / Legal	Pre-built report template, minimum viable dataset

If you cannot measure these benchmarks today, your six-hour readiness is assumed, not confirmed.

Regulatory Requirements, Translated Into Operations

Regulatory text describes obligations. This section translates those obligations into the specific operational actions that satisfy them. CISOs and Legal teams should review this section together.

CERT-In: The Six-Hour Reporting Obligation

Under the CERT-In Directions (April 2022) and associated FAQs, organisations must report specified cyber incidents within six hours of detection or awareness, whichever is earlier. The six-hour clock creates four specific operational requirements:

- Detect and validate incidents continuously, across all material systems
- Decide reportability quickly, using pre-agreed criteria rather than in-flight deliberation
- Submit an initial report with available facts. Completeness is not required at T+6 hours. Submission is.
- Preserve a defensible evidence trail from the moment of detection

Regulatory Ambiguity: Four Grey Areas To Pre-Interpret

WHAT CONSTITUTES "AWARENESS"? If an alert triggers but is not yet validated, does the clock start at signal time or confirmation time? Safeguard: record both timestamps. Maintain alert-to-validation interval metrics. In any regulatory discussion, you will be able to demonstrate diligence regardless of which interpretation prevails.

THIRD-PARTY NOTIFICATION: If a vendor informs you of a compromise affecting your systems, the six-hour clock should be treated as starting at notification time. Safeguard: vendor contracts must include immediate breach notification clauses and evidence-sharing requirements as standard.

PARTIAL FACTS AT REPORTING TIME: CERT-In permits reporting with available information. Waiting for completeness is not a valid reason for delay. Safeguard: define a minimum viable reporting dataset in advance so teams do not hesitate at submission.

INTERNAL DEBATE RISK: Legal review must not stall operational reporting. Safeguard: the severity matrix must define reportability thresholds in advance. Legal's role at the six-hour gate is to validate, not to decide.

DPDP Act, 2023: Personal Data Breach Obligations

The Digital Personal Data Protection Act, 2023 introduces obligations for breach assessment and intimation to the Data Protection Board and affected Data Principals where personal data is involved. The specific timelines and notification formats are subject to rules that were still being notified at the time of publication.

Important Note on DPDP Rule Status

DPDP rules specifying precise notification timelines, formats, and Board procedures were in draft or pending notification at the time this document was prepared (February 2026).

Organisations should treat the posture described here as an operational preparedness standard, not a confirmed legal obligation.

Legal counsel should be engaged to monitor and incorporate final rule notifications as they are published.

The DPDP framework creates five specific operational requirements:

- Confirm personal data presence in affected systems within the initial scope assessment
- Determine evidence of access, disclosure, alteration, loss, or exfiltration
- Assess likelihood of harm to affected Data Principals
- Prepare Board and Data Principal intimation communications where required
- Document all assessment decisions with timestamps and named decision-makers

CERT-In tests speed. DPDP tests judgement and documentation discipline. The Six-Hour Assurance Model's evidence defensibility dimension is the common foundation for both.

Decision Models And Evidence Standards

CERT-In Reportability Decision Logic

Decision Step	Action Required
Confirm validated incident	True positive confirmed. Not a false alarm.
Map to CERT-In categories	Does the incident type appear in CERT-In's specified list? Apply the pre-agreed severity matrix.
Capture minimum viable facts	Affected systems, initial timeline, estimated scope, incident type. Completeness is not required.
Submit initial report within 6 hours	Bias toward reporting when indicators are credible and systems are critical. Do not wait.
Schedule follow-up updates	CERT-In expects updates as the investigation progresses. Build the follow-up cadence into the IR plan.

Severity and Regulatory Linkage Matrix

Severity	Operational Definition	CERT-In Action	DPDP Action
CRITICAL	Confirmed compromise, business disruption, ransomware, or data breach confirmed	Treat as reportable. Submit within 6 hours.	Initiate breach assessment immediately
HIGH	Confirmed intrusion or unauthorised access, partial containment	Assess reportability. Escalate immediately.	Assess personal data exposure scope
MEDIUM	Credible suspicious activity, no confirmed impact	Monitor. Escalate if situation worsens.	Assess if personal data systems are in scope
LOW	Isolated event, no business or data impact confirmed	Document and close with rationale.	Not applicable

This matrix should be reviewed and customised to your enterprise risk profile, sector, and data architecture. Version-control it and re-validate it at least annually or after any significant regulatory development.

Evidence Readiness Standard

Your regulatory defence rests on your evidence chain. Evidence must be captured from the moment of detection, not reconstructed after containment. The following represents the minimum set of artefacts required to support a defensible CERT-In submission and any subsequent investigation.

Evidence Category	Specific Artefacts	Capture Priority
Detection record	Alert identifier, SIEM correlation ID, first-seen timestamp	Immediate at T+0
Identity events	Authentication logs, MFA records, privileged access activity, role changes	Within 30 minutes
Affected asset inventory	Hostnames, IPs, cloud resource IDs, system classification	Within 30 minutes
Endpoint artefacts	Process execution logs, lateral movement indicators, persistence mechanisms	Within 60 minutes
Network and DNS logs	Connection logs, DNS queries, data transfer volume indicators	Within 60 minutes
Cloud control plane	API calls, configuration changes, IAM events	Within 60 minutes
Data access logs	File access, database query logs, exfiltration indicators where applicable	Within 90 minutes

Maintain a single authoritative incident timeline. Record who captured what, and when. Assign a dedicated evidence custodian from the first hour. Containment activities must not overwrite or modify evidence sources.

Financial Impact Model: The Cost Of Detection Delay

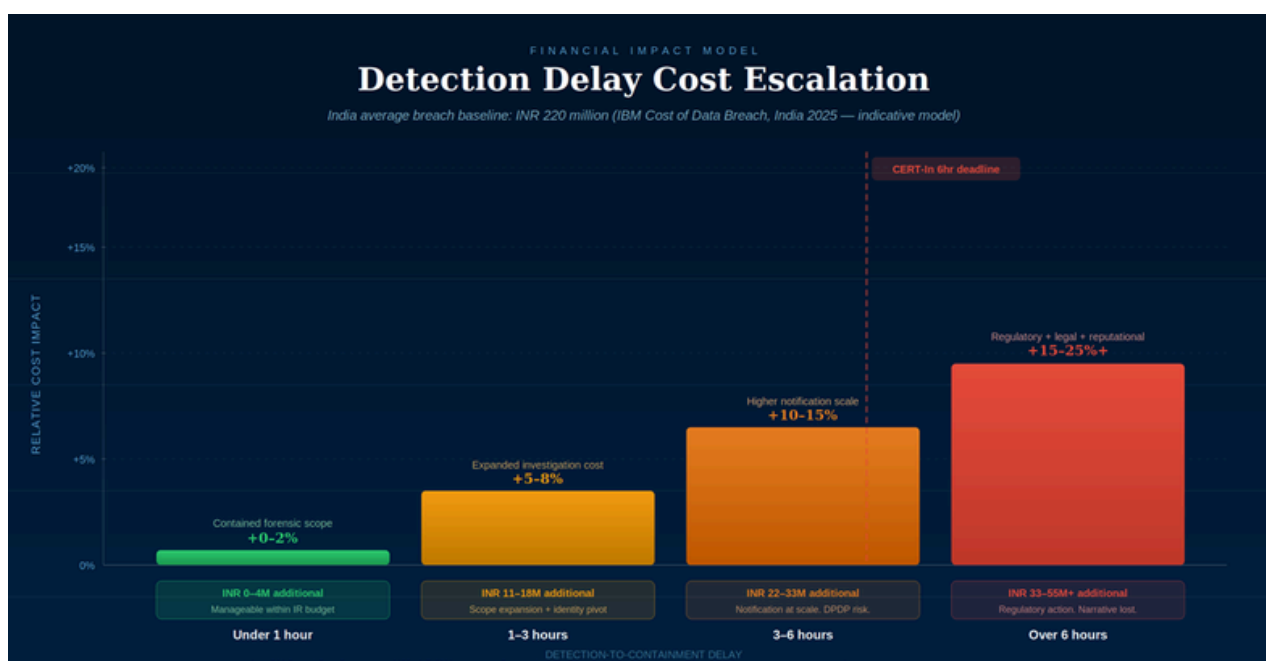


Figure 3: Detection Delay Cost Escalation - indicative model based on IBM India 2025 baseline of INR 220 million

The cost escalation bands above are illustrative operating benchmarks, not empirically derived findings. They are designed to provide a planning framework for quantifying the financial argument for investment in detection latency reduction. Actual cost impact will vary by sector, incident type, data volume, and regulatory outcome. Organisations should calibrate the model against their own breach cost assumptions.

Sector Overlays

Applying the Six-Hour Assurance Model to specific Indian industries

The Six-Hour Assurance Model applies across sectors, but its implementation priorities differ materially by industry context. The following overlays should be read as starting points for sector-specific calibration rather than definitive prescriptions.

Banking, Financial Services, and Insurance (BFSI)

Illustrative BFSI Scenario

A private sector bank's internet banking platform experiences a credential stuffing attack affecting 4,200 accounts. The attack is detected via anomaly scoring at 11:15 PM on a Friday. The CISO is not in office. The SOC lead cannot confirm the CERT-In reporting officer for after-hours escalations.

Outcome without readiness: The incident is not formally escalated until Saturday morning. The six-hour window passes. The bank faces regulatory scrutiny not primarily for the breach, but for the reporting delay.

Outcome with readiness: The after-hours rotation schedule names a deputy reporting officer. The severity matrix immediately classifies the event as Critical given the volume of affected accounts. The CERT-In submission is filed by 04:45 AM with available facts.

BFSI organisations operate under multi-regulator expectations. CERT-In's reporting obligation sits alongside RBI's cybersecurity framework for banks and NBFCs, SEBI's cybersecurity and cyber resilience framework for market participants, and IRDAI's guidelines for insurers. These frameworks share reporting principles but differ in specific timelines and submission formats.

- Align the CERT-In severity matrix with RBI/SEBI/IRDAI reporting obligations. Incidents may require simultaneous or sequential notifications to multiple regulators.
- Integrate fraud operations teams into the first-six-hour workflow. Fraud indicators often precede or accompany identity-based breaches.
- Target the lower end of detection benchmarks. Board scrutiny in BFSI is immediate and intense.
- Maintain regulator-ready evidence trails with separate log repositories that cannot be modified by containment actions.

Manufacturing and Industrial

Illustrative Manufacturing Scenario

A precision engineering firm in Pune detects anomalous lateral movement from an IT network segment toward an OT-connected system. The SOC identifies the vector as a vendor remote access session that was not terminated after a maintenance window.

Challenge: OT systems do not generate standard SIEM-compatible log formats. The IR Lead cannot immediately determine whether the OT network was accessed. Scope validation stalls.

Readiness requirement: OT visibility must be part of the detection architecture. Vendor access must be auto-revoked at session timeout. A separate OT-specific scope assessment runbook must exist.

Manufacturing organisations face a distinctive challenge: the convergence of IT and OT environments creates scope validation complexity that can consume the entire six-hour window. Detection architectures that cover only IT are operationally incomplete for this sector.

- Include OT log visibility in the readiness scope assessment. If OT telemetry cannot be queried within 30 minutes, this is a signal integrity gap.
- Validate IT-OT segmentation as a live control, not an architecture assumption. Penetration tests of segmentation boundaries should be included in readiness exercises.
- Ensure vendor access governance includes immediate revocation capability. Third-party access events are a primary breach vector in manufacturing.
- Protect plant-level configuration backups as incident evidence. These are frequently overwritten during recovery activities.

Information Technology and IT-Enabled Services (IT/ITeS)

Illustrative IT/ITeS Scenario

A mid-sized IT services firm discovers that a client-dedicated cloud environment was accessed using a compromised developer credential. The breach affects a client's production data. The firm's own CERT-In obligation is clear, but the client's contractual notification requirement is a separate and potentially shorter deadline.

Compounding factor: The firm operates a distributed remote workforce. The identity event was triggered from an overseas IP. Determining whether the access was by a legitimate employee operating remotely or by a threat actor using stolen credentials takes additional time.

Readiness requirement: Cloud control plane logs must be centralised and queryable in real time. Client notification obligations must be pre-mapped and included in the escalation workflow.

For IT/ITeS organisations, contractual exposure to clients may equal or exceed statutory regulatory exposure. The six-hour operating model must be capable of simultaneously satisfying CERT-In obligations and client contractual notification timelines.

- Centralise cloud control plane and SaaS logs into the primary SIEM. Cloud environments are the primary attack surface for this sector.
- Map client contractual incident notification obligations before an incident occurs. Some enterprise client contracts require notification within two to four hours.
- Monitor remote workforce identity risk as a continuous, elevated-priority signal. Credential compromise in distributed workforces is the dominant breach vector.
- Establish clear client communication templates in advance. Drafting client notifications during an active incident is a significant time cost.

Governance And Board Exposure

Incident response maturity is a governance issue, not only a technical one. Boards and audit committees are increasingly expected to demonstrate active oversight of cyber risk management, and regulatory bodies are examining that oversight quality in post-incident reviews.

Boards examine three questions after a significant incident:

Board Question	What Regulators and Auditors Examine
Was reporting timely?	Timestamps from detection to submission. Any gap in excess of six hours requires a documented rationale.
Was decision-making documented?	Written records of classification decisions, reportability assessments, and escalation actions with named decision-makers.
Was evidence preserved?	Chain of custody records from detection through reporting. Absence of preservation creates audit vulnerability.

Failure in these three areas creates audit vulnerability and potential director scrutiny under DPDP's governance provisions. Operational failure becomes governance failure when documentation is weak.

Governance Safeguards

- Board-approved incident reporting owner, documented and reviewed annually
- Quarterly readiness score presentation to Audit Committee or Risk Committee, using the Six-Hour Assurance Model maturity dimensions

- Tabletop simulation exercises documented in formal minutes, available for regulator review
- Post-incident review reports shared with the Audit Committee within 30 days of closure
- Legal counsel briefed on CERT-In and DPDP obligations before an incident, not during one

Readiness Scorecard

Score each dimension of the Six-Hour Assurance Model quarterly using the following maturity scale. Scoring should be conducted by the IR Lead in consultation with Legal, and the results presented to the CISO and Audit Committee.

Maturity Level	Definition
Level 1 - Absent	The dimension has not been assessed. No defined processes or ownership exist.
Level 2 - Developing	Processes exist in documentation but have not been tested operationally.
Level 3 - Operationally Reliable	Processes have been tested in tabletop exercises and the team can execute within benchmarks under controlled conditions.
Level 4 - Board-Tested	Processes have been tested in full simulation exercises, results have been presented to the board, and identified gaps have been closed.

Dimension	Level 3 Indicators	Level 4 Indicators
Signal Integrity	All log sources centralised and queryable. Retrieval benchmark met in tabletop.	Live simulation confirmed retrieval within 15–30 min. Gap analysis presented to board.
Classification Discipline	Severity matrix documented and rehearsed. Legal aligned on thresholds.	Matrix tested in full simulation. Results reviewed by Audit Committee.
Escalation Certainty	Named reporting owner documented. Out-of-hours rotation in place.	Rotation tested out-of-hours. Board aware of named owner and deputy.
Evidence Defensibility	Artefact capture protocol defined. Evidence custodian role assigned.	Chain of custody tested in simulation. Board shown example timeline output.

90-Day Readiness Roadmap

The following roadmap is designed for organisations beginning or materially improving their Six-Hour Assurance Model posture. Each activity maps to one or more Assurance Model dimensions. Organisations with existing IR programmes should use this as a gap assessment tool rather than a from-scratch implementation guide.

Phase	Activity	Owner	Assurance Dimension
Days 1–30	Confirm and document reporting ownership. Define deputy and out-of-hours rotation.	CISO + Legal	Escalation Certainty
Days 1–30	Finalise severity matrix mapped to CERT-In categories. Align with Legal.	IR Lead + Legal	Classification Discipline
Days 1–30	Audit log inventory. Identify retrieval gaps. Define remediation targets.	SOC Lead	Signal Integrity
Days 1–30	Define minimum viable CERT-In reporting dataset. Build submission template.	Legal + IR Lead	Escalation Certainty
Days 31–60	Deploy incident-type runbooks for top 5 scenario types.	IR Lead	All Dimensions
Days 31–60	Finalise DPDP assessment checklist and personal data scope map.	Legal + Privacy Lead	Evidence Defensibility
Days 31–60	Conduct cross-functional tabletop exercise covering one realistic scenario.	CISO	All Dimensions
Days 31–60	Define evidence custodian role and artefact capture protocols.	IR Lead	Evidence Defensibility
Days 61–90	Run full simulation from detection to CERT-In submission. Time each step.	CISO + IR Lead	All Dimensions
Days 61–90	Measure results against benchmark targets. Score against maturity model.	IR Lead + Legal	All Dimensions
Days 61–90	Present simulation results to Audit Committee.	CISO	All Dimensions
Days 61–90	Close identified gaps. Update runbooks and matrix.	IR Lead	Dimension-specific

Readiness must be measured, not assumed. An organisation that completes this roadmap will have tested its six-hour capability under controlled conditions and will know, with evidence, where its gaps are before a real incident reveals them.

Architecture-To-Outcome Mapping

Controls must compress response time and reduce ambiguity. The following table maps architectural choices to their specific operational benefit in the first six hours and to their regulatory reporting benefit. This is intended as a prioritisation tool for CISOs planning technology investment with readiness improvement as an objective.

Control Domain	Operational Benefit	Reporting Benefit	Assurance Dimension
Phishing-Resistant MFA (e.g., FIDO2)	Reduces frequency of credential-based incident triggers	Fewer reportable identity incidents overall	Signal Integrity
Centralised Identity & Access Log Platform	Faster scope validation. MFA logs queryable within minutes.	Confident reportability decisions backed by log evidence	Signal Integrity
Policy-Based Network Segmentation	Limits lateral movement post-compromise. Contains blast radius.	Reduced scope uncertainty in the reporting submission	Classification Discipline
Unified SIEM / XDR Platform	Correlated alerts across identity, endpoint, cloud. Reduces false positives.	Rapid, defensible timeline reconstruction	Signal Integrity + Evidence Defensibility

Control Domain	Operational Benefit	Reporting Benefit	Assurance Dimension
Unified SIEM / XDR Platform	Correlated alerts across identity, endpoint, cloud. Reduces false positives.	Rapid, defensible timeline reconstruction	Signal Integrity + Evidence Defensibility
Vendor Access Governance Platform	Immediate revocation of third-party sessions on alert	Clear third-party responsibility mapping in report	Escalation Certainty
Cloud Control Plane Monitoring	Real-time visibility of API and IAM events in cloud environments	Complete cloud-scope evidence for CERT-In submission	Signal Integrity + Evidence Defensibility

Architecture determines whether six-hour readiness is structurally achievable or permanently aspirational. Organisations with fragmented log infrastructure cannot reliably meet the signal integrity benchmarks regardless of process investment. Both are necessary.

Adversary behaviour compounds the architectural requirement. Verizon's DBIR identifies credential abuse, token replay in cloud control planes, privileged account exploitation, and vendor trust relationship abuse as dominant breach vectors globally. Indian enterprise context reflects similar patterns. These vectors all target identity infrastructure first. Detection architectures that do not include identity telemetry as a primary signal source will consistently miss the early stages of these attacks.

Glossary

Term	Definition
Awareness (CERT-In)	The point at which an organisation becomes cognisant of a cyber incident, whether through internal detection or external notification. The CERT-In six-hour clock starts at the earlier of detection or awareness.
Chain of Custody	The unbroken record of who collected, handled, and preserved each piece of evidence, with timestamps. Required for evidence defensibility in regulatory and legal contexts.
Classification Discipline	The Six-Hour Assurance Model dimension measuring an organisation's ability to apply a pre-agreed severity matrix to an incident quickly and without internal debate.
CERT-In	The Indian Computer Emergency Response Team, established under the IT Act 2000. Issues Directions requiring organisations to report specified cyber incidents within six hours.
Data Principal	Under the DPDP Act, the individual to whom personal data relates. Fiduciaries may be required to notify Data Principals of breaches affecting their data.
DPDP Act	The Digital Personal Data Protection Act, 2023. Governs the processing of digital personal data in India and introduces breach notification obligations to the Data Protection Board and Data Principals.
Evidence Defensibility	The Six-Hour Assurance Model dimension measuring an organisation's ability to produce a complete, auditable incident timeline with preserved artefacts under regulatory scrutiny.

Term	Definition
Escalation Certainty	The Six-Hour Assurance Model dimension measuring whether reporting ownership is predefined, documented, and executable across all shifts and time zones.
Minimum Viable Reporting Dataset	The pre-agreed set of facts sufficient to file a CERT-In initial report. Includes incident type, affected systems, initial timeline, and estimated scope. Completeness beyond this threshold is not required at T+6 hours.
Reporting Officer	The named individual accountable for authorising and submitting the CERT-In notification on behalf of the organisation. Must be identified in advance with a documented deputy and out-of-hours contact protocol.
Signal Integrity	The Six-Hour Assurance Model dimension measuring an organisation's ability to generate accurate, correlated detection signals across identity, endpoint, network, and cloud within minutes of an anomalous event.
Six-Hour Assurance Model	A proprietary readiness framework developed by Proactive for evaluating and improving Indian enterprise capability to meet CERT-In six-hour reporting requirements. Consists of four dimensions: Signal Integrity, Classification Discipline, Escalation Certainty, and Evidence Defensibility.

Closing

Six hours is not a compliance formality.

It is a test of four things simultaneously: the quality of your detection signals, the clarity of your decision-making criteria, the discipline of your governance structure, and the strength of your evidence chain.

Most Indian enterprises have invested in detection technology. Fewer have tested whether their process and governance infrastructure can convert a detection signal into a defensible CERT-In submission within the regulatory window. Fewer still have measured that capability under realistic conditions and documented the results for board review.

The Six-Hour Assurance Model exists to make that test measurable, repeatable, and documentable. The 90-Day Roadmap provides the implementation path. The sector overlays provide the industry-specific context. The evidence standards provide the defensibility baseline.

Readiness is not a posture. It is a demonstrated, time-stamped, board-reviewed capability.

Appendix: About The Sponsor

SPONSOR DISCLOSURE

This section contains information provided by the sponsor of this research, Proactive. The editorial content, frameworks, and recommendations throughout the main body of this document were developed independently of this commercial content.

Readers should evaluate the sponsor's capabilities against their own enterprise requirements.

Proactive is a Cisco Preferred Security Partner operating in the Indian enterprise market. This playbook was commissioned to help Indian CISOs operationalise the Six-Hour Assurance Model through Proactive's implementation services.

Proactive applies the Six-Hour Assurance Model through the following service areas:

- Detection engineering aligned to identity-led risk, using Cisco Duo, Cisco ISE, Cisco Secure Access, and Cisco XDR
- Pre-built severity matrices mapped to CERT-In specified incident categories
- Escalation mapping workshops with Legal and executive teams to establish documented reporting ownership
- Evidence capture standardisation and incident timeline tooling
- Simulation exercises designed to measure detection-to-reporting time against the benchmark targets in this playbook

Every Proactive engagement concludes with a scored maturity assessment against the Six-Hour Assurance Model, a quantified readiness gap report, a 90-day remediation plan, and a simulated six-hour drill with documented results.

Sources

- CERT-In Directions on Cyber Security Incident Reporting, April 2022, and associated FAQs. Ministry of Electronics and Information Technology, Government of India.
- Digital Personal Data Protection Act, 2023. Government of India. Note: Implementing rules were pending notification at time of publication.
- IBM Security. Cost of a Data Breach Report 2024. India segment data. IBM Corporation.
- IBM Security. Cost of a Data Breach Report 2025. India segment data. IBM Corporation.
- Verizon. Data Breach Investigations Report 2025. Verizon Communications Inc.
- ISO/IEC 27035-1:2023. Information technology — Information security incident management. International Organization for Standardization.
- NIST Cybersecurity Framework 2.0. National Institute of Standards and Technology, U.S. Department of Commerce.

Proactive Data Systems is an IT infrastructure and services company that designs, deploys, and supports secure, high-performance technology environments for organisations that cannot afford downtime. With over 35 years of experience, we have enabled more than 1,500 enterprises across India to modernise their networks, strengthen security, and scale with confidence.

Recognised as a Cisco Preferred Partner across Networking, Security, Cloud & AI, and Collaboration, Proactive combines deep systems integration capability with disciplined delivery and managed services. Our expertise spans enterprise networking, cybersecurity, data centres, collaboration platforms, and structured cabling. We build and run infrastructure that performs reliably every day, not just at go-live.

To learn more about our solutions, write to us
at pro@proactive.co.in

 www.proactive.co.in

PROACTIVE™
Enhancing Digital Experience