CYBER FRAUD, SCAMS & DIGITAL RISK

IN INDIAN HIGHER EDUCATION

Evidence Dossier, Comparative Benchmarking & Institutional Risk Model

2021-2025	2026	INDIA + UK + US + EU
CORE STUDY PERIOD	LATEST RETROSPECTIVE RELEASES	COMPARATIVE FRAME

Prepared as a decision-grade research document for university leadership, registrars, finance, admissions, IT and cybersecurity teams. Updated 30 July 2026.

Evidence rule: measured facts, case reports, vendor telemetry and modeled estimates are never treated as interchangeable.

HOW TO USE THIS DOSSIER

Purpose, scope and claims discipline

This report is designed to be persuasive because it is auditable - not because it exaggerates the evidence.

The core question is not whether Indian higher education faces cyber risk; the public record establishes a large and rapidly growing national cyber-fraud environment, repeated attacks against education/research, recurring fake admissions and identity scams, and institution-level compromises. The harder question is prevalence: what percentage of India's universities and colleges experience attempts, successful compromises, operational harm or financial loss in a year? India does not yet publish a representative annual higher-education prevalence survey comparable with the UK. This report therefore separates four layers: exposure, compromise, negative outcome, and material loss.

What this report can support

- Board and governing-body cyber-risk briefings; procurement and budget justification; due-diligence discussions with prospective cybersecurity providers; institution-specific risk assessments; awareness campaigns for admissions, finance and IT teams; and evidence-backed proposals for managed monitoring, incident readiness and fraud defense.
- Use of the ~90% annual exposure estimate only with the words "targeted by / encounters at least one cyberattack, scam or impersonation attempt." It must not be rewritten as "90% are victims of fraud."
- Use of cost figures such as IBM's India average breach cost only as cross-sector context unless the underlying study specifically identifies research/education.

What this report does not claim

It does not claim that every attempted attack succeeds, that every NCRP complaint involves a university, or that vendor attack-count telemetry is a census of Indian institutions. Case reports are not used to infer prevalence. International data are benchmarks, not direct substitutes for Indian measurement.

SOURCE [S001-S019]

REPORT MAP

How the dossier is organized

Designed for both executive reading and forensic verification.

Part I - Executive case

Executive summary, claims discipline, four-layer risk model and the core institutional decision.

Part II - Methodology

Evidence grading, definitions, limitations, bias and rules for interpreting attempts, incidents, breaches and losses.

Part III - India macro evidence

NCRB cybercrime, fraud and cheating heads; CERT-In incidents; NCRP/CFCFRMS financial-fraud complaints and reported amounts; state distribution.

Part IV - Indian higher education

AISHE denominator, sector characteristics, education/research attack telemetry and fake-university trend.

Part V - Threat taxonomy

Phishing, impersonation, fake admissions, ransomware, privacy, academic integrity, BEC/payment diversion, supply chain, web compromise, insider and AI-enabled deception.

Part VI - Indian case register

Graded case profiles across 2021-2025, plus a 2026 watchlist item. Official/first-party/media evidence is distinguished.

Part VII - International benchmark

UK government prevalence measurement, US Verizon Educational Services breach patterns, ENISA Europe threat landscape, education ransomware and India breach-cost context.

Part VIII - India prevalence model

85-95% exposure planning range, central ~90%, with scenario-only compromise/outcome layers and explicit non-claims.

Part IX - Regulation and operating model

CERT-In reporting expectations, DPDP context, institutional controls, 90-day roadmap and board dashboard.

Part X - State profiles and assessment

State/UT cybercrime profiles, full state table, assessment framework, procurement questions and governance prompts.

Part XI - Appendices and sources

Source register, core data tables, derived growth calculations, comparison tables and closing decision statement.

EXECUTIVE SUMMARY

The evidence in one page

2.94m	2.40m	101,928	49,535
CERT-In cyber incidents, 2025	financial-fraud complaints, 2025	NCRB cybercrime cases, 2024	AISHE universities + colleges

India's national cyber-risk curve accelerated sharply during the study period. CERT-In observed 2,944,248 cyber security incidents in 2025, more than double 2021. NCRP/CFCFRMS financial-fraud complaints increased from 262,846 in 2021 to 2,402,579 in 2025. NCRB registered cybercrime cases rose from 50,035 in 2020 to 101,928 in 2024; cases under the "Fraud" head rose faster, from 10,395 to 29,758. [S001-S003]

Higher education sits inside that rising national exposure while also carrying characteristics that amplify risk: open networks, high identity turnover, extensive third-party systems, admissions/payment peaks, large stores of personal data, research assets, public-facing brands, decentralized departments and a population continuously targeted with job, scholarship, fee and credential scams.

The strongest international institutional-prevalence benchmark is the UK government's 2025/26 survey: 98% of higher-education institutions identified at least one breach or attack in the preceding 12 months. Among affected further/higher-education institutions, 96% saw phishing and 79% impersonation; 49% experienced a negative system outcome. [S010]

For India, this dossier models 85-95% annual exposure, central case ~90%, for "at least one cyberattack/scam/impersonation attempt encountered or targeted at an institution." Applied to 49,535 AISHE-registered universities and colleges in 2023-24, this corresponds to about 42,105-47,058 institutions, with a central estimate of 44,582. This is a scenario estimate, not an official statistic.

EXECUTIVE SUMMARY

Eight findings that should change university risk decisions

1. The national attack surface is expanding faster than institutional headcount.

CERT-In incidents increased 109.9% from 2021 to 2025, while the AISHE university+college frame grew much more slowly. This means the surrounding threat environment is intensifying even before institution-specific controls are considered.

2. Financial cyber fraud has become a mass-volume phenomenon.

Annual NCRP/CFCFRMS financial-fraud complaints grew more than ninefold from 2021 to 2025. The reported amount grew far faster, though reported amount is not synonymous with confirmed final loss.

3. Fraud within cybercrime is accelerating.

NCRB cases under the Fraud head increased 186% between 2020 and 2024, with a 52.9% jump from 2023 to 2024.

4. Education is consistently high-intensity in vendor telemetry.

Check Point published India education/research figures of 5,196 weekly attacks per organization in 2021 and 6,874 in 2024; 2025 reporting cited 8,487 over the preceding six months. These are attempts observed in vendor telemetry, not victim counts.

5. Brand abuse is part of cybersecurity.

Fake admissions sites, social pages, WhatsApp offers, cloned domains and fake universities can cause financial loss and identity theft without breaching the university network.

6. Integrity failures matter as much as confidentiality.

Marks, admissions decisions, fee instructions, examination data and credentials are high-consequence integrity assets. A university can suffer severe harm even if no large database is exfiltrated.

7. Third parties expand the blast radius.

Admissions vendors, SaaS platforms, payment providers, ERP integrators and cloud systems create inherited risk. Vendor compromise can reach applicants even when the university's own core network remains intact.

8. Controls must join cyber defense and fraud defense.

A mature program needs identity security, brand/domain monitoring, payment verification, attack detection, incident response, vulnerability management, backup resilience, vendor governance and student/staff awareness as one operating model.

EXECUTIVE SUMMARY

Board-level risk model

Layer	Question	India evidence position	Defensible conclusion
Exposure	Was the institution targeted / did it encounter an attempt?	No national HE prevalence survey; strong national growth + education telemetry + UK official comparator.	Modeled 85-95%; central ~90%.
Compromise	Did an attacker obtain unauthorized access or execute malicious action?	Institution-level cases exist; no representative all-India HE survey.	Do not publish a single national percentage as fact.
Negative outcome	Was there downtime, account misuse, data loss, payment diversion or other consequence?	No India HE prevalence measurement. UK affected FE/HE: 49% negative system outcome.	Use scenario range only, with explicit caveat.
Material loss	Was there major financial loss, ransomware, serious breach or academic-integrity damage?	Case evidence + cross-sector cost studies; no India HE census.	Budget for plausible high-severity tail risk rather than average incident.

This four-layer model prevents a common sales and risk-management error: treating “attacks per week” as if they imply thousands of successful breaches. Attack telemetry establishes exposure pressure. Successful compromise and impact must be measured separately.

METHODOLOGY

Evidence hierarchy

Every major claim in this dossier is assigned, explicitly or implicitly, to an evidence class. The hierarchy is designed to let a university procurement or audit team challenge the document without collapsing the underlying case.

Grade	Evidence type	Examples	Use in this dossier
A	Official Indian government/regulator or Parliament	MHA/PIB, NCRB, CERT-In, AISHE, UGC, Sansad answers	Primary quantitative baseline; highest reliance.
B	Institutional / public-authority first-party notice	University warning, local public authority	Case validation and institutional response.
C	Primary research / major vendor dataset	IBM, Verizon DBIR, Sophos, Check Point, academic study	Comparative benchmarks and telemetry with methodology caveats.
D	Reputable media citing institution/police	Indian Express, TOI, HT, FPJ	Case register; allegations labeled; not used to infer national prevalence.
E	Community/anecdotal claims	Forums/social posts	Excluded from quantitative conclusions; not used for exploit details.

Date rule

The core study period is 1 January 2021 through 31 December 2025. Government publications released in 2026 are used when they retrospectively report 2025 or earlier data. A clearly separated post-period watchlist uses 2026 information, including UGC's February 2026 fake-university list.

No denominator mixing

Complaint counts, FIRs, observed cyber incidents, vendor-detected attack attempts, affected organizations and confirmed breaches have different denominators and cannot be compared as if they were the same unit.

METHODOLOGY

Definitions that matter

Scam

A deceptive scheme intended to obtain money, credentials, identity information, access, academic advantage or another benefit.

Fraud

A deception-linked offense or loss category; in this dossier “fraud” may refer to official crime-head terminology or to broader economic deception, and the context is stated.

Cyberattack / breach

An attempt or successful event affecting confidentiality, integrity or availability. UK survey wording includes breaches or attacks identified by institutions.

Phishing

Deceptive electronic communication designed to induce a user to reveal information, visit a malicious resource or take a fraudulent action.

Impersonation

Unauthorized representation of a university, official, department, applicant, vendor or trusted party.

Brand abuse

Use of cloned domains, social accounts, logos, search ads, messaging identities or documents to exploit institutional trust.

Academic-integrity attack

Unauthorized manipulation of marks, admissions, examinations, certificates, credentials or academic records.

Ransomware

Malicious activity that encrypts and/or steals data to coerce payment or another concession.

Supply-chain incident

Risk transmitted through a vendor, SaaS provider, consultant, admissions partner, payment provider, hosting provider or other dependency.

METHODOLOGY

Known limitations and bias

- Under-reporting: institutions may not detect or publicly disclose incidents; police complaint and FIR conversion varies.
- Detection bias: better monitored institutions may report more attacks precisely because they can see them.
- Vendor telemetry bias: customer footprint, sensor coverage, definitions and time windows vary; attack counts may include automated noise and blocked attempts.
- Media bias: large universities and disruptive events are more likely to be reported.
- Regulatory list dynamics: UGC fake-university counts can change during a year as entities are added, removed or subject to action.
- Data-version bias: NCRP/CFCFRMS is dynamic. Annual tables and later aggregate totals can differ slightly after revision.
- International comparability: UK survey prevalence, US breach datasets and EU incident intelligence use different units and sector classifications.
- Cost-model bias: average breach cost is influenced by organization size and industry mix and should not be treated as the expected loss for a specific college.

Implication

The correct commercial conclusion is not “we know exactly how many Indian colleges are breached.” It is “the measured national threat environment is severe; international prevalence measurement shows near-universal targeting of universities; Indian education telemetry is extremely high; and enough Indian cases exist across multiple attack classes to justify institutional controls now.”

INDIA MACRO RISK

Cybercrime cases more than doubled, 2020-2024

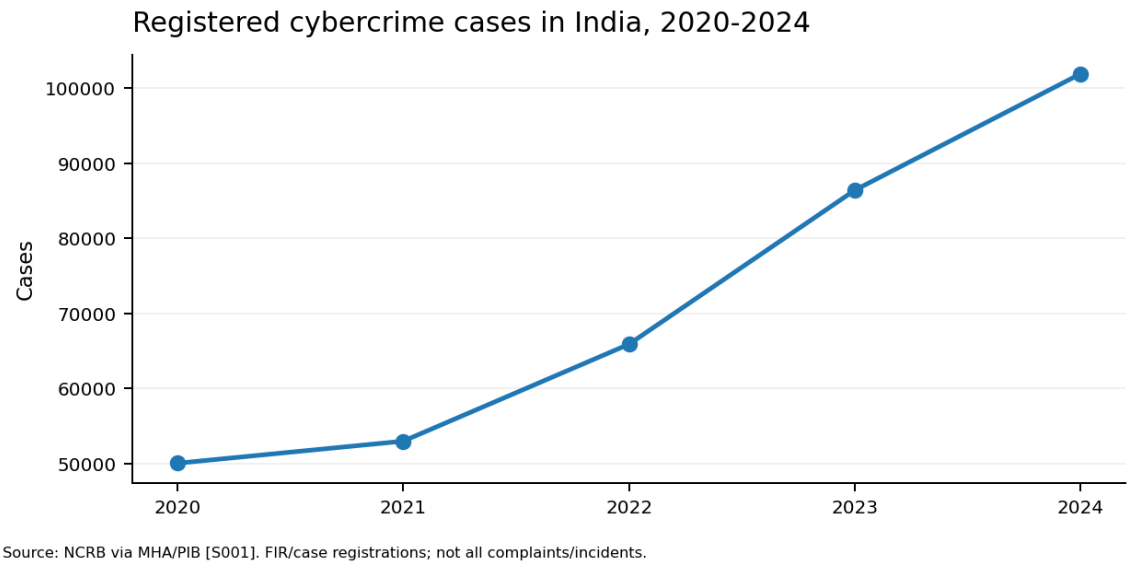


Figure 1. NCRB registered cybercrime cases. [S001]

+103.7%	+17.9%	101,928
2020 TO 2024	2023 TO 2024	2024 CASES

NCRB case registrations are a law-enforcement measure, not a count of attack attempts. They nevertheless show a steep rise in cases that crossed the threshold to registration. The latest published NCRB year identified by MHA in July 2026 is 2024. [S001]

INDIA MACRO RISK

Fraud is rising faster than overall cybercrime

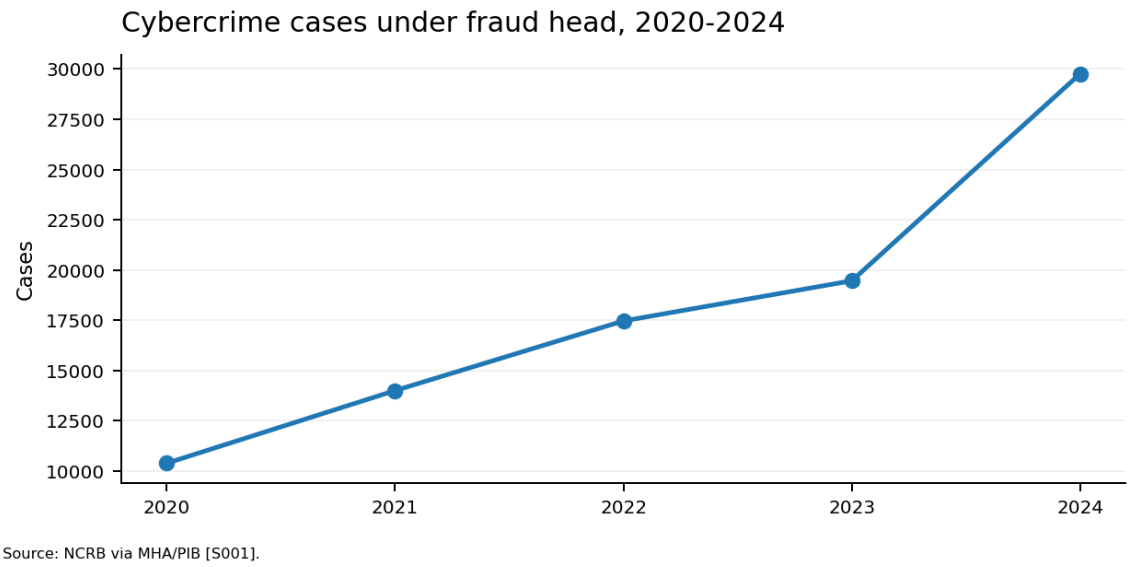


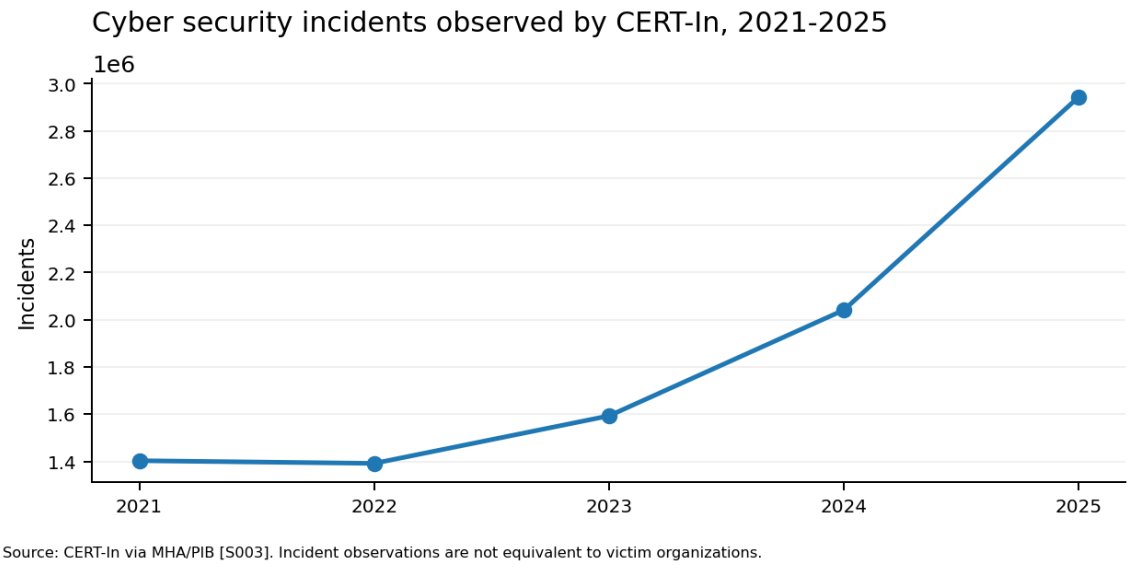
Figure 2. NCRB cybercrime cases under Fraud head. [S001]

+186.3%	+52.9%	29,758
2020 TO 2024	2023 TO 2024	2024 FRAUD-HEAD CASES

Fraud-head growth outpaced overall cybercrime-case growth over the same period. For universities, this matters because cyber risk is not confined to malware: payment diversion, impersonation, admissions deception and identity abuse can produce losses without a classic network breach.

INDIA MACRO RISK

CERT-In observed 2.94 million cyber incidents in 2025



Source: CERT-In via MHA/PIB [S003]. Incident observations are not equivalent to victim organizations.

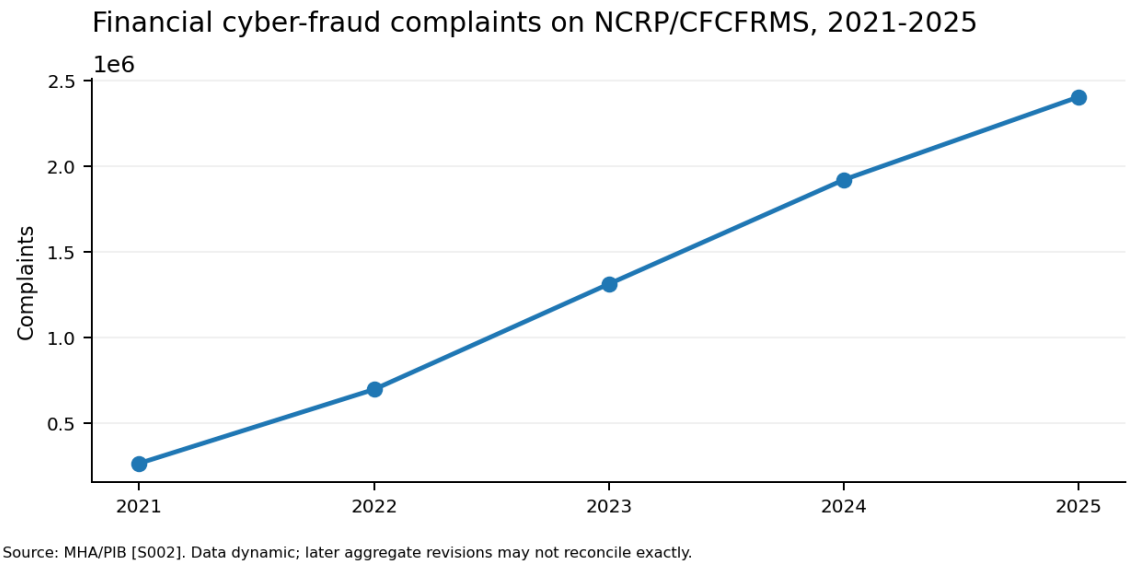
Figure 3. CERT-In cyber security incidents observed. [S003]

+109.9%	+44.2%	2,944,248
2021 TO 2025	2024 TO 2025	2025 INCIDENTS

CERT-In's count measures incidents reported to or tracked by the national response agency. It is not a count of victim organizations. In January 2026, CERT-In also reported 1,530 alerts, 390 vulnerability notes and 65 advisories during 2025, alongside drills, audits and training activity. [S004]

INDIA MACRO RISK

Financial cyber-fraud complaints rose more than ninefold



Source: MHA/PIB [S002]. Data dynamic; later aggregate revisions may not reconcile exactly.

Figure 4. NCRP/CFCFRMS financial cyber-fraud complaints. [S002]

+814%	9.14×	2.40m
2021 TO 2025	2025 VS 2021	2025 COMPLAINTS

The 2021-2025 annual table shows rapid scale-up in citizen financial-fraud reporting. MHA's later July 2026 aggregate said more than 6,589,201 financial-fraud complaints were recorded during 2021-2025, with more than ₹55,050 crore reported, more than ₹8,189 crore marked as lien and more than 195,760 FIRs. Because the system is dynamic, later aggregate revisions need not exactly equal the sum of an earlier annual table. [S001-S002]

INDIA MACRO RISK

Reported amount: from ₹551 crore to ₹22,495 crore

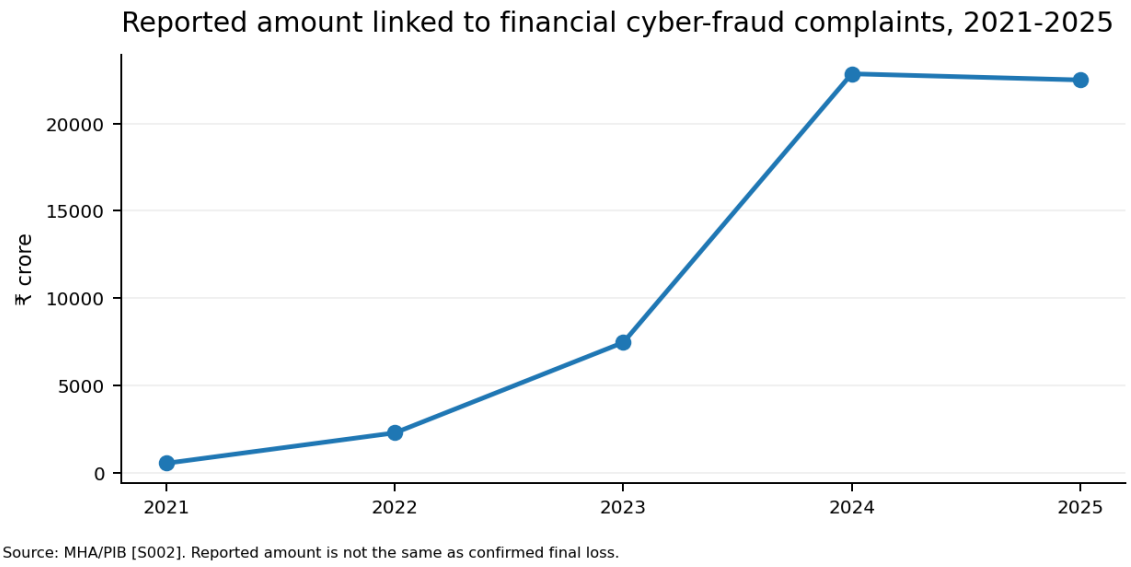


Figure 5. Reported amount in NCRP/CFCFRMS financial cyber-fraud complaints. [S002]

₹22,495 cr	~40.8×	-1.5%
2025 REPORTED AMOUNT	2025 VS 2021	2025 VS 2024

The reported amount rose extraordinarily over the five-year period, then remained near the 2024 peak in 2025. “Reported amount” should not be presented as confirmed, adjudicated final loss. Universities should nonetheless treat the payment ecosystem as exposed: students and families can be induced to pay attackers impersonating institutional brands even when university systems are not breached.

INDIA MACRO RISK

Crime-head detail: 2020-2024

Crime head	2020	2021	2022	2023	2024
Computer-related offences	21,926	19,915	23,894	35,329	36,920
Fraud	10,395	14,007	17,470	19,466	29,758
Cheating	4,480	6,343	10,509	16,943	19,296
Cyber blackmail / threatening	303	689	696	689	601
Fake profile	149	123	157	225	266
Data theft	98	170	97	113	88
IT Act total	29,643	27,427	31,908	44,237	44,872
IPC/BNS cyber offences total	20,201	25,384	33,798	41,849	56,747

The growth in fraud and cheating categories reinforces the case for anti-fraud capabilities to sit beside classic cybersecurity. A phishing email that convinces an applicant to pay a false account is a different technical event from ransomware, but it is part of the same institutional trust surface. [S001]

INDIA MACRO RISK

2024 state distribution

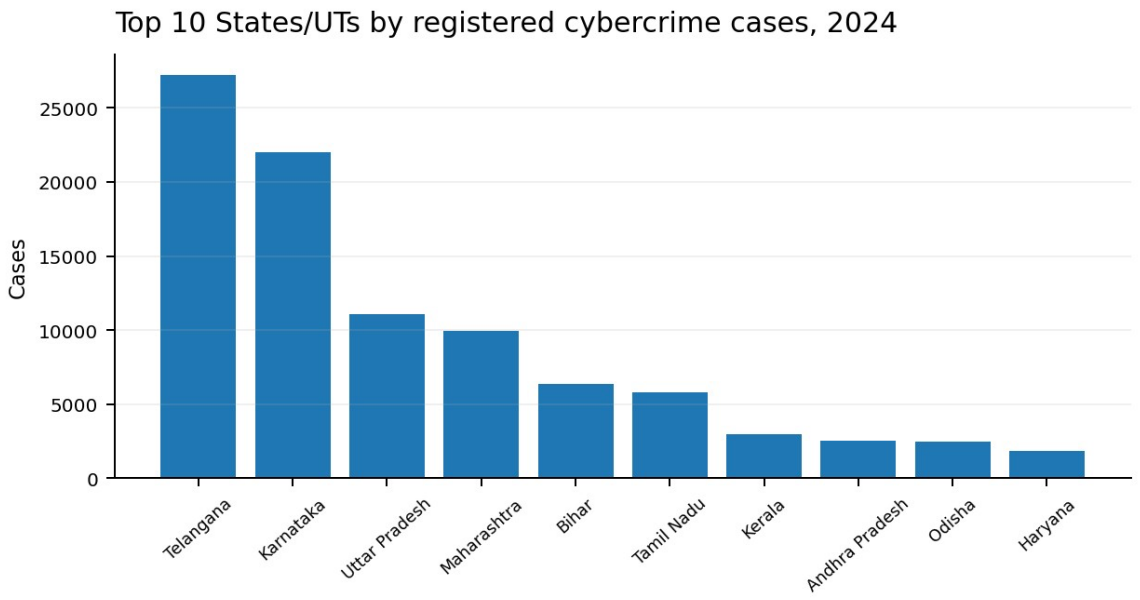


Figure 6. Top States/UTs by registered cybercrime cases in 2024. [S001]

Telangana and Karnataka account for exceptionally high registered case counts in the 2024 NCRB table, followed by Uttar Pradesh and Maharashtra. This is not a per-capita ranking and should not be used to label a state “more vulnerable” without controlling for population, reporting practices, digital adoption and policing. The state profiles later in this dossier show the full 2020-2024 series.

INDIA MACRO RISK

Complaints, incidents and FIRs: why the numbers look different

Metric	2025 / latest	What it measures	Do not interpret as
CERT-In cyber incidents	2,944,248 in 2025	Cyber security incidents reported/tracked	2.94m breached organizations
NCRP/CFCFRMS financial-fraud complaints	2,402,579 in 2025 annual table	Citizen complaints relating to financial cyber fraud	2.40m FIRs or proven crimes
NCRB cybercrime cases	101,928 in 2024	Cases registered under cybercrime heads	All attacks or all complaints
NCRP/CFCFRMS FIRs	>195,760 aggregate 2021-2025	FIRs associated with system complaints	Annual HEI victim count

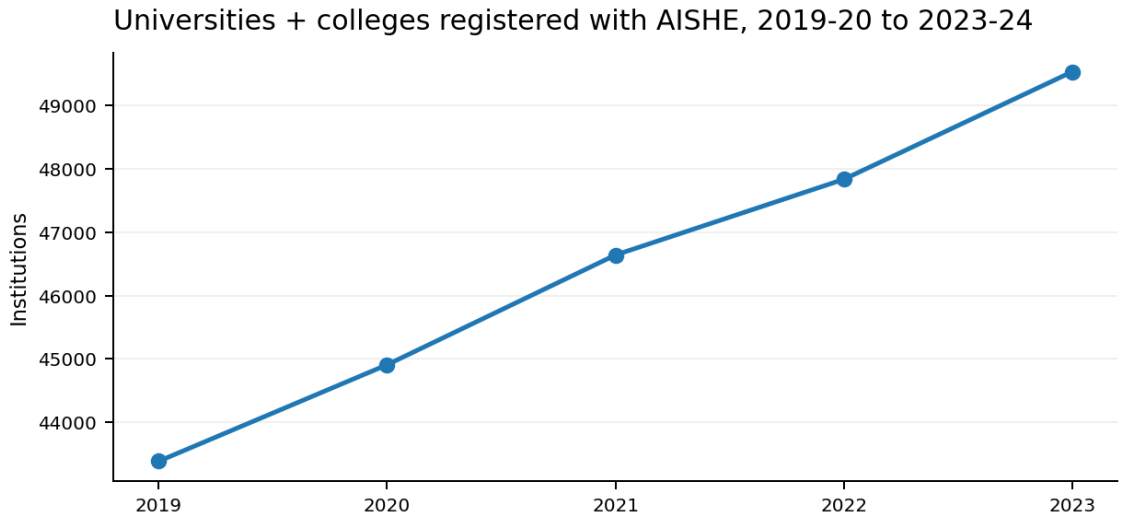
For procurement decision-making, scale across all four measures is important. For statistical claims, the denominators must remain separate. [S001-S003]

INDIAN HIGHER EDUCATION

A 49,535-institution university and college attack surface

1,289	48,246	49,535	64,756
UNIVERSITIES	COLLEGES	UNIVERSITIES + COLLEGES	ALL AISHE-FRAME HEIs

AISHE 2023-24 registered 1,289 universities/university-level institutions, 48,246 colleges and 15,221 standalone institutions. 1,278 universities and 46,468 colleges responded. Of responding colleges, 17.1% were government, 12.9% private aided and 70.0% private unaided. [S005]



Source: AISHE 2023-24 [S005]. Year labels denote academic survey year beginning year.

Figure 7. Universities + colleges registered with AISHE. [S005]

INDIAN HIGHER EDUCATION

Why the sector is structurally exposed

Identity churn

New applicants, students, alumni, adjuncts, researchers, contractors and vendors continuously enter and leave identity systems.

Open culture

Universities optimize for collaboration and access; security controls must coexist with research and academic openness.

Payment moments

Admissions, hostel fees, examinations, certificates, scholarships and vendor payments create predictable windows for impersonation.

Distributed authority

Departments and centers may operate websites, social accounts, SaaS tools and procurement with uneven security maturity.

High-value data

Identity, academic, financial, health, research and credential data can be monetized or used for extortion.

Academic integrity

Marks, exams, admissions, degrees and research results can be manipulated even when confidentiality is not the attacker’s goal.

Third parties

ERP, admissions, hosting, cloud, payment, LMS, email and outsourcing partners create inherited attack paths.

Public brand

Students often trust logos, domains, social profiles and official-looking documents - making universities attractive impersonation targets.

INDIAN HIGHER EDUCATION

Attack intensity: useful signal, wrong denominator

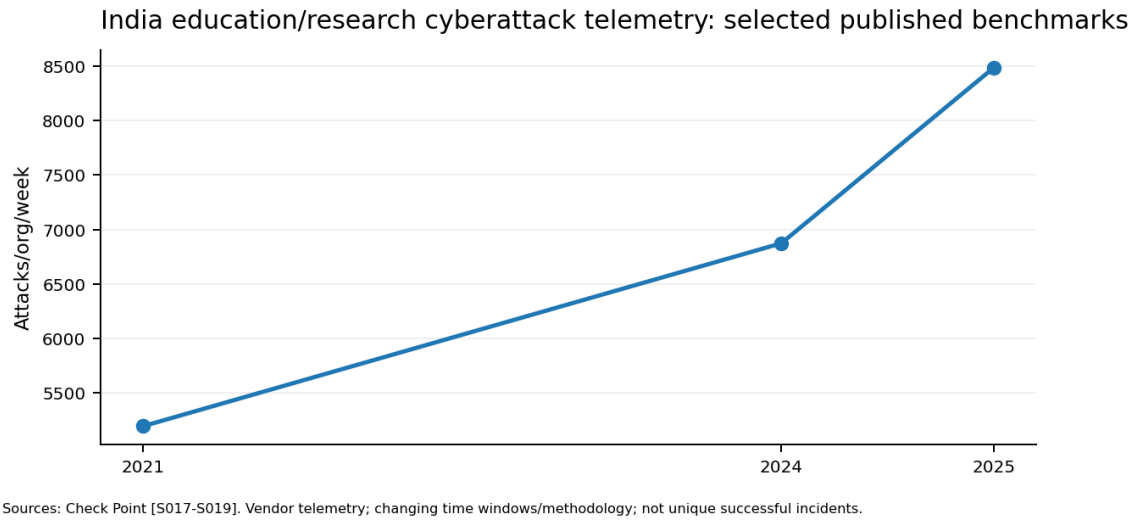


Figure 8. Selected Check Point education/research telemetry for India. [S017-S019]

Check Point reported 5,196 weekly attacks per education/research organization in India in July 2021 and 6,874 in 2024. 2025 Indian-market reporting cited 8,487 attacks per week over a preceding six-month window. The values suggest sustained, extreme automated and adversarial pressure. They cannot tell us how many unique institutions were successfully compromised, because a single institution may generate thousands of blocked or attempted events.

How to quote this

Good: “Vendor telemetry has repeatedly placed Indian education/research among the most heavily attacked environments, with thousands of attack attempts per organization per week.” Bad: “Every college is breached thousands of times per week.”

THREAT TAXONOMY

01. Phishing and credential theft

Fake login pages, malicious attachments, OAuth abuse, password-reset lures and MFA fatigue can target faculty, admissions staff, finance teams and students. Controls: phishing-resistant MFA for privileged roles, secure email, conditional access, credential monitoring, rapid account containment.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

THREAT TAXONOMY

02. University and executive impersonation

Attackers can impersonate registrars, deans, finance staff or the institution itself by lookalike domains, free-mail accounts, compromised accounts, social profiles or messaging apps. Controls: domain monitoring, DMARC/SPF/DKIM, verified communication policy, public scam alerts, takedown workflow.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

THREAT TAXONOMY

03. Fake admissions, fee and scholarship schemes

Attackers exploit application deadlines and payment urgency. Even without a network breach, the institution suffers reputational and support burden. Controls: one authoritative payment page, beneficiary-name verification, anti-fraud banners, published official channels, applicant warnings.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

THREAT TAXONOMY

04. Fake universities, degrees and recognition claims

Recognition fraud exploits information asymmetry. UGC's persistent fake-university list demonstrates that higher-education fraud extends beyond network security. Controls: recognition verification, credential validation, public registry linking, monitoring for brand/approval misuse.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

THREAT TAXONOMY

05. Ransomware and extortion

Availability pressure is particularly potent during admissions, exams, results and research deadlines. Extortion increasingly includes data theft without encryption. Controls: segmentation, EDR/MDR, immutable/offline backups, tested recovery, privileged-access control, patching, incident retainer.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

THREAT TAXONOMY

06. Data exposure and privacy incidents

Student/staff datasets can be exposed through misconfiguration, access-control failures, compromised credentials or third parties. Controls: data inventory, least privilege, encryption, DLP where appropriate, secure APIs, retention discipline, breach playbooks.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

THREAT TAXONOMY

07. Academic record and marks manipulation

Integrity attacks can alter marks, attendance, eligibility, admissions or credentials. Controls: strong admin authentication, separation of duties, tamper-evident logs, change approvals, anomaly detection, independent reconciliation.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

THREAT TAXONOMY

08. Payment diversion and BEC

An attacker impersonates or compromises a trusted party and changes bank instructions. Controls: out-of-band confirmation, beneficiary controls, dual approval, high-value payment hold, vendor master-data governance.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

THREAT TAXONOMY

09. Supply-chain compromise

Admissions vendors, ERP implementers, hosting providers, payment gateways, LMS platforms and contractors may become the access path. Controls: security clauses, breach notification, MFA, logging, scoped access, vendor inventory, evidence-based assurance.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

THREAT TAXONOMY

10. Website / portal compromise

Defacement, malicious redirects, fake notices, credential harvesting and disruption can damage trust quickly. Controls: secure SDLC, WAF, patching, hardening, backups, monitoring, DNS/domain security, content integrity checks.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

THREAT TAXONOMY

11. Social media and messaging abuse

Fake Facebook/Instagram pages, WhatsApp groups and Telegram channels can impersonate admissions or officials. Controls: verified accounts, monitoring, rapid reporting/takedown, official-channel education, scam keyword alerts.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

THREAT TAXONOMY

12. Insider and privileged misuse

Staff, students or contractors may misuse legitimate access intentionally or accidentally. Controls: least privilege, logging, peer review, separation of duties, rapid deprovisioning, behavioral/anomaly signals, clear sanctions.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

THREAT TAXONOMY

13. AI-enabled deception

Generative AI reduces the cost of convincing phishing, multilingual impersonation, synthetic documents and voice/deepfake scams. Controls: verification protocols for money/data requests, provenance checks, staff drills, high-risk transaction callbacks.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

THREAT TAXONOMY

14. Research espionage and IP theft

Universities can hold valuable unpublished research, grant data, source code and collaborations. Controls: research-zone segmentation, secure collaboration, data classification, export-control awareness where applicable, monitored privileged access.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

THREAT TAXONOMY

15. Denial of service and disruption

Public portals may be disrupted for activism, extortion or competitive motives. Controls: DDoS protection, CDN/WAF, capacity planning, alternate channels, incident communications.

University failure modes

- Trust is transferred from the university brand to the attacker.
- Peak academic timelines magnify urgency and reduce verification time.
- One compromised identity can become a bridge into ERP, email, cloud drives or finance workflows.
- A technically contained incident can still create reputational, regulatory and applicant-support consequences.

Evidence signals in this dossier

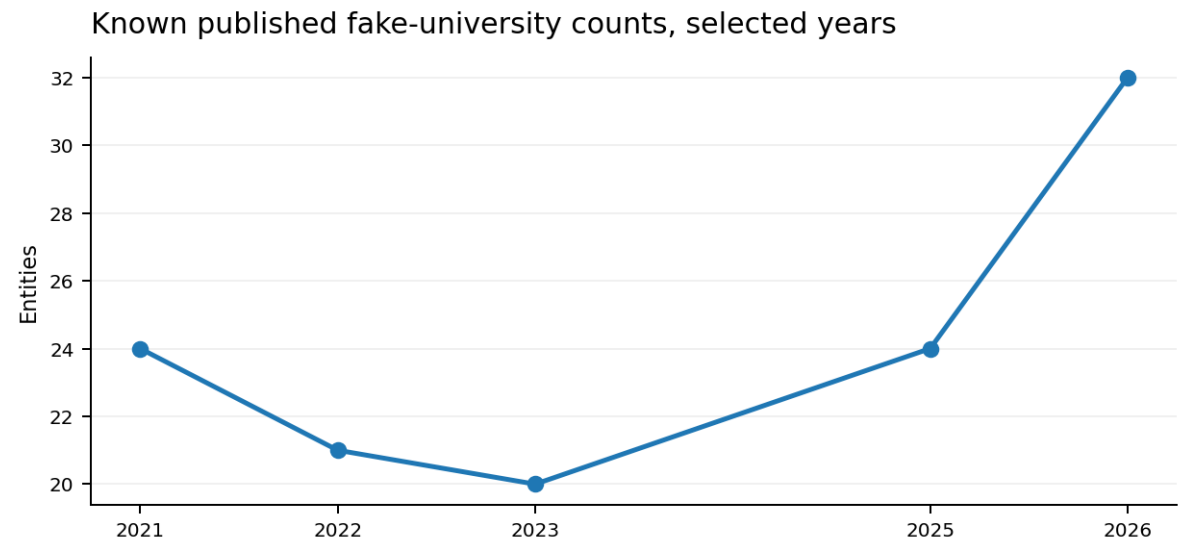
The Indian case register contains examples across impersonation, fake admissions, ransomware, website compromise, academic-integrity manipulation and third-party risk. UK official data additionally show phishing, impersonation, malware, denial-of-service, account takeover and unauthorized access occurring across affected colleges/universities. [S010, C01-C21]

Minimum control test

Ask whether the institution can detect this attack class, prevent the most common path, verify a suspected event, contain it within hours, communicate to affected people and produce evidence for management, law enforcement and regulators.

FRAUD ECOSYSTEM

Fake universities are a persistent recognition-fraud problem



Sources: UGC, Parliament and contemporaneous UGC-based reporting [S006, S021-S024]. 2024 omitted: no harmonized count used.

Figure 9. Selected published counts; list membership is dynamic. [S006, S021-S024]

Published UGC/UGC-based counts remained material throughout the study period: 24 in 2021, 21 in 2022, 20 in 2023 and 24 according to an official parliamentary answer on 1 December 2025. UGC's February 2026 list contains 32 entities. The changing list shows both persistence and the need for live verification rather than static "safe" lists.

This category is not the same as a cyber breach, but it is cybersecurity-adjacent trust fraud: victims encounter websites, digital advertising, online applications, messaging and payment channels that imitate the legitimacy of recognized higher education.

CASE REGISTER

How to read the incident pages

The following cases are not a prevalence sample. They are a structured illustration of attack diversity in and around Indian higher education. Grade A is official government/regulatory evidence; B is first-party institutional/public-authority; C is primary research/incident database; D is reputable media reporting. Allegations are described as allegations. No case is treated as proof that a whole institution was compromised unless the source establishes it.

ID	Year	Case	Grade
C01	2021	NTA / JEE Main fake application and fee websites	A
C02	2021	UGC fake-university list	B
C03	2022	New Alipore College website defacement	D
C04	2022	Delhi University admissions manipulation allegations	D
C05	2022	Kannur University data exposure report	C
C06	2022	AIIMS New Delhi ransomware disruption	A
C07	2023	Private university fake website case, Lucknow	D
C08	2023	UGC fake-university list	B
C09	2024	University of Mumbai CDOE impersonation	D
C10	2024	AICTE/UGC-style recognition impersonation ecosystem	A
C11	2025	Mumbai University fake social-media admissions page	D
C12	2025	BBD University fake Facebook admissions page	D
C13	2025	BHU fake WhatsApp admission offers	D
C14	2025	Bangalore University UUCMS marks-tampering case	D
C15	2025	Himachal Pradesh University website defacement	D
C16	2025	Kolkata college admissions vendor ransomware	D
C17	2025	Tezpur University fake advance-payment emails	B
C18	2025	MJPRU cloned website	D
C19	2025	Admission consultancy / quota scams	D
C20	2025	UGC fake-university list	A
C21	2026 watchlist	UGC current fake-university list	A

CASE REGISTER | C01

NTA / JEE Main fake application and fee websites

2021 • India • Admissions impersonation / payment diversion • Evidence grade A

What the public record indicates

Official alert warned candidates about fake sites purporting to receive JEE Main applications and fees.

Why this case matters to a university

The attack surface includes the institution’s identity, not only its servers. A fake admissions page or payment request can create direct victim loss while the university’s internal network remains technically uncompromised.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE S020

CASE REGISTER | C02

UGC fake-university list

2021 • India • Recognition / degree fraud • Evidence grade B

What the public record indicates

UGC-related reporting identified 24 self-styled/fake institutions; represents persistent recognition and credential fraud risk.

Why this case matters to a university

The attack surface includes the institution's identity, not only its servers. A fake admissions page or payment request can create direct victim loss while the university's internal network remains technically uncompromised.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE S021

CASE REGISTER | C03

New Alipore College website defacement

2022 • Kolkata, West Bengal • Website compromise / defacement • Evidence grade D

What the public record indicates

Media reporting said the official site was hacked/defaced immediately before admissions; restoration affected access to notices.

Why this case matters to a university

Public-facing digital services are institutional trust infrastructure. A compromise or impersonation can affect students, staff and reputation before technical teams have completed forensic confirmation.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE https://ciso.economictimes.indiatimes.com/

CASE REGISTER | C04

Delhi University admissions manipulation allegations

2022 • Delhi • Admissions / integrity manipulation • Evidence grade D

What the public record indicates

Police reportedly examined allegations involving attempts to manipulate admissions-related marks/data; mismatches led to cancellation in reported cases. Treat as alleged/investigated, not a proven system-wide breach.

Why this case matters to a university

The attack surface includes the institution's identity, not only its servers. A fake admissions page or payment request can create direct victim loss while the university's internal network remains technically uncompromised.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE https://indianexpress.com/

CASE REGISTER | C05

Kannur University data exposure report

2022 • Kerala • Data exposure • Evidence grade C

What the public record indicates

A cybersecurity incident database/media reporting described exposure of student information and dark-web posting. Not an official regulator dataset; included as a secondary case signal.

Why this case matters to a university

Public-facing digital services are institutional trust infrastructure. A compromise or impersonation can affect students, staff and reputation before technical teams have completed forensic confirmation.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE https://csidb.net/

CASE REGISTER | C06

AIIMS New Delhi ransomware disruption

2022 • Delhi • Ransomware / operational disruption • Evidence grade A

What the public record indicates

Government answers state five servers were affected, approximately 1.3 TB was encrypted, and critical e-Hospital services required roughly two weeks to restore.

Why this case matters to a university

Availability, data confidentiality and institutional continuity can fail together. Recovery planning must therefore be tested against real academic and administrative deadlines, not only technical restore objectives.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE S025 / S026

CASE REGISTER | C07

Private university fake website case, Lucknow

2023 • Lucknow, Uttar Pradesh • Brand impersonation / fake admissions • Evidence grade D

What the public record indicates

Registrar reportedly filed an FIR after a fake site mimicked a university admissions presence and redirected users; reported suspected financial motive.

Why this case matters to a university

The attack surface includes the institution's identity, not only its servers. A fake admissions page or payment request can create direct victim loss while the university's internal network remains technically uncompromised.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE https://timesofindia.indiatimes.com/

CASE REGISTER | C08

UGC fake-university list

2023 • India • Recognition / degree fraud • Evidence grade B

What the public record indicates

Contemporaneous UGC-based reporting listed 20 fake universities, showing persistence despite enforcement and awareness campaigns.

Why this case matters to a university

The attack surface includes the institution's identity, not only its servers. A fake admissions page or payment request can create direct victim loss while the university's internal network remains technically uncompromised.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE S023

CASE REGISTER | C09

University of Mumbai CDOE impersonation

2024 • Mumbai, Maharashtra • Brand impersonation / admissions scam • Evidence grade D

What the public record indicates

The university reportedly warned about a fake CDOE website/social accounts and filed a complaint with cyber police.

Why this case matters to a university

The attack surface includes the institution's identity, not only its servers. A fake admissions page or payment request can create direct victim loss while the university's internal network remains technically uncompromised.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE https://www.freepressjournal.in/

CASE REGISTER | C10

AICTE/UGC-style recognition impersonation ecosystem

2024 • India • Recognition / document fraud • Evidence grade A

What the public record indicates

Regulators repeatedly publish alerts and recognition-verification guidance; fake accreditation, approval, degree and admission claims remain a recurring ecosystem threat.

Why this case matters to a university

Public-facing digital services are institutional trust infrastructure. A compromise or impersonation can affect students, staff and reputation before technical teams have completed forensic confirmation.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE S006

CASE REGISTER | C11

Mumbai University fake social-media admissions page

2025 • Mumbai, Maharashtra • Social impersonation / data harvesting • Evidence grade D

What the public record indicates

A fake social-media admissions page reportedly solicited personal details and redirected applicants to a suspicious third-party site; complaint reported to cybercrime authorities.

Why this case matters to a university

The attack surface includes the institution's identity, not only its servers. A fake admissions page or payment request can create direct victim loss while the university's internal network remains technically uncompromised.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE https://timesofindia.indiatimes.com/

CASE REGISTER | C12

BBD University fake Facebook admissions page

2025 • Lucknow, Uttar Pradesh • Social impersonation / admissions fraud • Evidence grade D

What the public record indicates

Reports described a fake page impersonating university admissions; complaints of cheating and an FIR were reported.

Why this case matters to a university

The attack surface includes the institution's identity, not only its servers. A fake admissions page or payment request can create direct victim loss while the university's internal network remains technically uncompromised.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE https://timesofindia.indiatimes.com/

CASE REGISTER | C13

BHU fake WhatsApp admission offers

2025 • Varanasi, Uttar Pradesh • Messaging impersonation / admissions fraud • Evidence grade D

What the public record indicates

BHU reportedly cautioned candidates about WhatsApp messages offering admission and reiterated use of official channels.

Why this case matters to a university

The attack surface includes the institution's identity, not only its servers. A fake admissions page or payment request can create direct victim loss while the university's internal network remains technically uncompromised.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE https://indianexpress.com/

CASE REGISTER | C14

Bangalore University UUCMS marks-tampering case

2025 • Karnataka • Account compromise / academic integrity • Evidence grade D

What the public record indicates

Media reporting described unauthorized changes to marks after compromise of evaluation credentials, affecting 55 BCA students.

Why this case matters to a university

Academic systems are integrity systems. Unauthorized changes to marks or records can undermine the validity of decisions, credentials and student outcomes even without large-scale data theft.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE https://timesofindia.indiatimes.com/

CASE REGISTER | C15

Himachal Pradesh University website defacement

2025 • Himachal Pradesh • Website compromise / defacement • Evidence grade D

What the public record indicates

The university website was reportedly hacked/defaced and taken down while cyber investigators examined the incident.

Why this case matters to a university

Public-facing digital services are institutional trust infrastructure. A compromise or impersonation can affect students, staff and reputation before technical teams have completed forensic confirmation.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE https://www.hindustantimes.com/

CASE REGISTER | C16

Kolkata college admissions vendor ransomware

2025 • Kolkata, West Bengal • Third-party ransomware / payment fraud • Evidence grade D

What the public record indicates

Reports said a vendor serving college admissions suffered unauthorized access/ransomware and fraudulent payment instructions reached applicants, illustrating supply-chain risk.

Why this case matters to a university

Availability, data confidentiality and institutional continuity can fail together. Recovery planning must therefore be tested against real academic and administrative deadlines, not only technical restore objectives.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE https://timesofindia.indiatimes.com/

CASE REGISTER | C17

Tezpur University fake advance-payment emails

2025 • Assam • Email impersonation / payment request • Evidence grade B

What the public record indicates

A university caution reported unsolicited emails requesting advance payments or information; the institution said such requests were not official.

Why this case matters to a university

The attack surface includes the institution's identity, not only its servers. A fake admissions page or payment request can create direct victim loss while the university's internal network remains technically uncompromised.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE https://www.tezu.ernet.in/

CASE REGISTER | C18

MJPRU cloned website

2025 • Uttar Pradesh • Clone site / fee and identity risk • Evidence grade D

What the public record indicates

Media reporting described a cloned university website imitating the official domain and allegedly collecting fees/personal information; an FIR was reported.

Why this case matters to a university

Public-facing digital services are institutional trust infrastructure. A compromise or impersonation can affect students, staff and reputation before technical teams have completed forensic confirmation.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE https://timesofindia.indiatimes.com/

CASE REGISTER | C19

Admission consultancy / quota scams

2025 • Delhi / India • Admissions fraud / forged documents • Evidence grade D

What the public record indicates

Reports describe applicants/families being cheated through fake consultancy promises, official-looking letters and forged receipts. This is adjacent to, but not necessarily a compromise of, university systems.

Why this case matters to a university

The attack surface includes the institution's identity, not only its servers. A fake admissions page or payment request can create direct victim loss while the university's internal network remains technically uncompromised.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE https://timesofindia.indiatimes.com/

CASE REGISTER | C20

UGC fake-university list

2025 • India • Recognition / degree fraud • Evidence grade A

What the public record indicates

Official parliamentary answer on 1 Dec 2025 said 24 institutions were on UGC's fake-university list and described closure, FIR, warning and state-action measures.

Why this case matters to a university

The attack surface includes the institution's identity, not only its servers. A fake admissions page or payment request can create direct victim loss while the university's internal network remains technically uncompromised.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE S024

CASE REGISTER | C21

UGC current fake-university list

2026 watchlist • India • Recognition / degree fraud • Evidence grade A

What the public record indicates

UGC's February 2026 list contains 32 entities. This is outside the core 2021-2025 period and is included as a post-period risk indicator.

Why this case matters to a university

The attack surface includes the institution's identity, not only its servers. A fake admissions page or payment request can create direct victim loss while the university's internal network remains technically uncompromised.

Controls to test

- Identity and privileged-access protection
- Domain, website and social impersonation monitoring where relevant
- Immutable logging and incident evidence preservation
- Out-of-band verification for payment or high-risk record changes
- Documented escalation, communications and takedown process

SOURCE S006

INTERNATIONAL BENCHMARK

United Kingdom: 98% of universities identified a breach or attack

98%	88%	73%	43%
HIGHER EDUCATION	FURTHER EDUCATION	SECONDARY SCHOOLS	BUSINESSES

The UK government survey fielded Aug-Dec 2025 reported that 98% of higher-education institutions in the sample (n=49) identified a cyber breach or attack in the prior 12 months. The survey explicitly warns that unidentified attacks may mean prevalence is underestimated. [S010]

This is the strongest benchmark for the India exposure model because the unit is the institution and the time window is annual. It remains a UK statistic: it cannot simply be copied into an India claim.

INTERNATIONAL BENCHMARK

UK attack types among affected further/higher education

Type	Affected FE/HE
Phishing	96%
Impersonation	79%
Virus / spyware / malware	51%
Denial of service	49%
Unauthorized access by staff	29%
Unauthorized access by students	23%
Website/social/email takeover or attempt	18%
Unauthorized access by outsiders	17%
Ransomware	14%
Online bank-account hacking/attempt	10%

Attack-type percentages are conditional on institutions that identified a breach/attack, and FE+HE are combined because of base-size constraints. The pattern is directly relevant to Indian university control design: phishing and impersonation are near-universal among affected institutions, while internal access, malware, ransomware and account takeover are also non-trivial. [S010]

INTERNATIONAL BENCHMARK

UK consequences: detection is not the same as harm

49%	23%	16%	14%
AFFECTED FE/HE: NEGATIVE SYSTEM OUTCOME	COMPROMISED SYSTEMS USED ILLICITLY	SERVICES SLOWED / DOWN	LOST ACCESS TO FILES / NETWORKS

This distinction is central to this dossier's India model. The UK survey shows very high attack/breach identification at universities, but fewer affected FE/HE institutions report a negative system outcome. Exposure and impact are separate probabilities. [S010]

INTERNATIONAL BENCHMARK

UK controls: mature institutions are still targeted

98%	98%	96%	84%
HE 2FA	HE VPN	HE SECURITY MONITORING TOOLS	HE 14-DAY PATCH POLICY

The UK results are a useful antidote to “we have antivirus, therefore we are safe.” Higher education reported high adoption of core controls and still near-universal identification of attacks. Security programs therefore need both preventive hygiene and continuous detection/response. [S010]

A new 2025/26 question found 49% of higher-education institutions held employee or student personal data not protected by techniques such as anonymisation or encryption, illustrating that mature governance does not eliminate data-protection gaps. [S010]

INTERNATIONAL BENCHMARK

United States: 851 confirmed educational data disclosures

1,075	851	88%	30%
EDUCATIONAL SERVICES INCIDENTS	CONFIRMED DATA DISCLOSURES	FINANCIAL MOTIVE	RANSOMWARE: TOP MALWARE VARIETY

Verizon's 2025 DBIR Educational Services section recorded 1,075 incidents and 851 with confirmed data disclosure. System Intrusion, Miscellaneous Errors and Social Engineering represented 80% of breaches. External actors accounted for 62% of breaches and internal actors 38%; financial motive was reported in 88%, espionage in 18%. [S012]

Personal data appeared in 58% of breaches, internal data 49%, other data 35%, and credentials 12%. Error accounted for 29% of breaches, showing that not every breach is a sophisticated intrusion. [S012]

INTERNATIONAL BENCHMARK

United States: education attack path

DBIR signal	Educational Services 2025
Top patterns	System Intrusion, Miscellaneous Errors, Social Engineering
Malware action	42% of breaches
Hacking action	36% of breaches
Ransomware	30% - most prevalent malware variety
Use of stolen credentials	24% - top hacking variety
Social Engineering	16% of breaches
Within Social Engineering	77% phishing; 7% pretexting

The DBIR data reinforce the need for balanced controls: endpoint/network defense, credential protection, resilient processes that prevent error, and human anti-phishing measures. [S012]

INTERNATIONAL BENCHMARK

European Union: ransomware remains the most impactful threat

4,875	77%	60%	21.3%
ENISA INCIDENTS ANALYSED	DDoS SHARE OF REPORTED INCIDENTS	PHISHING: LEADING ACCESS POINT	VULNERABILITY EXPLOITATION

ENISA's 2025 Threat Landscape covers 4,875 incidents from 1 July 2024 to 30 June 2025. DDoS dominated incident volume, largely driven by hacktivism, while ransomware was identified as the most impactful threat. ENISA reported phishing as the leading intrusion access point, followed by vulnerability exploitation. [S013]

The EU dataset is not higher-education-specific in the headline figures, but it provides a regional threat backdrop and underscores two attack paths highly relevant to universities: human deception and unpatched/exploitable systems.

INTERNATIONAL BENCHMARK

Global education ransomware: 2025 victim survey

35%	58%	$697k	$463k
HE: EXPLOITED VULNERABILITIES	HE: DATA ENCRYPTED	HE MEDIAN DEMAND	HE MEDIAN PAYMENT

Sophos's 2025 education report surveyed 441 IT/cybersecurity leaders from education providers hit by ransomware in the previous year, including 198 higher-education providers. Because respondents were ransomware victims, these figures describe attack causes and outcomes - not the percentage of all universities hit. [S015]

Higher education reported exploited vulnerabilities as the most common technical root cause (35%); 58% of attacks resulted in encryption. Median demand was $697,000 and median payment $463,000. Mean recovery cost excluding ransom was $0.90 million. [S015]

INTERNATIONAL BENCHMARK

Ransomware trend: education has learned, attackers have adapted

Sophos's 2023 survey reported 79% of surveyed higher-education organizations had been hit by ransomware during 2022; the 2024 survey reported a lower 66% attack rate for higher education, while encryption among attacked HE organizations remained high. The 2025 report changed the relevant sample framing by focusing on victim experiences. Methodology differences mean the numbers should be read as a trend series with caution, not as a precise global prevalence curve. [S015-S016, S029]

Decision lesson

Ransomware defense should be evaluated by attack prevention, blast-radius containment, recovery reliability, data-theft detection, extortion readiness and time-to-resume critical academic services - not merely by whether backups exist.

INTERNATIONAL BENCHMARK

India breach economics: high-severity tail risk

₹22.0 cr	₹28.9 cr	18%	17%
INDIA AVG BREACH COST 2025	RESEARCH SECTOR AVG	PHISHING INITIAL VECTOR	THIRD-PARTY / SUPPLY CHAIN

IBM's 2025 Cost of a Data Breach reporting for India put the average total organizational cost at ₹220 million, up from ₹195 million in 2024. Phishing was the leading initial vector at 18%, followed by third-party/vendor/supply-chain compromise at 17% and vulnerability exploitation at 13%. The research sector recorded the highest reported India average at ₹289 million. [S014]

These are averages from studied organizations, not the expected cost for a typical Indian college. They are best used for stress testing: a single severe breach can plausibly create multi-crore impact across downtime, investigation, recovery, notification, professional services, lost activity and reputational consequences.

INDIA PREVALENCE MODEL

What can actually be estimated?

India does not publish an annual representative survey asking universities and colleges whether they identified at least one cyber breach/attack/scam in the prior 12 months. The prevalence model therefore triangulates three evidence families: (1) India's national growth in incidents, complaints and registered cases; (2) education/research attack-intensity telemetry in India; and (3) a measured institution-level comparator from UK higher education.

Evidence	Observed result	Role in model
UK HE official survey	98% identified breach/attack in prior 12 months	Sets a measured prevalence benchmark for a mature HE system.
India Check Point telemetry	Thousands of weekly attack attempts per education/research organization	Shows high exposure intensity; does not measure unique affected institutions.
CERT-In 2025	2.94m incidents nationally	Shows rapidly expanding national threat environment.
NCRP 2025	2.40m financial-fraud complaints	Shows mass scale of deception/payment risk.
Indian case register	Multiple attack classes across admissions, sites, records, ransomware, vendors	Shows relevance, not prevalence.

INDIA PREVALENCE MODEL

Modeled annual exposure: 85-95%, central ~90%

85%	90%	95%
LOW CASE	CENTRAL CASE	HIGH CASE

The model defines exposure as an institution being targeted by or encountering at least one cyberattack, scam, phishing campaign, impersonation attempt, account-takeover attempt or other malicious digital event during a year. It does not require a successful compromise.

Modeled exposure prevalence	Institutions out of 49,535
85%	42,105
90%	44,582
95%	47,058

The central estimate of 90% corresponds to approximately 44,582 universities and colleges. The range 85-95% corresponds to roughly 42,105-47,058. This scenario is deliberately set below the UK's measured 98% university prevalence while recognizing India's exceptionally high attack-intensity telemetry. It is an analytical estimate, not a government statistic.

INDIA PREVALENCE MODEL

Impact scenarios - not prevalence claims

Because India lacks representative HE outcome data, the following ranges are planning scenarios. They should be used to test program economics and control capacity, never as "X% of Indian universities were breached."

Scenario	Illustrative range	Count across 49,535 institutions	Interpretation
Exposure / targeting	85-95%	42,105-47,058	At least one malicious attempt/encounter.
Meaningful detected compromise	40-65%	19,814-32,198	Scenario only: unauthorized access/action detected.
Negative operational/financial/system outcome	20-45%	9,907-22,291	Scenario only: downtime, illicit use, loss, diversion, data impact.
Material serious event	10-25%	4,954-12,384	Scenario only: serious breach/ransomware/major fraud/integrity event.

The UK official survey provides an observed reference point for one conditional transition: among affected FE/HE institutions, 49% reported a negative system outcome. That cannot be directly transposed to India, but it shows why a very high exposure rate can coexist with a lower rate of harmful outcomes. [S010]

INDIA PREVALENCE MODEL

Sensitivity: what changes the estimate?

Factor	Pushes modeled exposure	Reason
Stricter definition: only successful breaches	Down	Excludes blocked phishing, impersonation and attack attempts.
Broader definition: scams targeting students using university brand	Up	Includes attacks outside university-owned infrastructure.
Better monitoring / SOC capability	Observed rate up	More attempts and breaches become visible.
Low reporting / weak telemetry	Observed rate down	Incidents may remain undetected or undocumented.
Peak admissions/exam windows	Seasonal intensity up	Attackers exploit urgency, payments and public communications.
Large multi-campus institution	Attack surface up	More identities, domains, vendors, endpoints and delegated systems.

For a sales or board deck, the safest headline remains: “An estimated 9 in 10 Indian universities and colleges may encounter at least one cyberattack, scam or impersonation attempt in a year.” The footnote should say “modeled estimate; not an official India prevalence statistic.”

REGULATORY CONTEXT

CERT-In: six-hour incident reporting changes operational readiness

CERT-In's 28 April 2022 directions apply to categories including body corporates and government organizations and require specified cyber incidents to be reported within six hours of noticing or being informed. CERT-In's FAQs clarify that available information may be supplied first, with additional information later. [S007-S008]

University implication

A six-hour reporting clock makes "we will figure out the incident process during the breach" untenable. Institutions need a named point of contact, severity criteria, evidence-preservation procedure, decision authority, legal/compliance escalation and a pre-drafted reporting workflow.

Operational minimum

- 24/7 route for high-severity alerts
- Incident commander and deputies
- Time-synchronized logs retained per applicable requirements
- Evidence capture without destroying forensic value
- Pre-approved regulator/law-enforcement escalation map
- Third-party contracts requiring prompt notification

REGULATORY CONTEXT

DPDP Act/Rules: personal-data security becomes board- relevant

MeitY published the Digital Personal Data Protection Rules, 2025 on 14 November 2025, alongside enforcement-timeline materials and Data Protection Board establishment documents. The exact commencement of provisions and institution-specific obligations must be checked against the official timeline and any applicable exemptions. [S009]

For higher education, the practical risk question is broader than legal compliance: can the institution identify what personal data it holds, who has access, how vendors process it, what security safeguards apply, how quickly a breach can be assessed, and how affected individuals will be handled?

This report is not legal advice. Institutions should obtain legal interpretation for specific statutory duties, exemptions, effective dates and contractual obligations.

INSTITUTIONAL CYBERSECURITY PROGRAM

01. Governance and board oversight

A higher-education security program should be evaluated by whether it reduces the probability and consequence of the specific scam and attack classes documented in this report. Controls below are deliberately framed as auditable outcomes.

- ☐ Assign accountable executive and board reporting cadence
- ☐ Maintain risk register tied to academic/business services
- ☐ Define cyber risk appetite and exception process
- ☐ Track controls, incidents, near misses and fraud losses as management metrics

Evidence to request

Policy or standard; configuration/export proving implementation; recent test result; accountable owner; remediation backlog; incident/exception history; and a date for the next review. “We use product X” is not evidence that the control outcome exists.

INSTITUTIONAL CYBERSECURITY PROGRAM

02. Identity and access management

A higher-education security program should be evaluated by whether it reduces the probability and consequence of the specific scam and attack classes documented in this report. Controls below are deliberately framed as auditable outcomes.

- ☐ MFA for all feasible access; phishing-resistant MFA for privileged/admin roles
- ☐ Separate admin identities from daily-use accounts
- ☐ Automated joiner/mover/leaver process
- ☐ Conditional access and impossible-travel/anomalous-login detection
- ☐ Quarterly privileged-access review

Evidence to request

Policy or standard; configuration/export proving implementation; recent test result; accountable owner; remediation backlog; incident/exception history; and a date for the next review. “We use product X” is not evidence that the control outcome exists.

INSTITUTIONAL CYBERSECURITY PROGRAM

03. Email, domain and brand protection

A higher-education security program should be evaluated by whether it reduces the probability and consequence of the specific scam and attack classes documented in this report. Controls below are deliberately framed as auditable outcomes.

- ☐ SPF, DKIM and DMARC with enforcement roadmap
- ☐ Lookalike-domain monitoring and takedown workflow
- ☐ Monitor official social identities and admissions impersonation
- ☐ Publish authoritative payment/admissions channels
- ☐ Rapid banner/notice process during active scams

Evidence to request

Policy or standard; configuration/export proving implementation; recent test result; accountable owner; remediation backlog; incident/exception history; and a date for the next review. “We use product X” is not evidence that the control outcome exists.

INSTITUTIONAL CYBERSECURITY PROGRAM

04. Endpoint, server and network defense

A higher-education security program should be evaluated by whether it reduces the probability and consequence of the specific scam and attack classes documented in this report. Controls below are deliberately framed as auditable outcomes.

- ☐ EDR or equivalent endpoint telemetry
- ☐ Network segmentation around critical systems
- ☐ Secure configuration baselines
- ☐ Vulnerability scanning and patch SLA
- ☐ Asset inventory including shadow/departmental systems
- ☐ Restrict exposed remote management

Evidence to request

Policy or standard; configuration/export proving implementation; recent test result; accountable owner; remediation backlog; incident/exception history; and a date for the next review. “We use product X” is not evidence that the control outcome exists.

INSTITUTIONAL CYBERSECURITY PROGRAM

05. Application and ERP security

A higher-education security program should be evaluated by whether it reduces the probability and consequence of the specific scam and attack classes documented in this report. Controls below are deliberately framed as auditable outcomes.

- ☐ Secure SDLC for institution-built systems
- ☐ Independent security testing for critical apps
- ☐ Strong authorization tests on APIs and object access
- ☐ Admin actions logged and reviewed
- ☐ Change control for marks, fees, admission and credentials

Evidence to request

Policy or standard; configuration/export proving implementation; recent test result; accountable owner; remediation backlog; incident/exception history; and a date for the next review. “We use product X” is not evidence that the control outcome exists.

INSTITUTIONAL CYBERSECURITY PROGRAM

06. Ransomware resilience

A higher-education security program should be evaluated by whether it reduces the probability and consequence of the specific scam and attack classes documented in this report. Controls below are deliberately framed as auditable outcomes.

- ☐ Immutable/offline backup tier
- ☐ Documented RTO/RPO by critical service
- ☐ Restore tests, not backup-success dashboards
- ☐ Segmentation and privileged-access containment
- ☐ Extortion communications and legal/law-enforcement plan
- ☐ Critical-service manual fallback

Evidence to request

Policy or standard; configuration/export proving implementation; recent test result; accountable owner; remediation backlog; incident/exception history; and a date for the next review. “We use product X” is not evidence that the control outcome exists.

INSTITUTIONAL CYBERSECURITY PROGRAM

07. Financial fraud controls

A higher-education security program should be evaluated by whether it reduces the probability and consequence of the specific scam and attack classes documented in this report. Controls below are deliberately framed as auditable outcomes.

- ☐ Dual approval for beneficiary/master-data change
- ☐ Out-of-band verification of payment instructions
- ☐ Applicant fee page with fixed official beneficiary guidance
- ☐ High-risk transaction hold/review
- ☐ Fraud reporting channel and rapid victim communications

Evidence to request

Policy or standard; configuration/export proving implementation; recent test result; accountable owner; remediation backlog; incident/exception history; and a date for the next review. “We use product X” is not evidence that the control outcome exists.

INSTITUTIONAL CYBERSECURITY PROGRAM

08. Admissions and student protection

A higher-education security program should be evaluated by whether it reduces the probability and consequence of the specific scam and attack classes documented in this report. Controls below are deliberately framed as auditable outcomes.

- ☐ Official channel registry
- ☐ Applicant anti-scam warnings at every high-risk step
- ☐ No-admission-via-WhatsApp policy where applicable
- ☐ Verified social accounts and fake-page monitoring
- ☐ Easy “is this real?” verification mechanism

Evidence to request

Policy or standard; configuration/export proving implementation; recent test result; accountable owner; remediation backlog; incident/exception history; and a date for the next review. “We use product X” is not evidence that the control outcome exists.

INSTITUTIONAL CYBERSECURITY PROGRAM

09. Vendor and supply-chain risk

A higher-education security program should be evaluated by whether it reduces the probability and consequence of the specific scam and attack classes documented in this report. Controls below are deliberately framed as auditable outcomes.

- ☐ Vendor inventory with service criticality
- ☐ Security requirements and breach-notification SLA
- ☐ Scoped access and MFA for vendor identities
- ☐ Evidence-based assurance, not questionnaire-only
- ☐ Exit/offboarding and data-return/destruction requirements

Evidence to request

Policy or standard; configuration/export proving implementation; recent test result; accountable owner; remediation backlog; incident/exception history; and a date for the next review. “We use product X” is not evidence that the control outcome exists.

INSTITUTIONAL CYBERSECURITY PROGRAM

10. Detection and MDR/SOC operations

A higher-education security program should be evaluated by whether it reduces the probability and consequence of the specific scam and attack classes documented in this report. Controls below are deliberately framed as auditable outcomes.

- ☐ Centralize critical logs
- ☐ 24/7 coverage for high-severity signals
- ☐ Use cases for identity, payment, ERP and web compromise
- ☐ Threat intelligence tuned to education brand/sector
- ☐ Metrics: MTTD, MTTC, false-positive burden, recurring root cause

Evidence to request

Policy or standard; configuration/export proving implementation; recent test result; accountable owner; remediation backlog; incident/exception history; and a date for the next review. “We use product X” is not evidence that the control outcome exists.

INSTITUTIONAL CYBERSECURITY PROGRAM

11. Incident response and evidence

A higher-education security program should be evaluated by whether it reduces the probability and consequence of the specific scam and attack classes documented in this report. Controls below are deliberately framed as auditable outcomes.

- ☐ Severity matrix
- ☐ Named incident commander
- ☐ Preserve logs/images/communications
- ☐ Six-hour CERT-In workflow where applicable
- ☐ Tabletop exercises with registrar, finance, admissions, legal, PR
- ☐ Post-incident corrective-action tracking

Evidence to request

Policy or standard; configuration/export proving implementation; recent test result; accountable owner; remediation backlog; incident/exception history; and a date for the next review. “We use product X” is not evidence that the control outcome exists.

INSTITUTIONAL CYBERSECURITY PROGRAM

12. Human security and culture

A higher-education security program should be evaluated by whether it reduces the probability and consequence of the specific scam and attack classes documented in this report. Controls below are deliberately framed as auditable outcomes.

- ☐ Role-based training rather than annual generic module
- ☐ Phishing simulations with coaching
- ☐ Finance/admissions verification drills
- ☐ Student-facing scam awareness
- ☐ Executive deepfake/urgent-payment procedure
- ☐ Measure reporting speed, not only click rate

Evidence to request

Policy or standard; configuration/export proving implementation; recent test result; accountable owner; remediation backlog; incident/exception history; and a date for the next review. “We use product X” is not evidence that the control outcome exists.

INSTITUTIONAL CYBERSECURITY PROGRAM

90-day implementation roadmap

Window	Priority outcomes
Days 0-15	Executive owner; critical-service map; incident contacts; privileged identity inventory; active scam/brand monitoring; emergency payment-verification rule.
Days 16-30	MFA gaps closed on privileged systems; central logging for email/identity/core apps; vulnerability triage; backup restore test; vendor criticality list.
Days 31-60	Incident tabletop; domain/email controls; ERP integrity logging; high-risk payment workflow; admissions scam-awareness campaign; supplier notification clauses.
Days 61-90	24/7 detection path; penetration/vulnerability assessment remediation; measured phishing drill; second restore test; board metrics; residual-risk and investment plan.

Success test at day 90

The institution should be able to answer, with evidence: What are our most critical digital services? Who is attacking or impersonating us? Which identity can do the most damage? Can we restore core services? Can finance/admissions detect diverted payment instructions? Can we report a severe incident within the required window? Can leadership see residual risk in one page?

INSTITUTIONAL CYBERSECURITY PROGRAM

Board dashboard - suggested monthly metrics

Metric	What it reveals	Red flag
Critical assets with current owner	Accountability/coverage	Unknown assets or owners
Privileged identities protected by strong MFA	Identity blast radius	Exceptions on ERP/email/cloud admins
Critical vulnerabilities past SLA	Exploit exposure	Recurring internet-facing backlog
Mean time to contain high-severity alerts	Response effectiveness	Hours/days without ownership
Backup restore success for critical services	Resilience	Backups never restore-tested
Impersonation domains/pages detected and removed	Brand-fraud pressure	No monitoring despite public scams
High-risk payment changes independently verified	Fraud control	Email-only beneficiary changes
Critical vendors with current assurance	Supply chain	Unknown subcontractors/access
Phishing/reporting drill result	Human detection	Low reporting or slow reporting
Open post-incident actions	Learning loop	Repeat root causes

STATE / UT CYBERCRIME PROFILE

Telangana

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

27,230	26.7%	+442%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
5,024	10,303	15,297	18,236	27,230

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Karnataka

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

21,993	21.6%	+105%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
10,741	8,136	12,556	21,889	21,993

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Uttar Pradesh

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

11,073	10.9%	-0%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
11,097	8,829	10,117	10,794	11,073

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Maharashtra

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

9,922	9.7%	+81%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
5,496	5,562	8,249	8,103	9,922

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Bihar

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

6,380	6.3%	+322%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
1,512	1,413	1,621	4,450	6,380

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Tamil Nadu

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

5,793	5.7%	+641%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
782	1,076	2,082	4,121	5,793

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Kerala

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

2,962	2.9%	+595%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
426	626	773	3,295	2,962

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Andhra Pradesh

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

2,528	2.5%	+33%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
1,899	1,875	2,341	2,341	2,528

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Odisha

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

2,501	2.5%	+30%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
1,931	2,037	1,983	2,348	2,501

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Haryana

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

1,815	1.8%	+177%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
656	622	681	751	1,815

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Gujarat

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

1,592	1.6%	+24%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
1,283	1,536	1,417	1,995	1,592

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Rajasthan

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

1,527	1.5%	+13%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
1,354	1,504	1,833	2,435	1,527

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Jharkhand

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

1,423	1.4%	+18%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
1,204	953	967	1,079	1,423

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Madhya Pradesh

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

1,081	1.1%	+55%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
699	589	826	685	1,081

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Punjab

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

888	0.9%	+135%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
378	551	697	511	888

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Delhi

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

404	0.4%	+140%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
168	356	685	407	404

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Himachal Pradesh

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

148	0.1%	+51%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
98	70	77	127	148

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

STATE / UT CYBERCRIME PROFILE

Assam

NCRB registered cybercrime cases - general environment proxy, not a higher-education victim count.

408	0.4%	-88%
2024 CASES	SHARE OF INDIA 2024	CHANGE 2020-2024

2020	2021	2022	2023	2024
3,530	4,846	1,733	909	408

Interpretation for university outreach

Use these numbers as geographic context when briefing institutions in the state. They do not show how many universities or colleges were victims. Differences may reflect population, reporting propensity, police registration, digital activity and other factors. The appropriate institutional next step is local risk assessment, not a state-label assumption.

Institution questions

- What incidents and scams did the institution itself record in the last 12 months?
- Which public-facing brands/domains and payment channels are monitored?
- Does the institution track fraud attempts against applicants even when internal systems are not breached?
- Can the institution map local law-enforcement and CERT-In escalation paths before a severe event?

SOURCE [S001]

APPENDIX A

Full NCRB State/UT table, 2020-2024

State/UT	2020	2021	2022	2023	2024
Andhra Pradesh	1,899	1,875	2,341	2,341	2,528
Arunachal Pradesh	30	47	14	24	78
Assam	3,530	4,846	1,733	909	408
Bihar	1,512	1,413	1,621	4,450	6,380
Chhattisgarh	297	352	439	473	660
Goa	40	36	90	86	77
Gujarat	1,283	1,536	1,417	1,995	1,592
Haryana	656	622	681	751	1,815
Himachal Pradesh	98	70	77	127	148
Jharkhand	1,204	953	967	1,079	1,423
Karnataka	10,741	8,136	12,556	21,889	21,993
Kerala	426	626	773	3,295	2,962
Madhya Pradesh	699	589	826	685	1,081
Maharashtra	5,496	5,562	8,249	8,103	9,922
Manipur	79	67	18	3	5
Meghalaya	142	107	75	64	97
Mizoram	13	30	1	31	50
Nagaland	8	8	4	2	14
Odisha	1,931	2,037	1,983	2,348	2,501
Punjab	378	551	697	511	888
Rajasthan	1,354	1,504	1,833	2,435	1,527
Sikkim	0	0	26	12	15
Tamil Nadu	782	1,076	2,082	4,121	5,793
Telangana	5,024	10,303	15,297	18,236	27,230
Tripura	34	24	30	36	33
Uttar Pradesh	11,097	8,829	10,117	10,794	11,073
Uttarakhand	243	718	559	494	543
West Bengal	712	513	401	309	282
A&N Islands	5	8	28	47	28
Chandigarh	17	15	27	23	116
D&N Haveli and Daman & Diu	3	5	5	6	5

State/UT	2020	2021	2022	2023	2024
Delhi	168	356	685	407	404
Jammu & Kashmir	120	154	173	185	114
Ladakh	1	5	3	1	1
Lakshadweep	3	1	1	1	0
Puducherry	10	0	64	147	142
ALL INDIA	50,035	52,974	65,893	86,420	101,928

SOURCE [S001]

APPENDIX B

Institutional Cyber Fraud & Resilience Assessment

Suggested scoring: 0 = absent; 1 = informal; 2 = documented; 3 = implemented; 4 = implemented and evidenced/tested. Items carry a suggested importance weight shown in parentheses. This is a commercial assessment framework, not a statutory certification.

APPENDIX B - ASSESSMENT

Governance

Control outcome	Weight	Score	Notes
Board/executive owner is formally assigned	3	0 1 2 3 4	Evidence / action: _____
Cyber risk is reviewed at least quarterly	2	0 1 2 3 4	Evidence / action: _____
Risk exceptions have owners and expiry dates	3	0 1 2 3 4	Evidence / action: _____
Material incidents trigger documented board escalation	3	0 1 2 3 4	Evidence / action: _____

Decision rule

Any score of 0-1 on a weight-4 item should be treated as a near-term remediation candidate. A high total score should not override a single catastrophic gap such as unprotected privileged access or untested recovery.

APPENDIX B - ASSESSMENT

Identity

Control outcome	Weight	Score	Notes
MFA covers all privileged accounts	4	0 1 2 3 4	Evidence / action: _____
Privileged admins use separate accounts	4	0 1 2 3 4	Evidence / action: _____
Leavers are disabled rapidly and automatically	3	0 1 2 3 4	Evidence / action: _____
Dormant accounts are reviewed	2	0 1 2 3 4	Evidence / action: _____
High-risk logins generate actionable alerts	3	0 1 2 3 4	Evidence / action: _____

Decision rule

Any score of 0-1 on a weight-4 item should be treated as a near-term remediation candidate. A high total score should not override a single catastrophic gap such as unprotected privileged access or untested recovery.

APPENDIX B - ASSESSMENT

Email & brand

Control outcome	Weight	Score	Notes
DMARC is deployed with enforcement roadmap	3	0 1 2 3 4	Evidence / action: _____
Lookalike domains are monitored	3	0 1 2 3 4	Evidence / action: _____
Fake social/admissions accounts have takedown process	3	0 1 2 3 4	Evidence / action: _____
Official payment/admission channels are public and easy to verify	4	0 1 2 3 4	Evidence / action: _____

Decision rule

Any score of 0-1 on a weight-4 item should be treated as a near-term remediation candidate. A high total score should not override a single catastrophic gap such as unprotected privileged access or untested recovery.

APPENDIX B - ASSESSMENT

Vulnerability & infrastructure

Control outcome	Weight	Score	Notes
Asset inventory covers internet-facing and departmental systems	4	0 1 2 3 4	Evidence / action: _____
Critical patches follow defined SLA	4	0 1 2 3 4	Evidence / action: _____
External attack surface is continuously reviewed	3	0 1 2 3 4	Evidence / action: _____
Network segmentation protects critical systems	4	0 1 2 3 4	Evidence / action: _____

Decision rule

Any score of 0-1 on a weight-4 item should be treated as a near-term remediation candidate. A high total score should not override a single catastrophic gap such as unprotected privileged access or untested recovery.

APPENDIX B - ASSESSMENT

Data & applications

Control outcome	Weight	Score	Notes
Sensitive data has an owner and retention rule	3	0 1 2 3 4	Evidence / action: _____
Critical applications undergo security testing	4	0 1 2 3 4	Evidence / action: _____
ERP/marks/admin changes are logged immutably	4	0 1 2 3 4	Evidence / action: _____
APIs enforce server-side authorization	4	0 1 2 3 4	Evidence / action: _____

Decision rule

Any score of 0-1 on a weight-4 item should be treated as a near-term remediation candidate. A high total score should not override a single catastrophic gap such as unprotected privileged access or untested recovery.

APPENDIX B - ASSESSMENT

Resilience

Control outcome	Weight	Score	Notes
Critical backups are immutable/offline	4	0 1 2 3 4	Evidence / action: _____
Restore tests occur at least quarterly for critical services	4	0 1 2 3 4	Evidence / action: _____
RTO/RPO are service-specific	3	0 1 2 3 4	Evidence / action: _____
Manual fallback exists for critical academic/administrative operations	3	0 1 2 3 4	Evidence / action: _____

Decision rule

Any score of 0-1 on a weight-4 item should be treated as a near-term remediation candidate. A high total score should not override a single catastrophic gap such as unprotected privileged access or untested recovery.

APPENDIX B - ASSESSMENT

Fraud controls

Control outcome	Weight	Score	Notes
Beneficiary changes require independent verification	4	0 1 2 3 4	Evidence / action: _____
High-value payments use dual approval	4	0 1 2 3 4	Evidence / action: _____
Admissions teams have scam-response playbook	3	0 1 2 3 4	Evidence / action: _____
Victims can rapidly verify suspicious university messages	3	0 1 2 3 4	Evidence / action: _____

Decision rule

Any score of 0-1 on a weight-4 item should be treated as a near-term remediation candidate. A high total score should not override a single catastrophic gap such as unprotected privileged access or untested recovery.

APPENDIX B - ASSESSMENT

Third parties

Control outcome	Weight	Score	Notes
Critical vendor inventory is current	3	0 1 2 3 4	Evidence / action: _____
Contracts require rapid incident notification	4	0 1 2 3 4	Evidence / action: _____
Vendor access is scoped and MFA protected	4	0 1 2 3 4	Evidence / action: _____
Evidence-based assurance is reviewed periodically	3	0 1 2 3 4	Evidence / action: _____

Decision rule

Any score of 0-1 on a weight-4 item should be treated as a near-term remediation candidate. A high total score should not override a single catastrophic gap such as unprotected privileged access or untested recovery.

APPENDIX B - ASSESSMENT

Detection & response

Control outcome	Weight	Score	Notes
High-severity monitoring is 24/7	4	0 1 2 3 4	Evidence / action: _____
Critical logs are centralized and time-synchronized	4	0 1 2 3 4	Evidence / action: _____
Incident roles and contacts are current	4	0 1 2 3 4	Evidence / action: _____
CERT-In reporting workflow is documented where applicable	4	0 1 2 3 4	Evidence / action: _____
Tabletops involve IT, finance, admissions, legal and communications	3	0 1 2 3 4	Evidence / action: _____

Decision rule

Any score of 0-1 on a weight-4 item should be treated as a near-term remediation candidate. A high total score should not override a single catastrophic gap such as unprotected privileged access or untested recovery.

APPENDIX B - ASSESSMENT

Human layer

Control outcome	Weight	Score	Notes
Training is role-based	2	0 1 2 3 4	Evidence / action: _____
Phishing drills measure reporting speed	2	0 1 2 3 4	Evidence / action: _____
Finance/admissions practice verification scenarios	3	0 1 2 3 4	Evidence / action: _____
Students receive scam warnings during peak periods	2	0 1 2 3 4	Evidence / action: _____

Decision rule

Any score of 0-1 on a weight-4 item should be treated as a near-term remediation candidate. A high total score should not override a single catastrophic gap such as unprotected privileged access or untested recovery.

APPENDIX C

How to present the evidence without overclaiming

Use	Recommended wording
Headline prevalence	“An estimated 85-95% of Indian universities and colleges may encounter at least one cyberattack, scam or impersonation attempt annually; central modeled estimate ~90%.”
Footnote	“Model-based estimate using India national cyber trends, education/research attack telemetry and international HE prevalence benchmarks. Not an official India prevalence statistic.”
National trend	“CERT-In observed 2.94 million cyber security incidents in 2025; NCRP/CFCFRMS logged 2.40 million financial-fraud complaints in the 2025 annual table.”
International comparator	“UK official survey: 98% of higher-education institutions identified a breach or attack in the prior 12 months.”
Cost context	“IBM’s 2025 India study estimated average breach cost at ₹22 crore across studied organizations; research sector average ₹28.9 crore.”

Never say

- “90% of Indian colleges are hacked every year.”
- “8,487 attacks per week means every university is breached 8,487 times.”
- “₹22 crore is what a college will lose if breached.”
- “Every fake admission page means the university’s servers were compromised.”

APPENDIX C

Procurement questions for a cybersecurity program

- ☐ What exact threats are covered: network compromise, identity, payment fraud, brand impersonation, ransomware, academic-integrity attacks and third parties?
- ☐ Which controls are preventive vs detective vs response?
- ☐ What telemetry does the provider need and where is it stored?
- ☐ What happens at 2:00 AM on a holiday if a high-severity alert fires?
- ☐ Who can authorize containment of an account, endpoint or service?
- ☐ How are false positives, service exclusions and residual risk reported?
- ☐ What evidence proves controls are working every month?
- ☐ How does the program support CERT-In reporting and evidence preservation?
- ☐ What is the process for fake-domain/social-page detection and takedown?
- ☐ How are admissions and finance workflows integrated rather than treated as purely IT issues?
- ☐ What are RTO/RPO and incident response commitments?
- ☐ What exit provisions guarantee data/log portability and secure offboarding?

SOURCE REGISTER

Primary and comparative sources

Accessed 30 July 2026 unless the source itself carries a publication date shown below. Media homepages in case references are pointers to the contemporaneous report family; before quoting a media-only case externally, the original article should be retained in the institution’s due-diligence file.

SOURCE REGISTER

Sources 1-5

S001 National Cyber Crime Data

Ministry of Home Affairs / Press Information Bureau | 21 Jul 2026

Official NCRB 2020-2024 state and crime-head tables; latest published Crime in India year is 2024.

https://www.pib.gov.in/PressReleasePage.aspx?PRID=2287039&lang=1&reg=3

S002 Cyber financial fraud complaints and reported amount via NCRP/CFCFRMS

Ministry of Home Affairs / Press Information Bureau | 11 Feb 2026

Official annual 2021-2025 complaint and reported-amount table. Data are dynamic.

https://www.pib.gov.in/PressReleasePage.aspx?PRID=2226441&lang=1&reg=1

S003 Assistance to States to Tackle Cyber Incidents

Ministry of Home Affairs / Press Information Bureau | 24 Mar 2026

Official CERT-In incident counts for 2021-2025.

https://www.pib.gov.in/PressReleasePage.aspx?PRID=2244504&lang=1&reg=3

S004 CERT-In: India's Frontline Defender against Cyber Threats

Press Information Bureau / CERT-In | 23 Jan 2026

2025 CERT-In operational statistics, alerts, audits, drills and capacity building.

https://www.pib.gov.in/PressReleasePage.aspx?PRID=2217537&lang=1&reg=3

S005 All India Survey on Higher Education 2023-24

Department of Higher Education, Ministry of Education | Jul 2026

Official AISHE frame: 1,289 universities, 48,246 colleges, 15,221 standalone institutions.

https://www.dohe-education.gov.in/static/uploads/2026/07/8616f33dfee644ab6b87a2bd0658b18d.pdf

SOURCE REGISTER

Sources 6-10

S006 HEIs Violating Regulations - List of Fake Universities

University Grants Commission | Feb 2026 list; page current Jul 2026

Official current fake-university list: 32 entities as of Feb 2026.

https://www.ugc.gov.in/universitydetails/HEIs_Violating_Regulations?tab=fakeuni

S007 Directions under section 70B(6), Information Technology Act

CERT-In | 28 Apr 2022

Mandatory incident-reporting directions; specified incidents reportable within six hours.

https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

S008 FAQs on Cyber Security Directions

CERT-In | May 2022

Clarifies six-hour reporting and what may be supplied initially.

https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf

S009 Digital Personal Data Protection Rules, 2025

Ministry of Electronics and Information Technology | 14 Nov 2025

Official Rules, corrigendum and enforcement-timeline materials.

https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa

S010 Cyber security breaches survey 2025/2026: education institutions findings

UK Department for Science, Innovation and Technology | 30 Apr 2026

Official UK survey; fieldwork Aug-Dec 2025; HE n=49.

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-education-institutions-findings

SOURCE REGISTER

Sources 11-15

S011 Cyber security breaches survey 2025: education institutions findings

UK Department for Science, Innovation and Technology | 10 Apr 2025

Official prior-year UK benchmark.

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-education-institutions-findings

S012 2025 Data Breach Investigations Report - Educational Services

Verizon | 2025

Educational Services: 1,075 incidents, 851 confirmed data disclosures.

https://www.verizon.com/business/resources/T838/reports/2025-dbir-data-breach-investigations-report.pdf

S013 ENISA Threat Landscape 2025

ENISA | 1 Oct 2025

EU threat landscape analyzing 4,875 incidents, Jul 2024-Jun 2025.

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

S014 India Records Highest Average Cost of a Data Breach at INR 220 million in 2025

IBM | 7 Aug 2025

India average breach cost; attack vectors; research-sector average cost.

https://in.newsroom.ibm.com/2025-08-07-India-Records-Highest-Average-Cost-of-a-Data-Breach-IBM

S015 The State of Ransomware in Education 2025

Sophos | 2025

Survey of 441 education IT/cyber leaders hit by ransomware in prior year.

https://www.sophos.com/en-gb/resources/white-papers/state-of-ransomware-in-education

SOURCE REGISTER

Sources 16-20

S016 The State of Ransomware in Education 2023

Sophos | Jul 2023

Higher-ed ransomware survey benchmark.

https://www.sophos.com/en-us/press/press-releases/2023/07/the-state-of-ransomware-in-education

S017 Education sector sees 29% increase in attacks globally

Check Point Research | 2021

Vendor telemetry: India education/research 5,196 weekly attacks per organization in Jul 2021.

https://blog.checkpoint.com/security/check-point-research-education-sector-sees-29-increase-in-attacks-against-organizations-globally/

S018 Education Sector as Top Target in 2024

Check Point Research | 13 Aug 2024

Vendor telemetry: India education/research 6,874 weekly attacks per organization.

https://blog.checkpoint.com/research/check-point-research-warns-every-day-is-a-school-day-for-cybercriminals-with-the-education-sector-as-the-top-target-in-2024/

S019 India education and research threat intelligence benchmark

Economic Times CIO / Check Point Software | 2025

Contemporaneous reporting of Check Point India threat-intelligence figure: 8,487 attacks per week over prior six months; treated as vendor telemetry, not prevalence.

https://ciso.economictimes.indiatimes.com/amp/news/cybercrime-fraud/indias-education-sector-faces-alarming-surge-in-cyberattacks-8487-weekly-threats-uncovered/121876688

S020 Alert against fake website(s) to receive online application and fee payment for JEE Main 2021

National Testing Agency / JEE Main | 2021

Official admissions-ecosystem fake-website warning.

https://jeemain.nta.nic.in/

SOURCE REGISTER

Sources 21-25

S021 UGC declares 24 self-styled institutions fake

Indian Express | 2021

Contemporaneous report based on UGC list.

https://indianexpress.com/

S022 UGC lists 21 fake universities

Indian Express | 2022

Contemporaneous report based on UGC list.

https://indianexpress.com/

S023 UGC lists 20 fake universities

Indian Express | 2023

Contemporaneous report based on UGC list.

https://indianexpress.com/

S024 Lok Sabha Unstarred Question 135: Fake Universities

Parliament of India / Ministry of Education | 1 Dec 2025

Official answer: 24 institutions on UGC fake-university list; enforcement steps described.

https://sansad.in/getFile/loksabhaquestions/annex/186/AU135_P0SH7F.pdf?source=pqals

S025 Rajya Sabha Unstarred Question 1223 - AIIMS cyber incident

Parliament of India / Ministry of Electronics and IT | Dec 2022

Official: improper network segmentation, five servers, ~1.3 TB data encrypted.

https://sansad.in/getFile/annex/258/AU1223.pdf?source=pqars

SOURCE REGISTER

Sources 26-30

S026 Rajya Sabha Unstarred Question 1478 - AIIMS cyber incident

Parliament of India / Ministry of Health | Dec 2022

Official: critical e-Hospital services restored after about two weeks; manual operations during disruption.

https://sansad.in/getFile/annex/258/AU1478.pdf?source=pqars

S027 Cyber incident / ransomware public information

University of Maribor | 2024

Institutional notice on ransomware-related disruption in 2024.

https://www.um.si/en/

S028 Fake College of Suffolk website warning

Suffolk Trading Standards / Suffolk County Council | 18 Jan 2024

UK public-authority example of university-brand/admissions impersonation.

https://www.suffolk.gov.uk/

S029 Most Educational Organizations Paid More Than Original Ransom Demand

Sophos | Sep 2024

2024 global ransomware education survey.

https://www.sophos.com/en-us/press/press-releases/2024/09/most-educational-organizations-paid-more-original-ransom-demand-says

S030 Cyber Attacks and Cyber Security in Schools

Verizon | 2025

Education-sector context derived from 2025 DBIR.

https://www.verizon.com/business/resources/articles/s/data-security-in-higher-education-and-universities/

APPENDIX D

Core national data tables

NCRB registered cybercrime cases

Year	All cybercrime cases	Fraud-head cases	Cheating cases
2020	50,035	10,395	4,480
2021	52,974	14,007	6,343
2022	65,893	17,470	10,509
2023	86,420	19,466	16,943
2024	101,928	29,758	19,296

CERT-In incidents

Year	Cyber security incidents observed
2021	1,402,809
2022	1,391,457
2023	1,592,917
2024	2,041,360
2025	2,944,248

NCRP/CFCFRMS financial cyber fraud

Year	Complaints	Reported amount (₹ crore)
2021	262,846	551
2022	694,446	2,290
2023	1,310,357	7,465
2024	1,918,835	22,848
2025	2,402,579	22,495

SOURCE [S001-S003]

APPENDIX D

Derived growth rates - transparent calculations

Series	From	To	Start	End	Total change	CAGR
NCRB all cybercrime	2020	2024	50,035	101,928	+103.7%	19.5%
NCRB fraud head	2020	2024	10,395	29,758	+186.3%	30.1%
CERT-In incidents	2021	2025	1,402,809	2,944,248	+109.9%	20.4%
NCRP complaints	2021	2025	262,846	2,402,579	+814.1%	73.9%
NCRP reported amount	2021	2025	551	22,495	+3982.6%	152.8%

CAGR = (ending / beginning)^(1 / number of intervals) - 1. These are calculations from the cited official source values, not additional government statistics.

APPENDIX D

Selected international benchmark table

Dataset	Population / frame	Headline	Key limitation
UK CSBS 2025/26	49 HE institutions; official survey	98% identified breach/attack in prior 12 months	Small HE sample; UK context; self-identified incidents.
Verizon 2025 DBIR	Global contributed incident/breach data; Educational Services	1,075 incidents; 851 confirmed disclosures	Contributor visibility; not institution prevalence.
ENISA TL 2025	4,875 EU incidents	DDoS 77%; ransomware most impactful; phishing leading access point	Not HE-specific in headline figures.
Sophos Education 2025	441 education ransomware victims; 198 HE	HE encryption 58%; exploited vulnerabilities 35%	Victim-only sample; not prevalence.
IBM India 2025	Studied breach organizations	₹22 cr average India cost; research ₹28.9 cr	Cost average, not expected HEI loss.
Check Point India education	Vendor telemetry	Thousands of attacks/org/week	Attempts/telemetry; not unique breaches.

CONCLUSION

The institutional decision

Indian universities do not need an invented “breach percentage” to justify cybersecurity investment. The hard evidence is already sufficient: national cyber incidents and financial-fraud complaints have risen dramatically; registered cybercrime and fraud-head cases have climbed; education/research telemetry shows extraordinary attack intensity; fake universities and admissions impersonation persist; Indian institutions have experienced ransomware, website compromise, record-integrity incidents and vendor-linked fraud; and the strongest comparable official higher-education survey finds near-universal annual attack identification.

The reasonable planning assumption is therefore that attempted digital abuse is routine, not exceptional. The modeled 85-95% annual exposure range - central ~90% - expresses that planning reality while preserving statistical honesty. The cybersecurity program that follows from the evidence must protect not only servers, but identity, money, academic integrity, applicant trust, research, third parties and institutional continuity.

The line to carry into a governing-body meeting

> “The question is no longer whether our institution will be targeted. The question is whether we can identify the attempt, prove what happened, prevent trust from being converted into loss, contain the event quickly, and continue the academic mission.”

SOURCE [S001-S019; C01-C21]