THREAT INTELLIGENCE & SECTOR RISK ASSESSMENT

Cyber Fraud in Indian Higher Education

An evidence review of scams, frauds and cyber intrusions affecting Indian universities and colleges, 2020–2026, with comparative analysis of the United Kingdom, United States and European Union

Prepared by	Fortify Detection & Intelligence Wing (FDIW) · fdiw.org
Edition	First edition — July 2026
Coverage period	2020 to July 2026; Indian and international data
Institutional base assessed	64,456 registered Indian higher education institutions (AISHE 2023-24)
Primary sources	40 sourced references — see Appendix A
Intended readership	Registrars, directors, vice-chancellors, chief financial officers, IT heads, controllers of examinations, tender evaluation committees
Classification	Confidential — for institutional distribution

On the use of figures in this document. No Indian authority publishes a measured rate of cyber fraud incidence among universities and colleges. This report says so plainly and constructs a labelled estimate from named sources rather than asserting a number. Every quantitative claim carries a bracketed reference resolving to the Source Register at Appendix A. Estimates are identified as estimates and their derivation is shown. Section 18 sets out, in detail, the ways in which this report could be wrong. It is written on the assumption that a document arguing for security must itself withstand audit.

Contents

Tables

1. Executive Summary

> **The single most important finding in this report is not the attack rate. It is the detection gap.** Indian higher education institutions are, by every available measure, the most heavily targeted sector in the country. They are also among the least instrumented to know it. The distance between those two facts is where institutional liability now accumulates.

1.1 The headline estimate

There is no published, measured figure for the percentage of Indian universities and colleges that experience online fraud in a given year. No Indian authority — not the University Grants Commission (UGC), the All India Council for Technical Education (AICTE), the Indian Computer Emergency Response Team (CERT-In), the National Crime Records Bureau (NCRB), nor the Indian Cyber Crime Coordination Centre (I4C) — publishes sector-segmented institutional incident rates for higher education. This report states that absence plainly rather than concealing it, because the absence is itself one of the findings.

What can be done, and what this report does, is construct a defensible estimate from four independent evidence streams: (a) Indian education-sector attack telemetry from commercial sensor networks; (b) the Indian national cybercrime and cyber-financial-fraud baseline; (c) documented Indian institutional incidents; and (d) directly measured institutional incident rates from comparable jurisdictions, principally the United Kingdom, where the government conducts an annual statistically designed survey of universities and colleges.

The resulting estimate is expressed as a four-layer ladder rather than a single number, because "facing a scam or fraud" means four materially different things, and conflating them is how vendors lose credibility with procurement committees.

Table 1.1 — Estimated annual incidence, Indian higher education institutions (per 12-month period)

Layer	Definition	Estimate	Confidence
L1 — Targeted	Institution is subject to at least one attempted attack or fraud event: phishing, credential stuffing, automated vulnerability scanning, brand impersonation, or fraudulent solicitation of its students in its name.	approx. 100%	High
L2 — Impacted	At least one event produces a real consequence: funds lost, personal data exposed, an account compromised and misused, a service disrupted, a portal defaced, or a fee/admission fraud successfully executed against applicants using the institution's identity.	85–95%	Moderate
L3 — Institution-internal impact only	Excludes fraud committed against students and applicants in the institution's name; counts only compromise of institution-operated systems, accounts, funds or data.	60–75%	Moderate
L4 — Detected	The institution actually identifies the event, contemporaneously or within the same year, through its own monitoring or a report reaching its administration.	20–35%	Low–Moderate
L5 — Disclosed	The event is disclosed to a regulator, to affected data principals, or publicly.	under 5%	Moderate

The figure to quote, if a single figure is required, is L2: approximately 85 to 95 percent, with a central working estimate of 90 percent. It should always be quoted with its definition attached and labelled as an estimate. The nearest directly measured analogue in the world — the UK Government's Cyber Security Breaches Survey — found that 98 percent of higher education institutions identified a breach or attack in the preceding twelve months [S9]. India has a higher per-organisation attack volume and a lower average security maturity than the United Kingdom. There is no credible mechanism by

which the Indian figure would be materially lower.

1.2 Ten findings

1. **Education is the most attacked sector in India.** Seqrite Labs, monitoring more than 8 million endpoints, recorded 265.52 million detections between October 2024 and September 2025. Education accounted for nearly 24 percent of them — 4.92 million detections — the largest share of any Indian industry [S5].
2. **Per-institution attack volume is extreme.** Check Point Research measured Indian education at an average of 7,095 cyberattacks per organisation per week, placing the sector above government bodies and consumer goods companies [S7]. Globally, Check Point found education the most targeted sector, at between 4,248 and 9,817 attacks per organisation per week [S6].
3. **Indian institutions are measurably weaker than international peers.** A CyberPeace Foundation pilot study recorded more than 200,000 cyberattacks and nearly 400,000 data breaches across participating Indian educational institutions in nine months, and concluded that Indian institutions are likely five times more vulnerable to data breaches than counterparts with stronger practices [S8].
4. **The credentials being used against them are trivial.** The same study found brute-force campaigns cycling more than 8,000 unique usernames and 54,000 unique passwords, with "root" and "admin" among the most-targeted accounts and "123456" and "password" among the most-attempted credentials [S8]. This is not sophisticated attack; it is unlocked-door attack.
5. **Indian breaches persist for years before discovery.** The August 2025 IIT Roorkee exposure — names, mobile numbers, caste category, financial background, email addresses and graduation details for more than 30,000 students and alumni — originated in records left openly accessible on a public-facing website, with evidence suggesting the database may have been reachable for over a decade [S24]. This is the detection gap made concrete at one of India's best-resourced institutions.
6. **Fraud in the institution's name is now an industrialised market.** CYFIRMA documented a cloned university website in December 2025 collecting student fees and personal data behind convincing academic content, alongside dark-web advertisement of structured datasets containing millions of Indian student records including admission details and payment data [S25]. The institution is the brand being counterfeited; it bears the reputational loss whether or not its own servers were touched.
7. **The regulatory clock is running and the penalties are institution-ending.** The Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025. Penalty provisions activate 13 November 2026; full compliance is required by 13 May 2027. Failure to maintain reasonable security safeguards attracts a penalty of up to Rs. 250 crore; failure to notify a breach, up to Rs. 200 crore; penalties are assessed per violation and can stack [S27].
8. **Examination fraud is now a criminal-liability question for institutions, not only a disciplinary one.** The Public Examinations (Prevention of Unfair Means) Act, 2024 came into force on 21 June 2024. Organised offences carry five to ten years' imprisonment and a minimum fine of Rs. 1 crore, and the enumerated offences explicitly include tampering with a computer resource and creating fake examination websites [S28].
9. **The international comparison does not flatter India — it indicts the measurement, not the threat.** The UK measures its institutional incidence annually and finds 98 percent [S9]. The United States requires Title IV institutions to report breaches and has accumulated 3,173 education breaches across two decades [S17]. India measures nothing comparable. India's apparently lower incident counts are an artefact of not looking.
10. **Third-party and shared-platform risk is the dominant multiplier.** In 2025 global education ransomware counts were essentially flat — 251 attacks against 247 the prior year — while breached records rose 27 percent to 3.96 million, driven by a small number of large third-party compromises

[S15]. A single shared examination or student-information platform is now the highest-consequence asset most institutions own and the one they control least.

1.3 What this means for an institution deciding whether to act

The defensible reading of the evidence is not "you will probably be attacked." It is: **you are being attacked now, the attacks are mostly unsophisticated, you almost certainly cannot see them, and from November 2026 not seeing them becomes a quantified financial liability rather than an operational embarrassment.**

Every figure in this report is sourced. Where a figure is an estimate, it is labelled as an estimate and its derivation is shown. Where Indian data does not exist, this report says so. Section 23 sets out the limitations of the entire evidence base, including the limitations of the sources this report relies on most heavily.

2. Scope, Method and Data Integrity Statement

2.1 What this report covers

This report assesses the incidence, typology, cost and regulatory consequence of online scams, frauds and cyber intrusions affecting higher education institutions in India between 2020 and mid-2026, with comparative analysis against the United Kingdom, the United States and the European Union. It covers fraud committed *against* institutions, fraud committed *through* institutional systems, and fraud committed *in the name of* institutions against their students, applicants and staff. All three categories are treated as institutional exposure, because in each case the institution absorbs financial, regulatory or reputational loss.

It does not cover academic misconduct unmediated by digital systems, physical security, or campus safety. It does not cover schools (K-12) except where school-sector data is the only available proxy for a phenomenon, in which case the substitution is stated explicitly.

2.2 Method

Evidence was assembled from five source classes, listed in descending order of the weight given to them:

1. **Government statistical instruments.** NCRB *Crime in India*; Ministry of Education All India Survey on Higher Education (AISHE); Ministry of Home Affairs parliamentary replies; UK Department for Science, Innovation and Technology (DSIT) Cyber Security Breaches Survey; ENISA Threat Landscape. These are given primary weight because their methodologies and sample designs are published.
2. **Statutory and regulatory instruments.** The Digital Personal Data Protection Act, 2023 and Rules, 2025; the Public Examinations (Prevention of Unfair Means) Act, 2024 and Rules; CERT-In directions; state examination ordinances.
3. **Sector-specific research from non-commercial bodies.** CyberPeace Foundation, Jisc, EDUCAUSE, MS-ISAC.
4. **Commercial vendor telemetry and research.** Seqrite, Check Point, Sophos, Comparitech, CYFIRMA, Cyble, Bitsight, Microsoft. These are the richest source of education-sector specifics and are used extensively, but they carry a structural bias discussed in Section 23 and are always attributed to the vendor by name.
5. **Documented individual incidents.** Reported breaches at named institutions, used as illustration and existence-proof, never as a basis for rate estimation.

2.3 Data integrity commitments

This document is intended to be read by university registrars, chief financial officers, directors, IT heads and tender evaluation committees. Its usefulness depends entirely on its figures surviving scrutiny. Accordingly:

- Every quantitative claim carries a bracketed source reference resolving to the Source Register at Appendix A, which gives publisher, publication, period covered, and where known the sample size and methodology.
- Estimates are labelled as estimates, with their derivation shown, and are never presented in the same typographic register as measured figures.
- Where Indian data does not exist, the report states that it does not exist rather than substituting a foreign figure silently. Where a foreign figure is used as a proxy, the substitution and its justification are stated in the same sentence.

- Vendor-sourced figures are attributed to the vendor in the running text, not laundered into the passive voice. A detection count from a vendor sensor network is not an incident count and is not presented as one.
- Figures that are widely circulated but not traceable to a primary source have been excluded, however useful they would have been.
- Section 23 sets out, in detail, the ways in which this report could be wrong.

2.4 A necessary distinction: detections, attacks, incidents, breaches

Most confusion in this field, and most vendor overclaiming, comes from sliding between four quantities that differ by orders of magnitude. This report holds them apart throughout.

Table 2.1 — Units of measurement and what they do and do not mean

Unit	What it counts	What it does NOT mean
Detection	A single event flagged by a security product. One phishing email opened on three devices may generate several.	An attack. Detections number in the millions nationally and are dominated by blocked, low-consequence events.
Attack / attempt	A discrete adversarial action directed at an asset: one phishing campaign, one scan, one credential-stuffing run.	A compromise. The overwhelming majority of attempts fail or are blocked.
Incident	An attempt that produced a consequence requiring response: an account compromised, a service disrupted, funds moved.	A reportable breach. Many incidents involve no personal data.
Breach	An incident in which personal data was accessed, exposed, altered or lost.	A disclosed breach. Under the DPDP framework this distinction now carries a monetary penalty.

When this report says Indian education recorded 4.92 million detections [S5], that is a detection count from one vendor's sensor network and nothing more. When it says 98 percent of UK higher education institutions identified a breach or attack [S9], that is a survey-measured institutional incidence rate. The two are not comparable and are never compared in this document.

3. The Denominator: Scale of the Indian Higher Education Sector

Any incidence percentage requires a denominator. The authoritative count comes from the All India Survey on Higher Education (AISHE), conducted annually by the Ministry of Education since 2011. The 2023-24 edition is the most recent released.

Table 3.1 — Indian higher education institutional base, AISHE 2023-24 [S22]

Category	Count	Note
Universities / university-level institutions	1,289	Degree-awarding powers. Includes 18 women's universities and 19 open universities.
Colleges	48,246	Constituent, recognised or affiliated with universities. Approximately 70 percent are private unaided.
Standalone institutions	15,221	Outside the universities and colleges structure: technical/polytechnic, teacher training, nursing.
Total registered HEIs	64,456	4,376 added in a single year.
Total student enrolment	4.50 crore	Gross Enrolment Ratio 30.0, up from 23.7 in 2014-15.
Total faculty	17.32 lakh	44.9 percent women.
Foreign students hosted	58,134	From 173 countries.
AISHE participation rate	approx. 92%	59,553 of 64,756 registered institutions submitted data.

3.1 Why the structure of the sector matters to the risk picture

Three structural features of this denominator drive the risk profile, and each is a reason the Indian figure should be expected to exceed rather than trail the UK figure.

First, the sector is overwhelmingly composed of small private colleges. Roughly 70 percent of the 48,246 colleges are private unaided [S22]. An institution of this type typically has no dedicated security function, no security operations centre, no incident response retainer, and often a single IT administrator maintaining a website, a student management system, a fee payment integration and a campus network simultaneously. The UK sector, by contrast, comprises roughly 285 higher education providers, most with a named information security officer and all with access to a shared national security operations centre operated by Jisc [S13]. India has no equivalent shared defensive infrastructure for higher education.

Second, the data held is unusually sensitive by Indian standards. Indian institutions collect Aadhaar numbers, caste category, income certificates, scholarship banking details, photographs, birth certificates and medical records as a routine condition of admission. This is a materially more sensitive record than a Western university's student file, and it is precisely the combination required to open a bank account or take a loan in a student's name. The IIT Roorkee exposure included caste category and financial background alongside contact details [S24].

Third, the transaction volume is enormous and seasonally concentrated. With 4.50 crore students enrolled and roughly 400,000 net new entrants annually [S22], admission and fee cycles create predictable windows in which tens of millions of families are expecting to make payments to institutions they have never transacted with before, often on newly created portals, frequently under deadline pressure. This is close to an ideal condition for payment fraud, and it recurs on a published calendar.

Implication for estimation. A denominator of 64,456 institutions dominated by small, under-resourced private colleges holding Aadhaar-linked financial and caste data, transacting at scale on a predictable seasonal calendar, with no shared national defensive infrastructure. Against the UK's approximately 285 well-resourced providers with a national SOC, the structural expectation is that Indian incidence is at least as high and Indian detection is far lower.

4. The National Baseline: Indian Cybercrime and Cyber-Financial Fraud

Institutional education fraud does not occur in isolation. It sits inside a national fraud economy that has grown by roughly an order of magnitude in four years. The national trend establishes the direction of travel and the adversary capability that institutions face.

4.1 Recorded cybercrime, NCRB

Table 4.1 — Cybercrime cases registered in India, NCRB [S1][S2]

Year	Cases registered	Change	Rate per lakh population
2021	52,974 (over 52,000)	—	—
2022	65,893	+24.4%	—
2023	86,420	+31.2%	6.2
2024	1,01,928	+17.9%	7.3

In 2024, cyber fraud dominated the category: 73,987 cases, or 72.6 percent of all cybercrime cases, were fraud-motivated [S1]. Telangana recorded the highest volume at 27,230 cases, close to a 50 percent rise on 2023, followed by Karnataka at 21,003 [S1]. Roughly 35,000 cases were registered in metro cities [S1].

Two features of this dataset matter for how it should be used. First, the 2024 report is the first compiled substantially under the Bharatiya Nyaya Sanhita, which changed crime categorisation, so year-on-year comparison across 2023-24 requires caution [S1]. Second, and more importantly for this report's argument: **NCRB counts registered cases, which is to say cases where a victim reported and a police station registered.** Institutional victims very rarely register. An institution that discovers a student database has leaked has strong incentives to handle it quietly. NCRB is therefore a floor, and for institutional incidents a very low one.

The enforcement picture reinforces why institutions do not report. NCRB data for 2023 indicates that 22 percent of cybercrimes were charged and fewer than 3 percent resulted in conviction at trial [S38]. An institution weighing the reputational cost of disclosure against a 3 percent chance of conviction has, until the DPDP Rules, faced a rational incentive toward silence.

4.2 Cyber-financial fraud losses, I4C

The Indian Cyber Crime Coordination Centre operates the National Cyber Crime Reporting Portal (NCRP) and the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS). Its loss figures are the best available measure of the money moving through the Indian fraud economy.

Table 4.2 — Reported cyber-financial fraud losses and complaint volumes, I4C / NCRP [S3][S4]

Year	Reported losses	Complaints	Loss multiple vs 2022
2022	Rs. 2,290.23 crore	—	1.0x
2023	Rs. 7,463.20 crore	15.96 lakh	3.3x
2024	Rs. 22,849.49 crore	19,18,852	10.0x
2025	Rs. 19,812.96 crore	21,77,524	8.7x
2020–2025 cumulative	Rs. 52,976 crore	—	—

2025 alone accounted for Rs. 19,812 crore, close to one-third of the entire six-year loss total [S3]. Complaint volume rose in 2025 even as headline losses dipped from the 2024 peak, indicating a higher

number of smaller-ticket frauds — consistent with a broadening of the victim base rather than any reduction in criminal activity [S3]. State-level concentration in 2025: Maharashtra Rs. 3,203 crore, Karnataka Rs. 2,413 crore, Tamil Nadu Rs. 1,897 crore, Uttar Pradesh Rs. 1,443 crore, Telangana Rs. 1,372 crore, together over half the national total [S3].

Complaint volume on the NCRP grew from approximately 4.5 lakh in 2021 to over 22 lakh by 2024, a rise of more than 400 percent in four years [S4]. I4C projections cited in late 2025 estimated India might lose in excess of Rs. 1.2 lakh crore to cyber fraud across the year on a broader definition, equivalent to roughly 0.7 percent of GDP [S37].

4.3 The offshore and mule-account infrastructure

Institutional fraud is executed on shared criminal infrastructure, which is why an institution's exposure is not proportional to its own prominence. Of nearly 12 lakh cyber fraud complaints recorded in 2024, approximately 45 percent originated from Southeast Asian jurisdictions including Cambodia, Myanmar and Laos [S39]. I4C has reported blocking approximately 24.67 lakh Layer-1 mule accounts, preventing further losses of over Rs. 4,631 crore, and maintains a Suspect Registry holding more than 11 lakh identifiers [S40].

The operational consequence for an institution is specific: a fraudulent fee-collection portal impersonating a college in Bihar can be built, hosted, monetised through mule accounts and cashed out through offshore rails by an organisation with no connection to or interest in that college beyond its brand. The institution cannot deter this by being unimportant.

5. Education-Sector Attack Telemetry, India

This is the strongest India-specific evidence available, and it comes overwhelmingly from commercial sensor networks. It is presented with that provenance stated in every instance.

5.1 Seqrite: education is India's most-attacked sector

Seqrite Labs, the enterprise arm of Quick Heal, monitored more than 8 million endpoints and recorded 265.52 million detections between October 2024 and September 2025 — an average of 505 detections per minute across its India footprint. Education accounted for nearly 24 percent of all detections, at 4.92 million, making it the most heavily targeted Indian industry in the dataset [S5].

Seqrite attributes the sector's exposure to a sprawling digital footprint, an open collaboration model, and uneven security maturity, with attackers leveraging unpatched systems, shared Wi-Fi networks and poorly secured research infrastructure to drive credential theft, data exfiltration and cryptomining [S5]. Notably, Seqrite records that the threat extends beyond malware into impersonation-led scams: fake institution websites, fraudulent scholarship offers and fake job postings designed to extract identity documents, academic records and bank details from students and applicants [S5].

> **Reading this figure correctly.** 4.92 million detections is not 4.92 million attacks and is certainly not 4.92 million breaches. It is a count of flagged events across one vendor's installed base. Its analytic value is entirely in the *share*: education taking 24 percent of national detections, more than any other sector, in a country where education is not the largest sector by endpoint count. That ratio is the finding.

5.2 Check Point: per-organisation attack rates

Check Point Research measured the Indian education sector at an average of 7,095 cyberattacks per organisation per week, placing it above government institutions and consumer goods companies in the Indian ranking [S7]. Check Point's *State of Cyber Security in India 2025* reported that Indian organisations across all sectors faced an average of 2,011 attacks per week, substantially above the global average, and identified education as the most targeted sector worldwide at between 4,248 and 9,817 attacks per organisation per week [S6].

The comparison worth drawing is internal: Indian education at 7,095 weekly attacks per organisation against the Indian all-sector average of 2,011 [S6][S7]. Indian educational institutions absorb roughly three and a half times the attack volume of the average Indian organisation, while typically operating with a fraction of the security budget of an Indian bank or IT services firm.

5.3 CyberPeace Foundation e-Kawach: the closest thing to an Indian institutional study

The single most directly relevant Indian study is a pilot conducted under CyberPeace Foundation's e-Kawach initiative in collaboration with DELNET, Resecurity and Autobot Infosec, titled *Exploring Cyber Threats and Digital Risks to Indian Educational Institutions*, covering July 2023 to April 2024 and released in August 2025 [S8].

Across participating institutions over nine months it recorded more than 200,000 cyberattacks and nearly 400,000 data breaches. Brute-force campaigns cycled more than 8,000 unique usernames and 54,000 unique passwords; the most-targeted account names were "root" and "admin", and the most-attempted passwords included "123456" and "password" [S8].

Its central conclusion, stated in the report, is that **Indian educational institutions are likely five times more vulnerable to data breaches than counterparts with stronger cyber practices**, and that consequences include impersonation of faculty, phishing, deepfake content, theft of research data and leakage of examination papers [S8].

The study's limitations must be stated: it is described as a pilot, the participating institution count and sampling frame are not published in the coverage available, and participation in a security pilot is self-selecting. It cannot support a national incidence rate. What it does support — and this is not small — is that when Indian institutions are actually instrumented, the attack volume found is very large and the attacks are unsophisticated.

5.4 Corroborating Indian telemetry

- **CloudSEK (2022):** India was the single largest target of cyber threats to educational institutions and online learning platforms globally, ahead of the USA, UK, Indonesia and Brazil. Of education-sector threats detected across Asia-Pacific, 58 percent targeted Indian or India-based institutions and platforms, with Indonesia a distant second at 10 percent [S30].
- **Cyble (H1 2024):** India recorded 593 cyberattacks, 388 data breaches, 107 data leaks and 39 ransomware incidents in the first half of 2024 across all sectors [S31].
- **Microsoft Digital Defense Report 2025:** 39 percent of identity-based attacks Microsoft observed targeted research and academic institutions [S19]. Identity is the primary attack surface in this sector, not perimeter.
- **Bitsight:** 45 percent of all universities have at least one internet-facing asset running end-of-life PHP, and approximately 10 percent have open Remote Desktop Protocol ports. The education sector averages 151 days to remediate known exploited vulnerabilities [S20].

The Bitsight finding on end-of-life PHP deserves emphasis in an Indian context, because the Indian higher education web estate is disproportionately built on PHP hosted on shared or low-cost infrastructure. An institution running an unsupported PHP version on a public-facing student portal, with a 151-day average remediation window against adversaries who weaponise disclosed vulnerabilities within days, is not exposed to a hypothetical risk.

6. Typology: The Twelve Fraud Patterns Affecting Indian Institutions

Aggregate attack counts do not help an institution decide what to fix. This section decomposes the threat into the twelve distinct patterns evidenced in the Indian record, each with its mechanism, the party that bears the loss, and the observable evidence that it is occurring.

Table 6.1 — Fraud typology, Indian higher education

#	Pattern	Mechanism	Loss borne by
1	Fee and admission payment fraud	Cloned portal or spoofed payment link intercepts fee payments during admission windows. A cloned university website collecting fees and personal data was documented in December 2025 [S25].	Student/family; institution reputationally
2	Fake institution / degree fraud	Unrecognised entities award degrees; UGC-listed fake universities rose from 22 to 32 between October 2025 and February 2026 [S23].	Student; sector-wide trust
3	Student data breach and resale	Exposure of Aadhaar-linked records, caste category, financial background, contact data. IIT Roorkee: 30,000+ records [S24]. Dark-web datasets of millions of Indian student records advertised [S25].	Institution (DPDP liability); student
4	Credential compromise and account takeover	Brute-force and credential stuffing against admin accounts; "root"/"admin" with weak passwords are the primary targets [S8]. 39 percent of Microsoft-observed identity attacks hit academia [S19].	Institution
5	Business email compromise / vendor payment fraud	Impersonation of finance officers, vendors or the bursar to redirect procurement or payroll payments. Impersonation reported by 90 percent of UK HEIs experiencing incidents [S12].	Institution directly
6	Examination paper leakage via digital custody failure	Compromise of the systems holding question papers between setting and delivery. Explicitly named as a consequence of institutional breach [S8]; explicitly criminalised [S28].	Institution (criminal exposure); candidates
7	Examination portal compromise	Unauthorised access to assessment platforms. A 2023 disclosure affected an exam platform serving 1,000+ Indian institutions, approximately 1 million students and 65,000+ teachers [S33].	Institution; platform vendor
8	Scholarship and financial-aid fraud	Fraudulent scholarship offers harvesting identity and banking documents; diversion of genuine disbursements. Named by Seqrite as a growing impersonation vector [S5].	Student; state exchequer
9	Fake placement and job-offer fraud	Fraudulent job postings issued under the institution's placement-cell identity to extract documents and fees [S5].	Student; institution reputationally
10	Ransomware and operational disruption	Encryption or extortion halting admissions, examinations or results. In global higher education, exploited vulnerabilities were the leading root cause at 35 percent [S14].	Institution
11	Website defacement and hacktivism	Politically motivated defacement of institutional web properties. The Rajasthan Education Department site was defaced with inflammatory content in April 2025 [S34]; IIT Kanpur and IIT Madras sites were defaced in July 2026 by a rejected applicant [S32].	Institution reputationally
12	Research and IP exfiltration	Theft of research data and intellectual property, including by state-aligned actors. Named as a consequence in the Indian institutional study [S8] and a driver of academic targeting [S5].	Institution; funders; national interest

6.1 The three patterns most institutions systematically underweight

Patterns 1, 2, 8 and 9 do not require the institution to be breached at all. They require only that the institution's name, logo and reputation be usable. An institution with a perfectly secured network is fully exposed to all four. This is the single most common analytical error made by institutional IT functions: they scope the problem to assets they control, when the majority of fraud volume in this sector

operates on brand rather than infrastructure. Seqrite identifies precisely this shift, noting that the threat is no longer limited to malware and now includes fake institution websites, fraudulent scholarship offers and fake job postings [S5].

Pattern 3 is the one that has become a balance-sheet item. Before November 2026, a student data leak was a reputational event. After the DPDP penalty provisions activate, it is a quantified financial exposure of up to Rs. 250 crore for inadequate safeguards and a further Rs. 200 crore for failure to notify [S27]. The IIT Roorkee pattern — data left publicly reachable for possibly a decade, discovered externally [S24] — is precisely the fact pattern that maps onto "failure to maintain reasonable security safeguards."

Patterns 6 and 7 carry criminal rather than civil exposure. The Public Examinations (Prevention of Unfair Means) Act, 2024 enumerates tampering with a computer resource, and creating fake examination websites or issuing fake admit cards, as offences; organised offences carry five to ten years' imprisonment and a minimum Rs. 1 crore fine [S28]. An examination custody failure is no longer only an academic integrity matter.

7. The Documented Indian Incident Record, 2020–2026

This section is an existence-proof, not a rate estimate. India has no mandatory breach disclosure regime for educational institutions, so the incidents below are those that reached public reporting — a small and non-random subset of the total. Their analytic value is in what they reveal about mechanism, dwell time and discovery route.

Table 7.1 — Selected documented incidents affecting Indian educational and research institutions

Date	Institution / target	Nature and scale	Discovery route
Nov 2022	AIIMS Delhi	Ransomware halting operations. Five servers and approximately 1.3 TB of data affected; medical and personal records of close to four crore patients feared compromised [S26].	Operational failure
Nov 2022	ICMR	Approximately 6,000 breach attempts against the website within 24 hours, days after the AIIMS incident [S26].	Monitoring
2023	Examination platform serving 1,000+ institutions	Authentication weakness in a third-party examination portal permitting administrative password reset and access to student records, conducted examinations, questions, answers and results. Client base included multiple IITs and large private universities; approximately 1 million students and 65,000+ teachers in scope [S33].	External researcher
Jul 2023 – Apr 2024	Multiple institutions (e-Kawach cohort)	200,000+ cyberattacks and nearly 400,000 data breaches recorded across participating institutions in nine months [S8].	Instrumented study
Apr 2025	Rajasthan Education Department	Website compromised; homepage modified to display inflammatory messages [S34].	Public visibility
Aug 2025	IIT Roorkee	30,000+ student and alumni records exposed — names, mobile numbers, caste category, financial background, email addresses, graduation details. Originated from academic affairs records left openly accessible on a public-facing website; evidence suggested the database may have been reachable for over a decade [S24].	External disclosure
Dec 2025	Cloned university website (unnamed)	Fraudulent site collecting student fees and personal data while displaying convincing academic content [S25].	Threat intelligence
Dec 2025	Thane (individual case)	Former academic counsellor booked for using retained student records to fraudulently collect over Rs. 48,000 while posing as active staff [S25].	Victim complaint
2025–2026	Indian student data (dark web)	Threat actors advertising structured datasets containing millions of student records from Indian education platforms, including PII, admission details and payment data [S25].	Threat intelligence
Jul 2026	IIT Kanpur, IIT Madras	Websites defaced by a rejected applicant to the undergraduate cybersecurity programme, who publicised the intrusion on social media [S32].	Attacker publicity

7.1 What the discovery-route column shows

Read the right-hand column of Table 7.1 as the most important data in this report. Of ten documented incidents, the number discovered by the affected institution's own security monitoring is **one**. The rest were discovered because a service stopped working, because an external researcher reported it, because a threat intelligence vendor found the data for sale, or because the attacker announced it.

This is the empirical basis for the L4 detection estimate of 20 to 35 percent in Table 1.1. It is also the specific reason the DPDP breach notification obligation is dangerous for Indian institutions: an institution cannot notify within a statutory window a breach it will not learn about for a decade.

The IIT Roorkee case is the argument in miniature. One of the best-resourced technical institutions in India, with world-class computer science faculty, left student records including caste category and financial background publicly reachable for a period possibly exceeding ten years, and did not find it themselves [S24]. If this is the posture at an IIT, the posture at a private affiliated college in a tier-three city is not a matter requiring speculation.

8. Fake Institutions and Credential Fraud

This category is distinctive to the Indian market and has no close analogue in the UK or US comparators. It represents fraud against the sector's trust infrastructure rather than against any single institution's systems, and it directly degrades the commercial value of legitimate accreditation.

Table 8.1 — UGC-declared fake universities, distribution [S23]

State / UT	Count (Feb 2026)	State / UT	Count (Feb 2026)
Delhi (incl. New Delhi)	12	Karnataka	2
Uttar Pradesh	4	Kerala	2
Andhra Pradesh	2	Maharashtra	2
Puducherry	2	West Bengal	2
Arunachal Pradesh	1	Haryana	1
Jharkhand	1	Rajasthan	1
		Total	**32**

The count rose from 22 institutions in October 2025 to 32 by February 2026, across 12 to 13 states, with Haryana, Rajasthan, Jharkhand and Arunachal Pradesh appearing on the list for the first time [S23]. UGC issues periodic public notices naming individual entities; in December 2025 it warned specifically about institutions in Karnataka, Delhi and Maharashtra, and separately about entities in Delhi and Kerala [S23].

8.1 Why the count understates the phenomenon

The UGC list captures entities that have come to regulatory attention and that style themselves as universities. It does not capture: purely online operations with no physical presence; entities offering "certifications" or "diplomas" that avoid the word "university"; cloned websites impersonating *genuine* institutions, which are a separate and larger category [S25]; or document-forgery operations selling counterfeit degrees from real institutions.

That last category is the one that transfers loss to legitimate institutions directly. Every leaked student record containing a name, enrolment number, programme and graduation year is raw material for a forged credential attributed to that institution. The IIT Roorkee exposure included precisely this combination [S24], and dark-web datasets of Indian student records are advertised as including enrolment records and examination centre bookings [S25]. An institution's degree verification function becomes unreliable in proportion to how much of its student register has leaked.

9. Examination Integrity as a Cybersecurity Problem

India treats examination paper leakage as a law-and-order and academic-integrity issue. The evidence indicates it is now substantially a systems-security issue, and Indian law has been amended to reflect that.

9.1 The statutory position

The Public Examinations (Prevention of Unfair Means) Act, 2024 was passed by the Lok Sabha on 6 February 2024 and the Rajya Sabha on 9 February 2024, received Presidential assent in February 2024, and was brought into force on 21 June 2024 — days after the UGC-NET and NEET-UG controversies [S28]. It is India's first dedicated central law against organised examination fraud.

The enumerated offences are notable for how many are computer offences. They include leakage of question paper or answer key; **tampering with a computer network, computer resource or computer system**; **creation of a fake website to cheat or for monetary gain**; conduct of fake examinations and issuance of fake admit cards or offer letters; and manipulation of seating arrangements, dates and shifts [S28].

Table 9.1 — Penalty structure, examination fraud [S28][S29]

Instrument	Offender	Custodial	Financial
Public Examinations Act, 2024	Individual	3 to 5 years	Up to Rs. 10 lakh
Public Examinations Act, 2024	Organised group / institution	5 to 10 years	Minimum Rs. 1 crore
Proposed 2026 amendment (Cabinet-approved July 2026)	Enhanced tier	Up to 10 years	Up to Rs. 10 crore
UP Public Examinations Ordinance, 2024	Individual / organised	2 years to life	Rs. 1 crore

A special fast-track court at Delhi's Rouse Avenue Court has been designated to expedite trial of examination paper leak cases under the Act, and Cabinet approved amendments in July 2026 raising the maximum custodial term to ten years and financial penalties to Rs. 10 crore [S28]. Uttar Pradesh's state ordinance additionally makes distribution of fake examination papers and creation of fake employment websites punishable, with sentences extending to life imprisonment [S29].

9.2 Scale of the disruption when custody fails

The UGC-NET examination of June 2024 was cancelled after being conducted across 317 cities with over 1.1 million candidates — the first national-level examination scrapped after the anti-paper-leak law came into force [S28]. NEET-PG 2024 was postponed as a precautionary measure [S28]. The CBI was directed to investigate allegations in both UGC-NET and NEET-UG [S28].

The relevant institutional lesson is about the shape of the loss, not its cause. A custody failure at a single point produced a cancellation affecting 1.1 million candidates across 317 cities [S28]. The cost is not proportional to the number of papers leaked; it is proportional to the number of candidates whose examination becomes untrustworthy, which is the entire cohort. This is a catastrophic-tail risk with a very small triggering event, which is the characteristic risk profile that justifies cryptographic custody controls rather than procedural ones.

9.3 Why procedural controls are insufficient

The dominant Indian control model for examination custody is procedural: sealed envelopes, designated custodians, treasury or bank strongrooms, signed handover registers, and increasingly encrypted email or a password-protected download at the centre. Every element of this model shares one property — **at some point a small number of individuals hold, simultaneously and unilaterally, the capability**

to disclose the paper. Procedural control detects a breach after the fact, through investigation, and attributes it probabilistically.

The Indian institutional evidence indicates the digital layer of this model is the weak point. The e-Kawach study names leakage of examination papers explicitly among the consequences of institutional breach [S8]. The 2023 examination platform disclosure demonstrated administrative access to conducted examinations, questions and answers across 1,000+ institutions through a single authentication weakness [S33]. Both point to the same conclusion: where custody depends on the integrity of an administrative account, custody is exactly as strong as that account's password.

The control class that addresses this is threshold cryptography — splitting the decryption capability such that no single custodian, and no single compromised administrative account, can reconstruct the paper, combined with an append-only cryptographic custody ledger that makes any access attempt independently verifiable after the fact. This is a design property, not a policy, and it is the specific gap between current Indian practice and the standard the statutory penalty regime now implies.

10. Comparative Analysis I: The United Kingdom

The United Kingdom is the most valuable comparator in this report, for one reason: it is the only major jurisdiction that directly and repeatedly measures the proportion of its universities and colleges experiencing cyber incidents, using a government survey with a published methodology. It supplies the measured number that India lacks.

10.1 The measured institutional incidence rate

The Cyber Security Breaches Survey is an official statistic produced by the UK Department for Science, Innovation and Technology (DSIT), with fieldwork conducted by Ipsos. It includes a dedicated education annex covering primary schools, secondary schools, further education colleges and higher education institutions.

Table 10.1 — Proportion identifying a cyber breach or attack in the previous 12 months, UK [S9][S10][S11]

Survey edition	Higher education	FE colleges	Secondary schools	Primary schools	Businesses
2023	85%	—	—	—	32%
2024	97%	—	—	—	50%
2025	91%	85%	60%	44%	43%
2025/2026	98%	88%	73%	49%	43%

The 2025/2026 edition, with fieldwork conducted between August and December 2025, found that **98 percent of higher education institutions had identified breaches or attacks in the last 12 months** — higher than any other sector surveyed and more than double the 43 percent recorded for businesses as a whole [S9]. The 2025 edition, drawing on a sample of 32 universities and 52 colleges, found 91 percent for universities [S10]; the 2024 edition found 97 percent, and 2023 found 85 percent [S11].

10.2 Frequency, not just incidence

Incidence understates the picture. The 2025/2026 survey found that **29 percent of higher education institutions encountered breaches or attacks at least weekly, and 12 percent faced them daily** [S9]. The 2024/2025 edition recorded 34 percent of higher education institutions and 27 percent of further education institutions reporting weekly breaches [S9].

This is the finding that most changes the framing for an institutional buyer. The question is not whether an incident will occur in a given year — at 98 percent incidence that question is settled — but whether the institution has the capacity to absorb a weekly or daily event rate. An institution with no monitoring is not experiencing zero incidents at that base rate; it is experiencing an unknown number.

10.3 Attack composition

The 2024 education annex found that, among institutions that had experienced any incident, **100 percent of higher education institutions and 97 percent of further education colleges reported phishing**, with impersonation reported by 90 percent of HEIs and 78 percent of FE colleges [S12]. Earlier editions found higher education institutions more severely affected than schools, with six in ten of those identifying any breach reporting lost money or data, or compromised accounts used for illicit purposes [S11].

Phishing at 100 percent and impersonation at 90 percent [S12] should be read directly against the Indian evidence, where brute-force campaigns cycling trivial passwords were the dominant observed vector [S8] and Seqrite identifies impersonation-led scams as the growing threat [S5]. The UK and Indian pictures are converging on the same two attack surfaces: identity and brand.

10.4 Jisc: the shared-infrastructure model India lacks

Jisc operates the Janet Network as the UK's National Research and Education Network, together with a security operations centre and a computer security incident response team serving higher education providers, further education colleges and research establishments [S13]. Its annual threat intelligence reporting recorded **seven major incidents across HE, FE and research in 2025, down from 17 in 2024, while total incidents rose from over 11,000 to over 16,000**. Distributed denial of service attacks fell from 976 to 418 [S13].

> **The most important comparative fact in this report.** UK total incidents rose from 11,000 to 16,000 while major incidents fell from 17 to 7 [S13]. That divergence is what a functioning shared defensive capability produces: more events detected, fewer events escalating. India has no equivalent shared security operations centre for its 64,456 higher education institutions [S22]. Indian institutions are not defended more efficiently than UK institutions; they are undefended and unmeasured, which produces a lower apparent incident count and a higher real one.

Board-level engagement in the UK sector is also markedly higher than in Indian practice: 81 percent of surveyed higher education institutions had a governor or senior manager with explicit responsibility for cybersecurity, though this was down nine percentage points on the previous year [S10].

11. Comparative Analysis II: The United States

The US comparator contributes something different: a long-run disclosed-breach dataset, made possible by mandatory reporting, and the clearest available evidence on third-party platform concentration risk.

11.1 The long-run disclosure record

Over the twenty years to 2025, American educational institutions experienced **3,173 data breaches compromising more than 37.6 million records** [S17]. The worst year was 2023, with 954 breaches, driven overwhelmingly by the MOVEit file-transfer supply-chain compromise, which alone accounted for 802 breaches — 84 percent of the year's total — and affected more than 800 institutions using the software [S17]. The University of Georgia breach arising from MOVEit exposed names, dates of birth and Social Security numbers affecting 800,000 students, former students, faculty and staff [S17].

This dataset exists because since 2018 the US Department of Education has required Title IV institutions — which is to say the overwhelming majority of American colleges and universities, since Title IV covers federal student aid participation — to report any breach regardless of the number of records lost [S17]. India has no comparable obligation for educational institutions, which is the direct reason no comparable Indian dataset exists.

11.2 2025: flat incident counts, rising exposure

Table 11.1 — Global education ransomware, 2024 vs 2025, Comparitech [S15]

Measure	2024	2025	Change
Ransomware attacks claimed globally	247	251	+1.6%
Of which confirmed by target	—	94	—
Records breached (confirmed attacks)	3.11 million	3.96 million	+27%
US share of attacks	—	130	Highest of any country
US K-12 records breached	1.1 million	175,000	−84%
US higher education records breached	1.9 million	3.7 million	+95%
K-12 share of incidents	72%	74%	—

The mechanism behind the divergence is explicit: incident counts were flat while records exposed rose 27 percent because a small number of very large third-party compromises dominated. The principal vector was a zero-day vulnerability in Oracle E-Business Suite (CVE-2025-61882), exploited by the CL0P group from August 2025, producing confirmed breaches at five institutions [S15][S16].

Table 11.2 — Selected US higher education breaches, 2025 [S16]

Institution	Scale	Vector
University of Phoenix	approx. 3.5 million individuals	Oracle EBS zero-day (Clop)
Harvard University	1.3 TB data	Oracle EBS zero-day (Clop)
University of Pennsylvania	approx. 1.2 million records / 46,000 students and alumni	Email and marketing platform compromise
Columbia University	approx. 870,000 individuals	Phone-based phishing
Dartmouth College	approx. 100,000 individuals	Oracle EBS zero-day (Clop)

The Oracle E-Business Suite cases matter to Indian institutions for a reason that has nothing to do with Oracle. EBS was the financial backbone at these universities, handling tuition processing, payroll, vendor payments and student aid disbursement [S16]. The lesson is about concentration: **the single**

system that touches every financial transaction is the system whose compromise is total. For most Indian institutions that system is a student information and fee management platform, frequently supplied by a small regional vendor, frequently PHP-based, and frequently not subject to any security assessment as a condition of procurement.

11.3 The PowerSchool case: platform concentration as systemic risk

In December 2024, PowerSchool — a student information system provider estimated to hold records for around 75 percent of the North American K-12 market — was breached when an attacker used compromised credentials belonging to a technical support subcontractor to access a customer-support portal that lacked multi-factor authentication. The exposure reached approximately 62 million students and 9.5 million educators across roughly 18,000 schools [S36].

One absent MFA control on one subcontractor account produced the exposure of 62 million student records [S36]. This is the clearest available demonstration that in the education sector, institutional risk is largely *vendor* risk, and that vendor security posture is not something an institution can responsibly assume. Indian institutions running shared examination and student information platforms — one of which was already shown in 2023 to be compromisable across 1,000+ Indian institutions through a single authentication weakness [S33] — carry precisely this exposure with substantially less contractual leverage over their vendors.

11.4 US cost benchmarks and K-12 detection data

EDUCAUSE has documented that breaches cost higher education institutions in excess of USD 3 million per incident [S35]. The 2025 CIS MS-ISAC K-12 Cybersecurity Report, analysing more than 5,000 K-12 organisations between July 2023 and December 2024, found that **82 percent of reporting schools experienced cyber threat impacts**, recorded 14,000 security events and 9,300 confirmed cybersecurity incidents, and found that cybercriminals targeted human behaviour at least 45 percent more often than technical vulnerabilities [S21].

The 82 percent figure [S21] is a second independent instrument, in a second jurisdiction, arriving at an institutional incidence rate in the same band as the UK survey. Two differently designed studies in two countries converge on 82 to 98 percent. This is the principal external support for the L2 estimate of 85 to 95 percent for India in Table 1.1.

12. Comparative Analysis III: The European Union

The EU comparator is included for completeness and to establish a specific negative finding, which is itself useful.

12.1 What ENISA measures

The European Union Agency for Cybersecurity analysed 4,875 incidents in its Threat Landscape 2025, covering 1 July 2024 to 30 June 2025, drawn mainly from open sources supplemented by anonymised member-state contributions [S18].

Table 12.1 — Recorded incidents by sector, EU, ENISA Threat Landscape 2025 [S18]

Sector	Share of recorded incidents
Public administration	38.2%
Transport	7.5%
Digital infrastructure and services	4.8%
Finance	4.5%
Manufacturing	2.9%
Education	Not reported as a top-five sector

Threat composition: distributed denial of service accounted for 77 percent of reported incidents, with hacktivism representing nearly 80 percent of all incidents, though only around 2 percent resulted in actual service disruption. Ransomware remained the most impactful threat by damage. Within cybercrime incidents specifically, ransomware accounted for 81.1 percent and data breaches 15.2 percent. Some 53.7 percent of all incidents concerned essential entities as defined under the NIS2 Directive [S18].

12.2 The negative finding, and why it is instructive

Education does not appear among ENISA's top-five targeted EU sectors [S18]. This must not be read as evidence that European education is safe. Three explanations are more probable than a genuine sectoral difference:

1. ENISA's dataset is drawn mainly from open sources, and it explicitly notes that vague sectoral or geographic reporting affects the dataset [S18]. Education breaches in the EU are frequently handled under national GDPR notification without generating open-source reporting attributable to a sector.
2. The dataset is dominated by DDoS and hacktivism, at 77 to 80 percent [S18], which are directed disproportionately at public administration web properties. Education-sector attacks skew toward credential compromise and ransomware, which generate fewer discrete recorded incidents per campaign.
3. European universities are frequently classified within public administration or research categories rather than as a distinct education sector.

The methodological lesson transfers directly to India. ENISA's sectoral shares reflect **what gets reported through open channels**, not what occurs. A sector can be heavily attacked and statistically invisible. This is exactly the condition of Indian higher education, with the aggravating difference that India lacks even the GDPR-equivalent notification machinery that makes European education breaches visible to national regulators — until the DPDP Rules bring it into force in 2026-27 [S27].

13. Global Ransomware Economics in Education

Sophos publishes the only annual vendor-agnostic survey of education institutions that have actually been hit by ransomware. The 2025 edition, its fifth, surveyed 441 IT and cybersecurity leaders across 17 countries — 243 in lower education and 198 in higher education — all of whom had experienced a ransomware attack in the preceding year [S14]. Because the sample is drawn from victims, it measures consequence, not incidence.

Table 13.1 — Ransomware outcomes, global higher education, 2024 vs 2025, Sophos [S14]

Measure	2024	2025	Direction
Attacks resulting in data encryption	77%	58%	Improving (four-year low)
Attacks stopped before encryption	21%	38%	Improving
Median ransom demand	USD 3.55 million	USD 697,000	Falling
Median ransom paid	USD 4.41 million	USD 463,000	Falling
Mean recovery cost (excluding ransom)	USD 4.02 million	USD 0.90 million	Falling 77%
Fully recovered within one week	30%	59%	Improving
Data recovered in some form (of those encrypted)	—	97%	—
Extortion-only attacks (no encryption)	2%	3%	Rising

13.1 Root causes, and the one that matters for India

In higher education, **exploited vulnerabilities were the leading technical root cause, present in 35 percent of ransomware incidents** — a different profile from lower education, where phishing led at 22 percent [S14].

Set that 35 percent figure against the Bitsight finding that 45 percent of universities run at least one internet-facing asset on end-of-life PHP, roughly 10 percent expose Remote Desktop Protocol, and the education sector averages 151 days to remediate known exploited vulnerabilities [S20]. The leading cause of ransomware in higher education is unpatched internet-facing software, and higher education patches internet-facing software more slowly than any comparable sector. For the Indian estate, disproportionately PHP-based and disproportionately hosted on shared infrastructure without a managed patch pipeline, this is the highest-probability path to a catastrophic incident.

13.2 The human cost, and why it belongs in a business case

Sophos records that nearly 40 percent of respondents reported dealing with anxiety following an attack, and 34 percent of higher education IT leaders reported significant guilt at being unable to prevent it; increased pressure from senior leadership was the most commonly cited consequence for IT teams in both education tiers [S14].

This is not a soft finding. In an Indian private college with one or two IT staff, an incident of this kind reliably produces resignation of the person who holds all undocumented institutional knowledge about the systems. The second-order cost — loss of the only individual who understood the estate — routinely exceeds the direct recovery cost.

14. Comparative Synthesis

Table 14.1 — Cross-jurisdiction comparison, higher education cyber exposure

Dimension	India	United Kingdom	United States	European Union
Institutional base	64,456 HEIs; 1,289 universities; 48,246 colleges, approx. 70% private unaided [S22]	approx. 285 HE providers	approx. 4,000 degree-granting institutions	approx. 3,000+ HEIs across 27 states
Measured institutional incidence	**No measurement exists**	**98% (2025/26); 91% (2025); 97% (2024) [S9][S10][S11]**	Not surveyed; 3,173 breaches / 37.6M records over 20 years via mandatory reporting [S17]	Not reported as top-five sector [S18]
Per-institution attack rate	7,095 per week (Check Point) [S7]	29% weekly, 12% daily incidence [S9]	—	—
Sector share of national detections	approx. 24%, highest of any Indian sector (Seqrite) [S5]	—	—	Education not in top five [S18]
Shared national defensive capability	**None**	Jisc: Janet Network, national SOC, CSIRT [S13]	MS-ISAC, CISA, REN-ISAC	NIS2 framework; national CSIRTs
Mandatory breach disclosure	From Nov 2026 / May 2027 under DPDP Rules [S27]	UK GDPR, 72 hours	Title IV: any breach, any size, since 2018 [S17]	GDPR, 72 hours
Maximum regulatory penalty	Rs. 250 crore per violation, stacking [S27]	Higher of GBP 17.5m or 4% turnover	Varies by state and statute	Higher of EUR 20m or 4% turnover
Dominant attack vector	Brute force on weak credentials; impersonation and cloned portals [S5][S8]	Phishing 100%; impersonation 90% [S12]	Third-party platform compromise [S15][S36]	DDoS/hacktivism 77–80% [S18]
Distinctive national risk	Fake universities (32); Aadhaar-linked data; examination paper leakage at national scale [S23][S28]	Research IP and state-aligned targeting [S13]	Platform concentration; SSN exposure [S36]	NIS2 essential-entity classification [S18]
Institution-specific weakness	No monitoring; no shared SOC; PHP-heavy estate; unmeasured	Board engagement declining 9pp [S10]	Vendor concentration	Sectoral invisibility in reporting

14.1 The three conclusions the comparison supports

First: India's apparently lower incident numbers are a measurement artefact, not a security achievement. The UK measures and finds 98 percent [S9]. The US mandates disclosure and has accumulated 3,173 breaches [S17]. The EU relies on open-source aggregation and cannot see its education sector at all [S18]. India neither measures nor mandates, and correspondingly sees almost nothing — while simultaneously recording, through commercial telemetry, the highest sectoral attack share in the country [S5] and a per-institution attack rate of 7,095 per week [S7]. These are not in tension. They are the signature of a heavily attacked, unmonitored sector.

Second: the two jurisdictions that measure converge on 82 to 98 percent. The UK government survey finds 98 percent of HEIs [S9]; the US MS-ISAC K-12 analysis finds 82 percent of reporting schools [S21]. Independent instruments, different countries, different sectors within education, same band. An Indian institution asking whether the 85 to 95 percent estimate in this report is plausible should note that it sits inside a range established by two governments' own measurements, in jurisdictions with better defences than India's.

Third: the UK proves that the outcome is controllable. Jisc's data — total incidents up from 11,000 to over 16,000 while major incidents fell from 17 to 7 [S13] — is the single most actionable comparative finding in this report. Detection went up and severity went down, in the same sector, in the same year. That is not a consequence of the UK facing a gentler adversary. It is a consequence of shared monitoring capability, which India's 64,456 institutions do not have.

15. The Regulatory and Liability Position in India

Until November 2025 an Indian institution suffering a student data breach faced reputational consequence and, in principle, liability under Section 43A of the Information Technology Act, 2000 — a provision rarely enforced against educational institutions. That position has changed, on a published timetable, with quantified penalties.

15.1 The Digital Personal Data Protection framework

The Digital Personal Data Protection Act, 2023 received Presidential assent in August 2023. The Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025, converting the framework from principle into operative obligation. The Data Protection Board of India became operational on 13 November 2025 and is vested, for the purpose of inquiries, with the powers of a civil court including the ability to summon attendance, examine witnesses and inspect data and documents [S27].

Table 15.1 — DPDP commencement timetable [S27]

Date	What activates
13 November 2025	Rules notified. Data Protection Board of India operational. Core definitions in force.
13 November 2026	**Enforcement powers and the penalty framework commence.** Consent Manager registration begins.
13 May 2027	**Full compliance required.** Consent, notice, security safeguards and data-principal rights obligations in force (Sections 3–17; Rules 3, 5–16, 22, 23).

Table 15.2 — DPDP penalty schedule [S27]

Contravention	Maximum penalty
Failure of a Data Fiduciary to maintain reasonable security safeguards	**Rs. 250 crore**
Failure to notify the Board or affected Data Principals of a personal data breach	**Rs. 200 crore**
Contravention of obligations relating to children's data	**Rs. 200 crore**
Failure to observe Significant Data Fiduciary obligations	Rs. 150 crore
General non-compliance	Rs. 50 crore

Three features of this schedule are decisive for educational institutions.

Penalties are per violation and can stack. A single incident can trigger multiple categories simultaneously [S27]. A student data exposure caused by inadequate safeguards, not detected, and therefore not notified, engages both the Rs. 250 crore and the Rs. 200 crore heads. If any affected student is a minor — which is routine in an institution admitting students at 17 — the children's data head may also engage.

There is no revenue or size threshold for the core obligations. Every organisation processing digital personal data of individuals in India is a Data Fiduciary, regardless of size or sector; only the Significant Data Fiduciary tier adds further requirements [S27]. A private affiliated college with 800 students and no IT department carries the same core obligations as a national university.

The notification window is short and the clock starts at awareness. Affected Data Principals must be notified within 72 hours, with the notice required to state in plain language the nature of the breach, what data was exposed, protective measures the individual can take, and contact details for queries [S27].

The structural problem this creates for Indian institutions. Table 7.1 established that of ten documented Indian incidents, one was found by the institution's own monitoring. The IIT Roorkee data may have been publicly reachable for over a decade before external disclosure [S24]. A 72-hour notification obligation is unmeetable by an institution with no detection capability — not because it is unwilling to comply, but because the obligation is triggered by knowledge it does not have and has no mechanism to acquire. **From 13 November 2026, absence of monitoring converts directly into penalty exposure.**

15.2 Retention and erasure: an unusually difficult obligation for this sector

The Rules require erasure of personal data once the purpose for which it was collected is no longer served, with a 48-hour pre-erasure notification protocol, and require that consent records, processing logs and activity logs be retained for at least one year [S27]. Significant Data Fiduciaries face additional duties including appointment of a Data Protection Officer based in India and reporting to the board, annual audits, data protection impact assessments, and algorithmic due diligence for automated decision-making [S27].

Indian educational institutions are structurally poorly placed to meet the erasure obligation, for a reason specific to their operating model: they retain student records indefinitely by design, because degree verification requests arrive decades after graduation. Reconciling an indefinite verification requirement with a purpose-limitation erasure obligation requires a deliberate data architecture decision — typically separating a minimal, permanently retained verification register from the full admission file, which is then erased on schedule. Almost no Indian institution has made this separation. The IIT Roorkee exposure is a direct illustration: a full academic-affairs record set, including caste category and financial background, retained and reachable long after any processing purpose was being served [S24].

15.3 CERT-In directions

CERT-In's directions under Section 70B(6) of the Information Technology Act, 2000, issued in April 2022, require reporting of specified cyber incidents to CERT-In within six hours of noticing or being notified, mandate synchronisation of system clocks to NIC or NPL servers, and require retention of ICT system logs for a rolling period of 180 days within Indian jurisdiction. These obligations apply to body corporates and government organisations, including educational institutions, and predate the DPDP framework. They are, in the experience reflected across the Indian institutional record, very widely unmet in the higher education sector.

The practical implication is that an institution facing a DPDP inquiry after 13 November 2026 will be asked for logs. An institution that has not retained 180 days of ICT system logs cannot demonstrate what happened, cannot bound the scope of a breach, and cannot evidence that it maintained reasonable security safeguards. **Log retention is not a compliance formality; it is the only mechanism by which an institution can later prove the breach was small.**

16. Why Indian Institutions Are Structurally Vulnerable

The vulnerability is not primarily a technology gap. It is a set of eight structural conditions, each of which is addressable, and none of which is addressed by purchasing a product alone.

1. **No security function exists to own the problem.** Responsibility typically sits with an IT administrator whose primary duties are uptime and user support. Security is an unfunded addition to that role. The UK comparator has 81 percent of institutions with a governor or senior manager explicitly accountable for cybersecurity [S10]; the Indian equivalent figure is not measured and, on the available evidence, would be a small fraction of that.
2. **No detection capability, therefore no incident history, therefore no budget.** This is a self-sealing loop. An institution with no monitoring records no incidents; with no recorded incidents, no business case for monitoring can be built; the absence of a business case is then cited as evidence that the risk is low. The Jisc data breaks this loop empirically: instrumenting the sector raised recorded incidents from 11,000 to over 16,000 [S13]. Those incidents existed before they were counted.
3. **The web and application estate is old, PHP-heavy, and unpatched.** 45 percent of universities globally run at least one internet-facing asset on end-of-life PHP [S20]; the Indian proportion is very likely higher given the prevalence of shared cPanel hosting in the sector. Education averages 151 days to remediate known exploited vulnerabilities [S20], against adversaries weaponising disclosures within days. Exploited vulnerabilities are the leading ransomware root cause in higher education at 35 percent [S14].
4. **Credential hygiene is the primary observed weakness, and it is cultural.** The Indian institutional study found brute-force campaigns succeeding against "root" and "admin" accounts using passwords including "123456" and "password" [S8]. Shared administrative accounts, credentials passed between staff on WhatsApp, and absence of multi-factor authentication are normal rather than exceptional. 39 percent of Microsoft-observed identity-based attacks targeted academic and research institutions [S19].
5. **Third-party platforms are procured on price and features, never on security posture.** Student information systems, examination platforms, fee gateways and library systems are typically selected without any security assessment, penetration test evidence, or contractual security obligation. The 2023 disclosure affecting 1,000+ Indian institutions through one examination platform [S33] and the PowerSchool breach reaching 62 million records through one subcontractor account without MFA [S36] are the same failure at different scales.
6. **The institution's brand is unmonitored and undefended.** Cloned websites, fraudulent fee portals, fake scholarship offers and fake placement postings operate under the institution's name without the institution's knowledge [S5][S25]. Almost no Indian institution monitors for impersonation of itself. Because the compromised asset is the institution's reputation rather than its servers, the IT function does not regard it as in scope, and no other function has the capability to act.
7. **Reporting incentives run the wrong way.** With 22 percent of cybercrimes charged and under 3 percent convicted [S38], and with admissions competition acutely sensitive to reputational damage, the rational institutional response to a discovered breach has been silence. This has suppressed the sector's incident record, which in turn removed the evidence base for sector-wide investment. The DPDP notification obligation inverts this incentive from November 2026 [S27], but the decade of suppressed data cannot be recovered.
8. **Seasonal concentration creates predictable, unmanaged peak risk.** Admission, fee and examination cycles concentrate the highest-value transactions and the greatest volume of new, unfamiliar users into a small number of published windows. Attack campaigns are timed accordingly. Institutions do not typically increase monitoring or controls during these windows, because they have

no monitoring to increase.

17. Control Framework and Maturity Assessment

This section converts the preceding analysis into an assessable control set. It is organised so that an institution can locate itself, and is deliberately ordered by ratio of risk reduction to cost rather than by technical sophistication.

17.1 Maturity model

Table 17.1 — Institutional cyber maturity, five levels

Level	Description	Observable characteristics	Estimated share of Indian HEIs
0 — Blind	No security function, no monitoring, no logs, no incident history.	Cannot answer "were we breached last year?". No log retention. Shared admin credentials. No MFA.	Majority
1 — Reactive	Incidents handled when they become visible through operational failure.	Antivirus deployed. Backups exist but are untested. Response is ad hoc and undocumented.	Substantial minority
2 — Baseline	Core hygiene controls implemented and verifiable.	MFA on all administrative accounts. Patch pipeline for internet-facing assets. 180-day log retention. Tested backups. Named accountable owner.	Small minority
3 — Monitored	Detection capability exists; incidents are found rather than suffered.	Log aggregation and alerting. Brand and impersonation monitoring. Vendor security assessment at procurement. Documented and exercised incident response plan.	Very few
4 — Assured	Controls are independently verified and the institution can evidence its posture to a regulator.	External penetration testing. DPDP-mapped data inventory and retention schedule. Cryptographic custody for examination material. Board-level reporting. Demonstrable 72-hour notification capability.	Negligible

The share estimates in the right-hand column are this report's judgement and are not measured. They are inferred from the documented discovery routes in Table 7.1, the credential findings in the Indian institutional study [S8], and the absence of any shared defensive infrastructure [S13][S22]. They should be read as an ordering, not as statistics.

17.2 Control priorities, ordered by risk reduction per rupee

Table 17.2 — Prioritised control set

Priority	Control	Addresses	Evidentiary basis
1	Multi-factor authentication on every administrative and privileged account, without exception for convenience or seniority.	Patterns 4, 5, 7 (Table 6.1)	Brute force on admin accounts is the dominant observed Indian vector [S8]; 62M records exposed via one non-MFA account [S36]
2	Elimination of shared administrative credentials; individual named accounts with revocation on separation.	Patterns 3, 4, 6	Thane case: retained access used fraudulently post-separation [S25]
3	Inventory of internet-facing assets and a patch pipeline with a defined remediation SLA for known exploited vulnerabilities.	Patterns 3, 10	Exploited vulnerabilities lead ransomware root cause at 35% [S14]; 151-day sector remediation average [S20]; 45% run EOL PHP [S20]
4	ICT system log retention for 180 days minimum, within Indian jurisdiction, with clock synchronisation.	DPDP evidentiary position; all patterns	CERT-In directions; DPDP requires one-year retention of processing and activity logs [S27]

Priority	Control	Addresses	Evidentiary basis
5	Removal of publicly reachable data stores; authenticated access to all student record interfaces.	Pattern 3	IIT Roorkee: 30,000+ records reachable on a public-facing site, possibly for a decade [S24]
6	Brand and impersonation monitoring: detection of cloned sites, fraudulent fee portals, fake scholarship and placement offers.	Patterns 1, 2, 8, 9	Cloned fee-collecting site documented Dec 2025 [S25]; impersonation-led scams identified as growing vector [S5]
7	Security assessment as a mandatory condition of procurement for any platform holding student data or examination material.	Patterns 3, 7, 10	1,000+ Indian institutions compromisable via one platform weakness [S33]; Oracle EBS cases [S15][S16]
8	DPDP data inventory: what personal data is held, for what purpose, for how long, with a retention and erasure schedule separating the permanent verification register from the erasable admission file.	Regulatory exposure	Rs. 250 crore safeguards head; purpose-limitation erasure obligation [S27]
9	Cryptographic custody for examination material: threshold key splitting so that no single custodian or compromised account can reconstruct a paper, with an append-only verifiable access ledger.	Patterns 6, 7	Paper leakage named as breach consequence [S8]; statutory criminal exposure with Rs. 1 crore minimum fine for organised offences [S28]
10	Tested incident response plan with a defined 72-hour notification pathway, exercised at least annually.	Regulatory exposure; all patterns	Rs. 200 crore notification-failure head [S27]; 88–90% of UK HEIs have defined response actions [S9]

Controls 1 through 5 are largely configuration and discipline rather than procurement, and together address the majority of the attack volume evidenced in the Indian record. An institution that implements only these moves from Level 0 to Level 2 in Table 17.1 at close to zero licence cost. Controls 6 through 10 require capability the sector does not currently possess internally.

17.3 Cost of inaction

Table 17.3 — Quantified exposure per incident, Indian higher education institution

Exposure head	Basis	Magnitude
DPDP — inadequate security safeguards	Statutory maximum, per violation [S27]	Up to Rs. 250 crore
DPDP — failure to notify	Statutory maximum, per violation, stackable [S27]	Up to Rs. 200 crore
Direct recovery cost	Sophos global higher education mean, 2025 [S14]	approx. USD 0.90 million (approx. Rs. 7.5 crore)
Total incident cost benchmark	EDUCAUSE, higher education [S35]	In excess of USD 3 million
Ransom, if paid	Sophos global higher education median paid, 2025 [S14]	approx. USD 463,000
Examination fraud — organised offence	Public Examinations Act, 2024 [S28]	Minimum Rs. 1 crore; 5–10 years custodial
Admission cycle disruption	Judgement, not measured	A cancelled or compromised admission cycle can forgo an entire year's intake revenue
Examination cancellation	UGC-NET June 2024 precedent [S28]	1.1 million candidates across 317 cities

The comparison an institution should make is not between the cost of controls and zero. It is between the cost of controls and the cost of the first incident that the institution does not detect, does not notify, and cannot evidence a defence against. On the penalty schedule now in force, that comparison is not close.

18. Limitations of This Report

This section exists because the report's conclusions are only as strong as its acknowledged weaknesses, and because an institutional reader is entitled to know where to push. Every limitation below is material.

18.1 Limitations of the central estimate

- **The L2 estimate of 85 to 95 percent is an inference, not a measurement.** It rests on transferring a UK survey-measured rate [S9] to India on the argument that Indian attack volume is higher [S5][S7] and Indian security maturity lower [S8]. That argument is reasonable but it is an argument, not data. A properly designed Indian survey could return a materially different figure.
- **The definitional boundary does most of the work.** Including fraud committed against students in the institution's name raises the estimate substantially (L2 at 85–95%) versus counting only compromise of institution-operated systems (L3 at 60–75%). Any figure quoted from this report without its definition is misleading.
- **The detection and disclosure estimates (L4, L5) are the weakest in the report.** They are inferred principally from the discovery-route distribution across ten documented incidents in Table 7.1 — a very small and non-random sample. They should be treated as directional.
- **The maturity distribution in Table 17.1 is judgement.** It is not measured and is not presented as measured.

18.2 Limitations of the underlying sources

- **Vendor telemetry carries a structural incentive toward alarm.** Seqrite, Check Point, Sophos, Comparitech, CYFIRMA, Cyble and Bitsight all sell security products or services. Their data is the best available on education-sector specifics and is used extensively here, but a vendor reporting that its sector-of-interest is the most attacked has a commercial interest in that finding. This report attributes every such figure to the vendor by name for exactly this reason.
- **Detection counts are shaped by installed base, not by threat.** Seqrite's finding that education accounts for 24 percent of detections [S5] is partly a function of where Seqrite products are deployed. If Seqrite has disproportionate penetration in Indian education, the share is inflated. The sample size (8 million endpoints, 265.52 million detections) is large, but the sampling frame is not random.
- **The UK survey samples are small.** The 2025 edition drew on 32 universities and 52 further education colleges [S10]; the 2025/2026 edition on approximately 49 HEIs [S9]. Against a UK base of roughly 285 providers this is a substantial fraction, but the confidence interval around 98 percent is wider than the headline suggests, and part of the sample is recruited through an open link disseminated by Jisc and UCISA [S9], which self-selects toward institutions with engaged IT functions.
- **The CyberPeace study is a pilot with an unpublished sampling frame.** Its "five times more vulnerable" conclusion [S8] is the single most quotable Indian finding in this report and also one of the least methodologically transparent. The participating institution count is not published in available coverage. It should be cited as a pilot finding, never as a national statistic.
- **Sophos surveys victims only.** All 441 respondents had already been hit by ransomware [S14]. Its figures measure consequence and recovery, and cannot be used to infer how likely an attack is.
- **Comparitech counts claimed and confirmed attacks.** Of 251 claimed global education ransomware attacks in 2025, only 94 were confirmed by the targeted organisation [S15]. Record-count figures derive from confirmed attacks and will rise as further disclosures are filed, as Comparitech itself notes.

- **NCRB counts registered cases only** [S1], and the 2024 edition reflects recategorisation under the Bharatiya Nyaya Sanhita, limiting comparability with earlier years [S1].
- **ENISA is open-source dependent and explicitly acknowledges that vague sectoral reporting affects its dataset** [S18]. Its sectoral shares should not be read as incidence.
- **AISHE is self-reported.** Institutions voluntarily upload data which the Ministry then validates; the 2023-24 participation rate was approximately 92 percent [S22].
- **Several secondary sources are trade or aggregator publications** rather than the primary reports they describe. Where this is the case Appendix A identifies the intermediary. Readers requiring primary verification should obtain the underlying vendor and government reports directly; Appendix A gives the publisher and title for each.

18.3 What would materially improve this evidence base

A single intervention would resolve most of the uncertainty in this report: **an annual, statistically designed survey of Indian higher education institutions on the model of the UK Cyber Security Breaches Survey education annex**, conducted by or on behalf of the Ministry of Education or UGC, with a published sampling frame and methodology. The UK has run this instrument for a decade and can consequently state its sector's incidence rate to within a few percentage points [S9][S10][S11]. India cannot state its own to within thirty. Until such an instrument exists, every Indian figure in this domain — including this report's — will be an inference from commercial telemetry and foreign comparators.

Appendix A — Source Register

Every bracketed reference in this report resolves to an entry below. Each entry gives the publisher, the publication, the period covered, and where available the sample size and methodological caveats. Where this report relied on a trade or aggregator publication rather than the primary document, the intermediary is named so that a reader can obtain the primary source directly. Section 18 discusses the limitations of these sources.

S1 **National Crime Records Bureau (NCRB), Ministry of Home Affairs, Government of India.** *Crime in India 2024*. Cybercrime cases 1,01,928 (+17.9% on 2023); rate 7.3 per lakh; cyber fraud 73,987 cases (72.6% of total); Telangana 27,230; Karnataka 21,003; approx. 35,000 cases in metro cities. First edition compiled substantially under the Bharatiya Nyaya Sanhita, limiting comparability with prior years.

S2 **NCRB, Ministry of Home Affairs.** *Crime in India 2023*. Cybercrime cases 86,420 (+31.2% on 65,893 in 2022); rate 6.2 per lakh. Cheating by personation under the IT Act nearly doubled from 13,506 (2022) to 25,334 (2023).

S3 **Indian Cyber Crime Coordination Centre (I4C) / National Cyber Crime Reporting Portal, via The420.in.** Reported cyber fraud losses: 2022 Rs. 2,290.23 cr; 2023 Rs. 7,463.20 cr; 2024 Rs. 22,849.49 cr (19,18,852 complaints); 2025 Rs. 19,812.96 cr (21,77,524 complaints). Cumulative 2020–2025 Rs. 52,976 cr. State losses 2025: Maharashtra Rs. 3,203 cr; Karnataka Rs. 2,413 cr; Tamil Nadu Rs. 1,897 cr; UP Rs. 1,443 cr; Telangana Rs. 1,372 cr.

S4 **Ministry of Home Affairs, Government of India.** Lok Sabha Unstarred Question No. 432, answered 02.12.2025; and related parliamentary replies. NCRP complaint growth approx. 4.5 lakh (2021) to over 22 lakh (2024); 15.96 lakh in 2023 (+55.15%); 22.68 lakh in 2024 (+42.08%).

S5 **Seqrite Labs (Quick Heal Technologies Ltd).** *India Cyber Threat Report 2026*. Period October 2024 – September 2025; 8 million+ endpoints monitored; 265.52 million total detections (approx. 505 per minute). Education sector: approx. 24% of all detections, 4.92 million detections — highest of any Indian industry. Identifies fake institution websites, fraudulent scholarship offers and fake job postings as growing impersonation vectors.

S6 **Check Point Software Technologies.** *State of Cyber Security in India 2025*. Indian organisations averaged 2,011 attacks per week in 2025. Education identified as most targeted sector worldwide at 4,248–9,817 attacks per organisation per week.

S7 **Check Point Research, Threat Intelligence Report, via BW Education.** Indian education sector: average 7,095 cyberattacks per organisation per week — above government bodies and consumer goods companies.

S8 **CyberPeace Foundation, with DELNET, Resecurity and Autobot Infosec.** *Exploring Cyber Threats and Digital Risks to Indian Educational Institutions*, e-Kawach initiative pilot study. Period July 2023 – April 2024; released August 2025. 200,000+ cyberattacks; nearly 400,000 data breaches; 8,000+ unique usernames and 54,000+ unique passwords observed in brute-force attempts; "root" and "admin" most targeted; "123456" and "password" among most attempted. Concludes Indian institutions likely five times more vulnerable than counterparts with stronger practices. **Pilot study; participating institution count and sampling frame not published in available coverage.**

S9 **Department for Science, Innovation and Technology (DSIT), UK Government.** *Cyber Security Breaches Survey 2025/2026: education institutions findings*. Fieldwork August–December 2025. 98% of higher education institutions, 88% of FE colleges, 73% of secondary schools, 49% of primary schools identified a breach or attack in the last 12 months; 43% of businesses. 29% of HEIs weekly, 12% daily. 2024/2025 comparison: 34% HE and 27% FE weekly. HEI sample approx. 49.

S10 **DSIT, UK Government.** *Cyber Security Breaches Survey 2025*, education annex. Fieldwork August–December 2024. 91% of universities, 85% of FE colleges, 60% of secondary schools, 44% of primary schools; 43% of businesses (2,179 surveyed). Education sample: 250 primary, 240 secondary, 52 colleges, 32 universities. 81% of HEIs had a governor or senior manager responsible for cybersecurity, down 9 percentage points year on year.

S11 **DSIT, UK Government.** *Cyber Security Breaches Survey* 2024 edition (97% of HEIs) and 2023 edition (85% of HEIs). 2023 annex: six in ten HEIs identifying any breach reported losing money or data, or compromised accounts used for illicit purposes.

S12 **DSIT, UK Government.** *Cyber Security Breaches Survey 2024: education institutions annex*. Among institutions experiencing any incident: phishing reported by 100% of HEIs and 97% of FE colleges; impersonation by 90% of HEIs and 78% of FE colleges.

S13 **Jisc.** Annual cyber threat intelligence report, UK further and higher education and research. 2025: seven major incidents across HE, FE and research, down from 17 in 2024; total incidents rose from over 11,000 to over 16,000; DDoS attacks fell from 976 to 418. Jisc operates the Janet Network (UK NREN), a sector security operations centre and a CSIRT.

S14 **Sophos.** *The State of Ransomware in Education 2025* (fifth annual edition, September 2025). Vendor-agnostic survey of 441 IT and cybersecurity leaders across 17 countries — 243 lower education, 198 higher education — all of whose organisations were hit by ransomware in the preceding year. Higher education: encryption rate 58% (from 77%); attacks stopped pre-encryption 38% (from 21%); exploited vulnerabilities leading root cause at 35%; median demand USD 697,000 (from 3.55m); median payment USD 463,000 (from 4.41m); mean recovery cost USD 0.90m (from 4.02m, −77%); 59% fully recovered within a week (from 30%); 97% of encrypted victims recovered data; extortion-only 3% (from 2%); approx. 40% reported anxiety, 34% guilt. Lower education: phishing leading root cause at 22%; encryption 29%; stopped pre-encryption 67% (from 14%); recovery cost USD 2.28m (from 3.76m).

S15 **Comparitech.** Education ransomware roundup, 2025. 251 attacks claimed globally on educational institutions (247 in 2024); 94 confirmed by targets; 3.96 million records exposed across confirmed attacks (+27% on 3.11m). US: 130 attacks — highest of any country — with 175,000 K-12 and 3.7 million higher education records. K-12 74% of incidents (72% in 2024). Principal 2025 vector: Oracle E-Business Suite zero-day CVE-2025-61882 exploited by CL0P from August 2025, five confirmed institutional breaches. Comparitech notes totals likely to rise with further disclosures.

S16 **archTIS; Breached.company.** Compilation of 2025 higher education breaches. University of Phoenix approx. 3.5 million individuals (Oracle EBS / Clop); Harvard University 1.3 TB (Oracle EBS / Clop); University of Pennsylvania approx. 1.2 million records, approx. 46,000 students and alumni; Columbia University approx. 870,000 individuals (phone phishing); Dartmouth College approx. 100,000 individuals. Oracle EBS versions 12.2.3–12.2.14, BI Publisher Integration component; EBS served as financial backbone for tuition, payroll, vendor payments and student aid.

S17 **Forbes (S. Weisman), drawing on Comparitech data.** US educational institutions: 3,173 data breaches over 20 years, 37.6 million records compromised. Worst year 2023: 954 breaches, of which 802 (84%) attributable to MOVEit, affecting 800+ institutions; University of Georgia exposure affected 800,000 individuals including Social Security numbers. Since 2018 the US Department of Education requires Title IV institutions to report any breach regardless of size.

S18 **European Union Agency for Cybersecurity (ENISA).** *ENISA Threat Landscape 2025*, published 1 October 2025. 4,875 incidents analysed, 1 July 2024 – 30 June 2025, mainly open-source plus anonymised member-state contributions. Public administration 38.2% of recorded incidents; transport 7.5%; digital infrastructure and services 4.8%; finance 4.5%; manufacturing 2.9%. Education not among top five. DDoS 77% of reported incidents; hacktivism approx. 80%, of which only approx. 2% caused actual service disruption. Within cybercrime incidents: ransomware 81.1%, data breaches 15.2%. 53.7% of incidents concerned NIS2 essential entities. ENISA explicitly notes that vague sectoral or geographic reporting affects the dataset.

S19 **Microsoft.** *Digital Defense Report 2025*. 39% of identity-based attacks observed by Microsoft targeted research and academic institutions.

S20 **Bitsight.** Education sector research. 45% of universities have at least one asset running end-of-life PHP; approx. 10% have open RDP ports; education sector averages 151 days to remediate known exploited vulnerabilities.

S21 **Center for Internet Security / MS-ISAC.** *2025 K-12 Cybersecurity Report*. Analysis of 5,000+ K-12 organisations, July 2023 – December 2024. 82% of reporting schools experienced cyber threat impacts; 14,000 security events; 9,300 confirmed cybersecurity incidents; cybercriminals targeted human behaviour at least 45% more than technical vulnerabilities.

S22 **Ministry of Education, Government of India.** *All India Survey on Higher Education (AISHE) 2023-24*. 64,456 registered HEIs: 1,289 universities/university-level institutions, 48,246 colleges, 15,221 standalone institutions; 4,376 added in one year. Enrolment 4.50 crore; GER 30.0 (29.5 in 2022-23; 23.7 in 2014-15); female GER 31.2. Faculty 17.32 lakh, 44.9% women. Approx. 70% of colleges private unaided. 58,134 foreign students from 173 countries. Participation 59,553 of 64,756 registered institutions (approx. 92%). Data is self-reported by institutions and validated by the Ministry.

S23 **University Grants Commission (UGC), Government of India.** Public notices and list of fake universities. 22 institutions listed October 2025; 32 institutions across 12–13 states as of February 2026. Distribution February 2026: Delhi and New Delhi 12, Uttar Pradesh 4, Andhra Pradesh 2, Karnataka 2, Kerala 2, Maharashtra 2, Puducherry 2, West Bengal 2, Arunachal Pradesh 1, Haryana 1, Jharkhand 1, Rajasthan 1. Haryana, Rajasthan, Jharkhand and Arunachal Pradesh newly added. December 2025 notices concerned institutions in Karnataka, Delhi and Maharashtra, and separately Delhi and Kerala. Under the UGC Act, 1956 only institutions established by Central or State Act, or recognised under Sections 2(f) or 3, may award degrees.

S24 **VARINDIA and related Indian technology press.** IIT Roorkee data breach, reported August 2025. 30,000+ student and alumni records exposed: names, mobile numbers, caste categories, financial backgrounds, email addresses, graduation details. Originated in academic affairs department records left openly accessible on a public-facing website; retrievable using a student enrolment number. Evidence suggested the database may have been publicly accessible for over a decade. Internal cybersecurity investigation confirmed by the institute's deputy director.

S25 **CYFIRMA, via GBHackers and Cyber Security News.** Indian student data weaponised for phishing, social engineering and financial fraud. Cloned university website discovered December 2025 collecting student fees and personal data behind convincing academic content. December 2025: former academic counsellor in Thane booked for using retained student records to fraudulently collect over Rs. 48,000 while posing as active staff. Dark-web advertisement of structured datasets containing millions of student records from Indian education platforms, including PII, admission details, enrolment records, examination centre bookings, parental details and payment data.

S26 **Rajya Sabha reply; Deccan Herald.** AIIMS Delhi ransomware incident, November 2022. Five servers and approximately 1.3 TB of data affected; medical records and personal data of close to four crore patients feared compromised. Approximately 6,000 attempts against the ICMR website within 24 hours the following week. 13.9 lakh recorded attacks on Indian servers and databases in 2022.

S27 **Government of India.** Digital Personal Data Protection Act, 2023 (Presidential assent August 2023); Digital Personal Data Protection Rules, 2025 (notified 13 November 2025). Data Protection Board of India operational 13 November 2025, with civil-court powers for inquiries. Enforcement powers, penalty framework and Consent Manager registration from 13 November 2026. Full compliance 13 May 2027 (Sections 3–17; Rules 3, 5–16, 22, 23). Penalties: up to Rs. 250 crore for failure to maintain reasonable security safeguards; up to Rs. 200 crore for failure to notify the Board or affected Data Principals; up to Rs. 200 crore for children's data contraventions; up to Rs. 150 crore for SDF obligation failures; up to Rs. 50 crore for general non-compliance. Penalties assessed per violation and may stack. Data Principal notification within 72 hours, with prescribed content. 48-hour pre-erasure notification (Rule 8). Processing, consent and activity logs retained at least one year. No revenue or size threshold for core obligations. SDF duties include India-based DPO reporting to the board, annual audits, DPIAs and algorithmic due diligence (Rule 13(3)).

S28 **Government of India.** Public Examinations (Prevention of Unfair Means) Act, 2024 and Rules, 2024. Passed Lok Sabha 6 February 2024, Rajya Sabha 9 February 2024; Presidential assent February 2024; in force 21 June 2024; Rules dated 23 June 2024. Offences include leakage of question paper or answer key; tampering with a computer network, computer resource or computer system; creation of a fake website to cheat or for monetary gain; conduct of fake examinations and issuance of fake admit cards or offer letters; manipulation of seating, dates and shifts. Penalties: individuals 3–5 years and up to Rs. 10 lakh; organised groups or institutions 5–10 years and minimum Rs. 1 crore. UGC-NET June 2024 cancelled after being conducted across 317 cities with over 1.1 million candidates; NEET-PG 2024 postponed; CBI directed to investigate UGC-NET and NEET-UG allegations. Special fast-track court designated at Rouse Avenue Court, Delhi. Cabinet approved amendments July 2026 proposing up to 10 years and up to Rs. 10 crore.

S29 **Government of Uttar Pradesh.** Uttar Pradesh Public Examinations (Prevention of Unfair Means) Ordinance, 2024, approved by state cabinet 25 June 2024. Applies to public service recruitment examinations, regularisation and promotion examinations, and entrance examinations for degree and diploma courses. Distribution of fake examination papers and creation of fake employment websites made punishable. Sentences from two years to life imprisonment with a fine of Rs. 1 crore.

S30 **CloudSEK, Threat Research and Information Analytics Division.** *Cyber Threats Targeting the Global Education Sector* (2022). India the largest global target for cyber threats to educational institutions and online platforms, followed by USA, UK, Indonesia and Brazil. 58% of education-sector threats detected across Asia-Pacific targeted Indian or India-based institutions and platforms; Indonesia second at 10%. 20% increase in global education-sector threats in Q1 2022 versus Q1 2021.

S31 **Cyble.** *India Threat Landscape Report 2024*. First half of 2024: 593 cyberattacks, 388 data breaches, 107 data leaks, 39 ransomware incidents recorded across all Indian sectors.

S32 **Careers360; PTI.** Defacement of IIT Kanpur and IIT Madras websites, July 2026, by an applicant rejected from the undergraduate cybersecurity programme, who publicised the intrusion on social media. Message left on the IIT Kanpur site. Institute director confirmed the applicant was not shortlisted.

S33 **Independent security researcher disclosure (V. K. Yadav), published 2023.** Authentication weakness in a third-party examination portal permitting administrative password reset and access to portal dashboards, student details, conducted examinations, questions, answers and results. Client base included multiple IITs and large private universities. Approximately 1,000+ Indian institutions, 1 million students and 65,000+ teachers in scope. Disclosed responsibly and remediated by the vendor within approximately two hours.

S34 **Indian technology press.** Defacement of the Rajasthan Education Department website, April 2025; homepage modified to display inflammatory messages.

S35 **EDUCAUSE.** Higher education breach cost benchmark: in excess of USD 3 million per incident.

S36 **Reported PowerSchool breach disclosure.** December 2024 compromise of PowerSchool, a student information system provider holding records for an estimated 75% of the North American K-12 market. Attacker used compromised credentials belonging to a technical support subcontractor to access a customer-support portal lacking multi-factor authentication. Exposure of approximately 62 million students and 9.5 million educators across approximately 18,000 schools.

S37 **I4C projection, via Drishti IAS and The420.in.** Projection that India may lose in excess of Rs. 1.2 lakh crore to cyber fraud across 2025 on a broader definition, equivalent to approximately 0.7% of GDP. Approximately 4,000 mule bank accounts identified daily; 18 ATM hotspots identified.

S38 **NCRB data, via Citizens for Justice and Peace analysis.** For 2023: 22% of cybercrimes were charged; fewer than 3% resulted in conviction at trial.

S39 **Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) / I4C, via The Indian Express and The Wire.** Nearly 12 lakh cyber fraud complaints in 2024, of which approximately 45% originated from Southeast Asian jurisdictions including Cambodia, Myanmar and Laos. Since inception in 2021, CFCFRMS recorded 30.05 lakh complaints with losses reaching Rs. 27,914 crore (as at late 2024). First nine months of 2024: Rs. 11,333 crore lost; stock trading scams Rs. 4,636 crore across 2,28,094 complaints; investment scams Rs. 3,216 crore across 1,00,360 complaints; digital arrest frauds Rs. 1,616 crore across 63,481 complaints. Approximately 4.5 lakh mule accounts frozen in the year. 17,000 WhatsApp accounts blocked in collaboration with the Department of Telecommunications.

S40 **I4C, Ministry of Home Affairs.** Suspect Registry launched September 2024 in collaboration with banks; holds more than 11 lakh suspect identifiers. 24.67 lakh Layer-1 mule accounts shared with participating entities and declined; further losses of over Rs. 4,631 crore prevented. Samanvaya platform: 10,599 arrests facilitated, 26,096 criminal linkages uncovered; Pratibimb module maps cybercrime networks geographically.

Appendix B — Institutional Self-Assessment Questionnaire

This questionnaire is designed to be completed by an institution without external assistance, and to be answerable in a single sitting by whoever currently holds responsibility for institutional IT. Its purpose is diagnostic rather than rhetorical: the questions are drawn directly from the failure modes evidenced in Sections 5 to 9 of this report. An institution that cannot answer a question is, for the purposes of the DPDP obligations discussed in Section 15, in the same position as an institution whose answer is unsatisfactory.

Scoring guidance. Count each question you can answer with documentary evidence as 1, each you can answer only from memory or belief as 0.5, and each you cannot answer as 0. A score below 50 per cent of the available total places the institution at Level 0 or 1 of the maturity model in Table 17.1.

A. Detection and evidence

1. Can you state, with evidence, whether any of your systems were compromised in the last twelve months?
2. Do you retain ICT system logs for at least 180 days, within Indian jurisdiction?
3. Are your system clocks synchronised to NIC or NPL time servers?
4. If a student reported today that their data was for sale, how long would it take you to determine whether it came from you?
5. Has any external party ever assessed your internet-facing systems? When, and do you still hold the report?

B. Identity and access

1. Is multi-factor authentication enforced on every administrative account, with no exceptions?
2. Do any administrative credentials exist that more than one person knows?
3. When a staff member with system access leaves, what is the documented time to revocation, and who verifies it?
4. How many accounts on your student information system currently hold administrative privilege? Can you produce the list today?
5. Does any account still use a default or dictionary password? How do you know?

C. Data holdings and DPDP position

1. Do you hold a documented inventory of what personal data you hold, where, for what purpose, and for how long?
2. Do you hold Aadhaar numbers, caste category, income certificates or banking details? Under what lawful basis, and with what retention limit?
3. Is any student record store reachable from the public internet without authentication?
4. Have you separated a minimal permanent verification register from the full admission file that must be erased on schedule?
5. Do you admit any student below 18? If so, have you addressed the children's data obligations, which carry a Rs. 200 crore head?

6. Could you notify affected Data Principals within 72 hours of becoming aware of a breach? Who is the named owner of that process?

D. Third-party platforms

1. List every third-party platform holding student personal data or examination material.
2. For each, what security assessment was conducted before procurement, and what security obligations are in the contract?
3. For each, who at the vendor is contractually obliged to notify you of a breach, and within what period?
4. Does any vendor support account have access to your production data without multi-factor authentication?
5. If your student information system vendor were breached tomorrow, how would you find out?

E. Examination integrity

1. Between setting and delivery, how many individuals could unilaterally disclose a question paper?
2. Is examination material protected such that no single custodian, and no single compromised administrative account, can reconstruct it?
3. Can you produce an independently verifiable record of every access to examination material for a past cycle?
4. If a paper leaked, could you determine which custody point failed, or only that one did?

F. Brand and impersonation

1. Do you monitor for websites impersonating your institution?
2. Do you monitor for fraudulent fee-collection portals using your name during admission windows?
3. How would you learn that a fake scholarship or placement offer was circulating under your name?
4. What is your documented takedown process, and how quickly has it worked in practice?

G. Governance

1. Who at governing-body level is named as accountable for cybersecurity? (81 percent of UK institutions have such a person [S10].)
2. When did your governing body last receive a written report on cyber risk?
3. Is there a documented incident response plan? When was it last exercised, rather than last written?
4. What is your budgeted annual security spend, and what proportion of total IT spend is it?

> **How to read your own answers.** The questions most institutions cannot answer are those in Section A. That is the detection gap described in Section 1.1 of this report, measured on your own estate. It is also the specific capability that the DPDP 72-hour notification obligation presumes you already have.

Appendix C — Glossary

AISHE	All India Survey on Higher Education. Annual Ministry of Education survey; the authoritative count of Indian higher education institutions and enrolment.
Brute-force attack	Automated attempts to guess credentials by trying large numbers of username and password combinations.
BEC	Business Email Compromise. Fraud in which an attacker impersonates a trusted party by email to redirect a payment.
CERT-In	Indian Computer Emergency Response Team. National agency for cyber incident response; issues binding directions under Section 70B(6) of the IT Act, 2000.
CFCFRMS	Citizen Financial Cyber Fraud Reporting and Management System. I4C platform for reporting and interdicting cyber-financial fraud.
Credential stuffing	Use of username and password pairs stolen from one service to attempt access to another, exploiting password reuse.
Data Fiduciary	Under the DPDP Act, 2023, any person or organisation determining the purpose and means of processing personal data. Every Indian educational institution is a Data Fiduciary.
Data Principal	Under the DPDP Act, the individual to whom personal data relates.
Detection	A single event flagged by a security product. Not equivalent to an attack, an incident or a breach.
DPDP	Digital Personal Data Protection. Refers to the Act of 2023 and the Rules of 2025.
DDoS	Distributed Denial of Service. Flooding a service with traffic to render it unavailable.
GER	Gross Enrolment Ratio. Enrolment as a proportion of the eligible age cohort; 30.0 for Indian higher education in 2023-24.
I4C	Indian Cyber Crime Coordination Centre, Ministry of Home Affairs. Operates the NCRP and CFCFRMS.
Jisc	UK non-profit operating the Janet Network, a sector security operations centre and CSIRT for UK education and research. India has no equivalent.
KEV	Known Exploited Vulnerability. A vulnerability confirmed to be actively exploited, and therefore requiring priority remediation.
MFA	Multi-factor authentication. Requiring more than one form of evidence to authenticate; the single highest-value control in this sector.
Mule account	A bank account used to receive and move fraud proceeds, typically opened using another person's identity documents.
NCRB	National Crime Records Bureau. Publishes *Crime in India*; counts registered cases only.
NCRP	National Cyber Crime Reporting Portal, operated by I4C.
NIS2	EU Directive establishing cybersecurity obligations for essential and important entities.
Ransomware	Malware that encrypts data, or exfiltrates it for extortion, to compel payment. Increasingly extortion-only, without encryption.
SDF	Significant Data Fiduciary. A DPDP classification attracting additional obligations including a DPO, annual audit and impact assessments.
Threshold cryptography	Splitting a cryptographic capability among multiple holders such that a defined minimum number must cooperate to use it, and no single holder can act alone.
UGC	University Grants Commission. Statutory regulator; maintains the list of fake universities.
Zero-day	A vulnerability exploited before the vendor has issued a fix. CVE-2025-61882 in Oracle E-Business Suite is the 2025 education-sector example.

End of report. Prepared by Fortify Detection & Intelligence Wing, July 2026. Figures current to the dates stated in Appendix A. This document contains estimates, labelled as such, alongside measured figures attributed to named

sources; the two are not interchangeable and should not be quoted as though they were.