



RESEARCH REPORT · 2026 EDITION

The State of Identity Security in Indian Enterprises

Where the gaps are. What the data
shows. What regulators now require.

Proactive Data Systems Pvt Ltd · Cisco Preferred Security Partner
Delhi · Mumbai · Pune · Bengaluru · Hyderabad · Indore · Singapore

About This Report

This report synthesises publicly available regulatory data, industry research, and deployment evidence to produce an assessment of identity security posture across Indian enterprises. It draws on: CERT-In Annual Report 2024; DSCI India Cyber Threat Report 2025; Cisco 2025 Cybersecurity Readiness Index; National Cyber Crime Reporting Portal data as of February 2025; NPCI and RBI Annual Report FY 2023-24; RBI Annual Report/press releases FY 2024-25; and Proactive Data Systems' deployment experience across Indian enterprise environments.

Where data is drawn from vendor-commissioned research, this is noted explicitly. Where findings are drawn from Proactive's deployment experience, they are presented as practitioner observations from a non-statistically representative sample, not as research data.

This report does not make recommendations about specific products. It maps the gap.

Key Findings

- India recorded 2.27 million cybersecurity incidents in 2024, the fourth consecutive year of rising volume, with credential compromise as the dominant attack vector across all sectors. (CERT-In Annual Report 2024)
- 73% of Indian organisations are unaware of whether they have ever been attacked, making visibility the primary gap rather than technology or budget. (DSCI India Cyber Threat Report 2025)
- 57% of Indian organisations lack basic cyber hygiene practices, including MFA for privileged access and individual account accountability. (DSCI India Cyber Threat Report 2025)
- Only 7% of Indian organisations have reached mature cybersecurity readiness, according to the Cisco 2025 Cybersecurity Readiness Index (vendor-commissioned study).
- Four regulatory frameworks now require identity security controls for Indian enterprises, SEBI CSCRf, CERT-In CISO-2025-02, RBI Authentication Directions 2025, and DPDPA 2023, with three already in force and DPDPA full enforcement thirteen months away.
- In every Proactive deployment engagement, a credential audit conducted before any MFA configuration finds accounts that should not exist. The number varies by engagement size and sector. The finding does not vary.
- The dominant identity security gap across Indian enterprise environments is not the absence of MFA but its coverage: visible systems are protected; the systems where attackers actually gain entry are typically not.

Foreword

The conversation about cybersecurity in India has a structural problem. It is conducted, mostly, in the language of awareness. Reports are published. Boards receive presentations. The conversation is almost always about what should be done.

This report attempts something different. It is built from what regulators have documented, what industry surveys have measured, and what deployment teams find when they open an access register and count the accounts that should not be there. The picture that emerges is not a prediction. It is a description of where Indian enterprises are in 2026, not where their policies say they are, but where the evidence puts them.

The gap between those two things is the subject of this report.

Part One: The Threat Picture

India recorded 2.27 million cybersecurity incidents in 2024. (CERT-In Annual Report 2024)

That number requires context. CERT-In's incident taxonomy covers a wide range, from defacements to ransomware to data breaches. But the directional signal is unambiguous. The volume has been rising for four consecutive years. The proportion of incidents classified as financially motivated, involving identity compromise as the primary attack vector, has grown.

The single most important thing to understand about the 2024 incident data is not the total. It is this: 73% of Indian organisations are unaware of whether they have ever been attacked. (DSCI India Cyber Threat Report 2025, based on survey data; sample size and methodology available in the source report)

That is not a finding about attack frequency. It is a finding about visibility. An organisation that does not know whether it has been attacked cannot assess its exposure, cannot evaluate its controls, and cannot present an accurate picture to its board or its regulators.

The DSCI finding sits alongside a second number: 57% of Indian organisations lack basic cyber hygiene practices. (DSCI India Cyber Threat Report 2025) The definition of basic cyber hygiene, in the DSCI framework, includes MFA for privileged access, documented access reviews, and individual account accountability for critical system access. More than half of Indian enterprises have not yet implemented the floor.

The Identity Security Gap in Three Numbers

2.27M

Cybersecurity incidents in India in 2024
CERT-In Annual Report 2024

7%

at mature cybersecurity readiness level
Cisco 2025 Readiness Index (vendor-commissioned)

73%

of organisations unaware of whether ever attacked
DSCI Cyber Threat Report 2025 (survey data)

The gap between what Indian enterprises know about their exposure and what their exposure actually is has never been wider.

The Identity Layer

The dominant attack pattern in India in 2024 was not sophisticated. It required a credential.

Financial cyber fraud losses reported on India's National Cyber Crime Reporting Portal reached ₹36,450 crore as of February 2025. (National Cyber Crime Reporting Portal, February 2025) The primary mechanisms: phishing, SIM-swap fraud, and credential stuffing. All three depend on the same underlying condition, authentication that can be defeated by an attacker who holds a username and password.

UPI fraud recorded 632,000 incidents in FY 2023-24. (NPCI / RBI Annual Report FY 2023-24) The authentication layer protecting those transactions was, in most cases, SMS OTP. The RBI's Authentication Mechanisms Directions 2025, effective 1 April 2026, are the regulatory response to that pattern.

Manufacturing: A Specific Exposure

India is the world's second most attacked country in manufacturing, absorbing more than 2,100 cyberattacks per organisation per week. (Check Point Research 2024, vendor-commissioned threat intelligence) The manufacturing attack surface has expanded as OT

and IT have converged. The authentication architecture of most Indian manufacturing plants has not kept pace with the connectivity it now supports.

BFSI: The Compliance Exposure

RBI issued ₹54.78 crore in penalties to 353 regulated entities in FY 2024-25 for cybersecurity non-compliance. (RBI Annual Report/press releases, FY 2024-25) The examination cycle has shifted from advisory review to evidence review. Examiners now ask for authentication logs, not policy documents.

Healthcare: The Data Exposure

India's healthcare sector is among the most targeted for personal data exfiltration. Clinical systems, patient records, and insurance data represent a concentration of sensitive personal information governed by the DPDPA 2023's reasonable security safeguards obligation. The authentication controls on most Indian hospital information systems were not designed for the threat environment that now exists.

Part Two: The Regulatory Reality

Four frameworks now govern identity security for Indian enterprises. They use different languages, apply to different sectors, and carry different penalties. They are all asking the same operational question: can you prove who accessed your systems, and when?

SEBI CSCRF

Compliance deadlines ran from January to April 2025. For registered market participants — brokers, asset managers, depository participants, market infrastructure institutions — MFA for privileged access is a current, enforceable requirement. The first post-deadline examination cycle is underway. Organisations that have not deployed are not approaching a deadline. They are already outside the compliance window.

CERT-In CISG-2025-02

Effective 25 July 2025. Annual cybersecurity audits are now mandatory for all Indian organisations operating digital systems. MFA for all remote access is an explicit audit requirement. 180-day log retention, stored in India, is required. The question is not whether an MFA policy exists. It is whether the logs demonstrate that MFA is enforced.

RBI Authentication Mechanisms Directions 2025

Effective 1 April 2026. Two-factor authentication is mandatory for all digital payment transactions. At least one factor must be dynamic for non-card-present transactions. The factor independence principle requires that the two factors operate through independent channels. Risk-based escalation is required for higher-value and anomalous transactions.

DPDPA 2023

Full enforcement deadline 13 May 2027. The Act requires 'reasonable security safeguards' for personal data. In the view of most practitioners and commentators, any credible interpretation of 'reasonable safeguards' in 2026 includes MFA for systems handling personal data, given the explicit authentication mandates in parallel regulatory frameworks. The penalty for failure to implement security safeguards is up to ₹250 crore per instance. (DPDPA 2023, Schedule 1 Item 4) Unlike the other three frameworks, DPDPA penalties are triggered by a breach, not an examination cycle.

Four Frameworks, One Question

Framework	Status	Core MFA Obligation	Evidence Required
SEBI CSCRf	WINDOW CLOSED Jan–Apr 2025	MFA for privileged access to market infrastructure systems	Annual SEBI-recognised audit. 90-day log retention.
CERT-In CISG-2025-02	IN FORCE 25 July 2025	MFA for all remote access. Named individual accounts. Annual audit.	180-day log archive in India. Access review records.
RBI Auth Directions 2025	EFFECTIVE NOW 1 April 2026	2FA for all digital payment transactions. Factor independence. Risk-based escalation.	Granular auth logs per transaction. RBI examination evidence package.
DPDPA 2023	13 MAY 2027 13 months away	Reasonable security safeguards for all systems handling personal data.	Breach investigation evidence. Penalty up to ₹250 crore per instance.

All four ask the same question:
Can you prove who accessed your systems, and when?

Part Three: The Identity Security Gap by Sector

The aggregate picture is instructive. The sector-level picture is where the specific exposures become visible.

IT / ITeS and GCCs

The IT/ITeS sector faces a compliance pressure that has no equivalent elsewhere in the Indian industry. Client contracts from US and European enterprise clients increasingly require SOC 2 Type II certification, which requires documented MFA enforcement across every system with access to client data. Simultaneously, CERT-In CISG-2025-02 applies domestically. DPDPA obligations apply to personal data handled for Indian clients.

The gap that deployment teams consistently find is not in corporate systems. Microsoft 365 and the primary VPN typically have MFA. The gap is in what lies beyond them: developer access to client production environments, contractor credentials that outlasted their engagements, and shared administrator accounts on legacy client systems. SOC 2 auditors find this gap. So do breach investigators.

For Global Capability Centres, the challenge compounds. Parent company security mandates — typically issued following a breach somewhere else in the group- arrive with specific timelines. The India entity's infrastructure, assembled organically over the years, rarely matches the architecture of the mandate that was written. The gap between the mandate and the implementation reality is where the exposure sits.

BFSI

The BFSI sector has the most layered regulatory exposure of any Indian industry in 2026. RBI, SEBI, CERT-In, and DPDPA all apply simultaneously to entities operating across banking, capital markets, and insurance.

The most significant finding from BFSI deployments is not the absence of MFA. Most institutions have some MFA deployed. The finding is coverage: Internet banking and corporate email are protected. Core banking terminals, treasury systems, and vendor remote access are typically not. The attacker does not need to defeat the protected applications. They need the one application the MFA policy never reached.

The examination evidence gap is equally significant. RBI examiners now ask for authentication logs — not architecture diagrams, not policy documents, but 180-day logs demonstrating individual accountability for every access event to critical systems. Most mid-tier banks cannot produce this on demand. The controls may have been deployed. The evidence of their operation was not systematically retained.

Manufacturing

The manufacturing sector's identity security challenge is architecturally distinct from every other sector. The authentication surface includes systems that predate modern authentication protocols — PLCs, SCADA platforms, DCS controllers that authenticate via LDAP against Active Directory or via proprietary interfaces with no second-factor capability.

The OT/IT convergence has created a network topology that the original security architecture did not anticipate. A SCADA system installed in 2009 now sits on a network segment reachable through the same VPN that 40 vendors use for remote maintenance. The VPN has no MFA. The SCADA system has a shared password that has not been changed since the commissioning engineer set it.

The vendor access register is the most consistently problematic element in Indian manufacturing environments. In Proactive's manufacturing deployment experience across India, credential audits find an average of 8 to 20 vendor accounts from closed engagements that remain active per engagement.

Healthcare

Healthcare is the sector where the DPDPA 2023 exposure is most acute. Patient records, diagnostic data, insurance claim histories, and clinical trial data all fall within the Act's definition of personal data. The systems holding that data were typically deployed for clinical functionality, not security architecture.

The intersection of clinical urgency and authentication friction is the sector-specific design constraint that most MFA deployments in healthcare fail to navigate. An emergency physician accessing patient records in a resuscitation scenario cannot be presented with a push notification timeout. The authentication architecture must accommodate clinical workflows, not impose corporate IT workflows onto clinical environments.

Part Four: Deployment Observations from Proactive Engagements



NOTE

The following findings are drawn from Proactive's deployment engagements across Indian enterprises in IT/ITeS, BFSI, Manufacturing, and Healthcare. They represent practitioner observations from a non-statistically representative sample and should be read as field evidence, not research data. Where specific numbers are cited, the deployment basis is stated explicitly.

The credential audit finding is consistent across sectors

Every Proactive deployment begins with a credential audit before any MFA configuration is written. Across Proactive's engagements in Indian enterprise environments, the credential audit finds, in every case, accounts that should not exist: vendor accounts from closed engagements, shared credentials across multiple individuals, and former-employee accounts with active access to production systems.

The number varies by organisation size, age, and sector. The finding does not vary.

In manufacturing environments, the average number of dormant or non-compliant vendor accounts found per engagement is between 8 and 20. In BFSI environments, the most consistently absent document in the compliance evidence package is the bypass code log, a specific CERT-In audit request that most institutions have never formally maintained. In IT/ITeS environments, developer access to client production environments is the most under-examined access surface. In healthcare, shared accounts on clinical systems are the norm rather than the exception.

The coverage gap is predictable

In virtually every Indian enterprise environment Proactive has deployed into, MFA covers corporate email and the primary VPN. It does not cover everything beyond them. The specific gaps vary by sector, but the pattern is consistent: MFA was deployed on the most visible systems and did not reach the systems where the actual exposure sits.

The evidence package is rarely ready

CERT-In auditors and RBI examiners ask for logs, bypass code registers, vendor access registers with current status, and documented break-glass procedures with evidence of testing.

In the majority of Proactive's BFSI deployment engagements, at least three of the seven elements of the standard compliance evidence package are missing or out of date at the time of engagement. The controls may exist. The documentation of their operation typically does not.

Part Five: What Mature Looks Like

The Cisco 2025 Cybersecurity Readiness Index defines four maturity levels: Beginner, Formative, Progressive, and Mature. Seven percent of Indian organisations reach Mature. (Cisco 2025 Cybersecurity Readiness Index — vendor-commissioned study)

Mature, in this framework, is not an advanced bar. It requires that fundamental identity controls are in place, operational, and evidenced: MFA across the full authentication surface, individual accountability for every access event, privileged access management with documented reviews, and log retention sufficient to support incident investigation and regulatory examination.

The gap between the 7% who have reached that level and the 93% who have not is not primarily a technology gap. The technology exists, is commercially available, and is deployable in Indian enterprise environments without replacing existing infrastructure. The evidence from Proactive's deployments suggests the gap is primarily a sequencing problem: organisations have deployed the visible controls and deferred the harder ones. The deferral window has closed. The regulatory deadlines have arrived.

Part Six: The Regulatory Calendar and What It Means

The convergence of four regulatory deadlines in a narrow window reflects a shared assessment by multiple regulators that the authentication controls Indian enterprises currently have in place are inadequate for the threat environment they face.

SEBI CSCRF's deadline has passed. CERT-In CISG-2025-02 is in force. RBI Authentication Directions 2025 are effective. DPDPA full enforcement arrives in thirteen months.

For most Indian enterprises, the practical implication is this: the question is no longer whether to deploy comprehensive identity security controls. The question is in what order, at what pace, and with what evidence architecture.

The organisations that will perform best in the examination cycles now running are not necessarily those with the most sophisticated controls. They are those with the most complete evidence of the controls they have deployed: logs that have been running since deployment, vendor access registers that are current, bypass code logs that reflect every exception. Building the evidence architecture alongside the deployment, from day one, is the difference between a deployment that satisfies a regulator and one that requires emergency documentation the week before an examination.

Conclusion

Indian enterprises are not as protected as they think they are.

Seventy-three percent of organisations do not know whether they have been attacked. Fifty-seven percent lack basic cyber hygiene. Seven percent are at mature readiness. The regulatory frameworks now in force were written specifically in response to the attack patterns that have been exploiting these gaps.

The gap is closable. The technology is available. The deployment frameworks exist. The regulatory deadlines are providing the urgency that commercial risk assessments alone sometimes did not.

What is required is honest assessment of where the gaps actually are — not where the policy documents say they should not be, but where the credential audit and the access register and the log review reveal them to be.

Data Sources and Methodology

All statistics in this report are attributed at the point of use. Primary sources:

CERT-In Annual Report 2024 (cert-in.org.in): Cybersecurity incident volumes and sector data.

DSCI India Cyber Threat Report 2025 (dsci.in): Organisational awareness and cyber hygiene data. Based on survey data, sample size and methodology in the source report.

Cisco 2025 Cybersecurity Readiness Index (cisco.com): Maturity level data. Vendor-commissioned study. Flagged throughout.

National Cyber Crime Reporting Portal, February 2025 (cybercrime.gov.in): Financial cyber fraud loss data.

NPCI / RBI Annual Report FY 2023-24 (rbi.org.in): UPI fraud incident data.

RBI Annual Report/press releases, FY 2024-25 (rbi.org.in): Cybersecurity penalty data.

DPDPA 2023, Schedule 1 Item 4 (meity.gov.in): Penalty ceiling for security safeguards failure.

Check Point Research 2024 (checkpoint.com): Manufacturing attack frequency data. Vendor-commissioned threat intelligence.

Proactive deployment data: Presented as practitioner observations, not statistically representative research. Sample provenance is stated at each citation.

This report is updated as new regulatory data and industry research become available.

Proactive Data Systems is an enterprise IT infrastructure and services company. For more than three decades, the company has designed, deployed, and operated the technology foundations behind some of India's most demanding enterprise environments, from regulated industries to large distributed operations.

Founded in 1991, Proactive serves more than 1,500 customers, from fast-growing businesses to Fortune 500 enterprises, across banking and financial services, manufacturing, healthcare, public sector, IT and ITES, retail, education, and global capability centres. Our work spans enterprise networking, cybersecurity, cloud and AI-ready data centres, collaboration platforms, structured cabling, and managed services.

A Cisco Preferred Partner under the Cisco 360 Partner Program, Proactive is recognised across the Networking, Security, Collaboration, Cloud & AI, and Services portfolios, and is a Cisco Advanced Customer Experience Specialised Partner. The company is ISO 9001:2015 and ISO/IEC 27001 certified, and engineers solutions in partnership with Dell, Nutanix, NetApp, Palo Alto Networks, Fortinet, VMware, Veeam, and CommScope.

Headquartered in Delhi NCR, with offices in Mumbai, Bengaluru, Pune, Hyderabad, Indore, and Singapore.

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

 www.proactive.co.in

PROACTIVE[™]
Enhancing Digital Experience

© 2026 Proactive Data Systems Pvt Ltd. All rights reserved.

This report is for informational purposes only. It does not constitute legal or regulatory advice. Statistical claims are attributed to named sources; readers should refer to original sources for complete methodology and context.