

Ransomware Awareness in Digital Era

Sohan Rajendra Shelar, Sahil Vinayak Kubade, Suyash Subhash Pisal

Department of Computer Science (M.Sc. Computer Application)

Pune Vidyarthi Griha's College of Science and Commerce, Pune

Savitribai Phule Pune University, Pune, India

Abstract—Ransomware has evolved from an occasional nuisance into a globally coordinated criminal industry, yet the human dimension of this threat—specifically how well individuals understand and defend against it—receives limited research attention. This paper addresses that gap through a mixed-methods study combining an original structured survey (n=30) of students, IT professionals, and educators at Indian academic institutions with secondary analysis of four major 2025–2026 threat intelligence reports. The survey reveals striking disconnects: while 70% of respondents reported prior awareness of ransomware, only 56.7% could correctly define it, 26.7% knew the exact steps to take during an active infection, and 36.7% consistently used Multi-Factor Authentication on all accounts. A concerning 40% backed up data rarely or never. These gaps mirror findings from the Sophos State of Ransomware 2025, which identifies lack of expertise as the leading operational root cause of ransomware victimization globally (40.2%) and in India (41%). Taken together, individual knowledge deficits and behavioural lapses aggregate into the organizational vulnerabilities that ransomware operators exploit systematically. This paper proposes an integrated defence framework grounded in both data streams.

Index Terms—ransomware, cybersecurity awareness, India, Multi-Factor Authentication, data backup, phishing, Ransomware-as-a-Service, incident response, DBIR.

I. Introduction

Few threats in modern computing have demonstrated the staying power of ransomware. From the rudimentary AIDS Trojan distributed via floppy disk in 1989 to the highly coordinated, AI-assisted campaigns of 2025, the core criminal logic has remained unchanged: encrypt a victim's data and extract payment before restoring access. What has changed dramatically is the scale, sophistication, and structural organization behind that logic.

The Verizon 2025 Data Breach Investigations Report, analysing 22,052 real-world security incidents, found ransomware present in 44% of all confirmed data breaches—a 37% increase over the prior year [1]. The Chainalysis 2026 Crypto Crime Report documents over \$820 million in on-chain ransomware payments in 2025, alongside a 50% year-over-year rise in claimed victims [2]. For India, the Sophos State of Ransomware in India 2025 reports that 42% of attacks on Indian organizations resulted in data encryption, with average recovery costs of \$1.01 million per incident [3].

What these macro statistics cannot reveal is the degree to which the people responsible for responding to these threats actually understand ransomware, recognize its delivery mechanisms, and know what to do when an attack begins. That question motivates this paper. The central premise is straightforward: organizational vulnerability to ransomware is not purely a technology problem—it is also a people problem. Individual knowledge gaps and behavioural lapses aggregate into the organizational vulnerabilities that attackers exploit routinely.

This paper contributes: (1) original empirical data on individual ransomware preparedness in an Indian academic context; and (2) an integrated analysis demonstrating that the individual gaps measured by the survey are structurally connected to the organizational vulnerabilities documented in global threat intelligence.

II. Related Work

Young and Yung introduced the concept of cryptoviral extortion in 1996, demonstrating that asymmetric cryptography could be weaponized to render data inaccessible without attacker cooperation [4]. Their framework directly anticipates the AES-RSA hybrid encryption architecture that characterizes virtually every modern ransomware variant—a design so effective that recovery without the attacker's private key remains computationally infeasible absent cryptographic implementation errors.

Oz et al. provide a comprehensive review of ransomware taxonomy and defence strategies through 2022, identifying backup integrity, behavioural endpoint monitoring, and network segmentation as the three most consistently validated countermeasures across the literature [5]. Each of these categories corresponds directly to gaps identified in the survey data presented in this paper.

Rajivan and Gonzalez demonstrated that phishing—the delivery mechanism underlying many ransomware infections—succeeds not through technical complexity but through exploitation of cognitive heuristics and contextual familiarity [6]. This has a direct implication for training design: knowing that phishing exists is not the same as being trained to recognize it under realistic pressure. The survey finding that 33.3% of respondents have accidentally clicked on suspicious content, despite broad awareness that phishing is the primary infection vector, reflects exactly this gap.

Blythe, Coventry, and Little examined conditions under which individuals comply with or deviate from stated security policies, finding that overconfidence in personal security practices is a consistent predictor of non-compliance [7]. This provides interpretive grounding for the observation that respondents' self-reported prevention confidence (mean=3.77/5) slightly exceeded their threat seriousness ratings (mean=3.67/5), suggesting that some participants may underestimate their own vulnerability.

III. Research Methodology

A. Study Design

This study adopts a mixed-methods, cross-sectional design. An original structured survey forms the primary data layer, while four industry threat intelligence reports constitute the secondary layer. The study is positioned as an exploratory inquiry; the sample size of $n=30$ supports descriptive analysis and pattern identification but does not permit population-level inference. All primary findings are presented as directional indicators and triangulated against large-scale secondary data before conclusions are drawn.

B. Survey Instrument

A 20-item structured questionnaire assessed five constructs: (1) conceptual knowledge of ransomware and the Ransomware-as-a-Service (RaaS) model; (2) familiarity with documented real-world incidents; (3) personal cyber hygiene behaviours including MFA usage, backup discipline, and software update practices; (4) institutional training availability and organizational readiness perceptions; and (5) threat perception, incident response knowledge, and payment attitude. Items used single-select multiple-choice formats and five-point Likert scales. The instrument was administered via Google Forms between April 2 and April 14, 2026.

C. Sample Characteristics

Thirty complete responses were collected. Table I summarizes the demographic profile. Students represent the largest share (70%), making the findings particularly relevant to higher education policy. The two faculty respondents produced a notable qualitative observation discussed in Section V-C.

TABLE I Respondent Demographics (n=30)

Attribute	Category	n	%
Role	Student	21	70.0
	IT Professional	4	13.3
	Faculty / Educator	2	6.7
	Other	3	10.0
Education	Undergraduate (UG)	17	56.7
	Postgraduate (PG)	8	26.7
	Working professional	2	6.7
	Pre-degree (10th/12th)	3	10.0
IT Experience	Less than 1 year	12	40.0
	1–3 years	11	36.7
	3–5 years	1	3.3
	More than 5 years	6	20.0

D. Secondary Data Sources

Four current intelligence reports provide the secondary layer: (1) Sophos State of Ransomware 2025 — Global, based on 3,400 IT/cybersecurity leaders across 17 countries [10]; (2) Sophos State of Ransomware in India 2025, drawn from 378 Indian respondents [3]; (3) Verizon 2025 Data Breach Investigations Report, analysing 22,052 incidents from 139 countries [1]; and (4) Chainalysis 2026 Crypto Crime Report, documenting on-chain ransomware financial flows [2]. All monetary figures are in U.S. dollars.

IV. Global and Indian Threat Landscape

A. Attack Vectors: How Ransomware Gets In

Fig. 1 shows the distribution of technical root causes across ransomware incidents for three consecutive years. Exploited vulnerabilities led for the third straight year at 32% in 2025, while phishing rose sharply from 11% to 18%—its fastest growth in the Sophos dataset [10]. The Verizon DBIR documents a 34% year-over-year increase in vulnerability exploitation, with edge devices and VPN appliances targeted in 22% of exploitation cases—nearly eight times the prior year [1]. Median time to remediate a known vulnerability was 32 days, and only 54% were fully remediated at all [1].

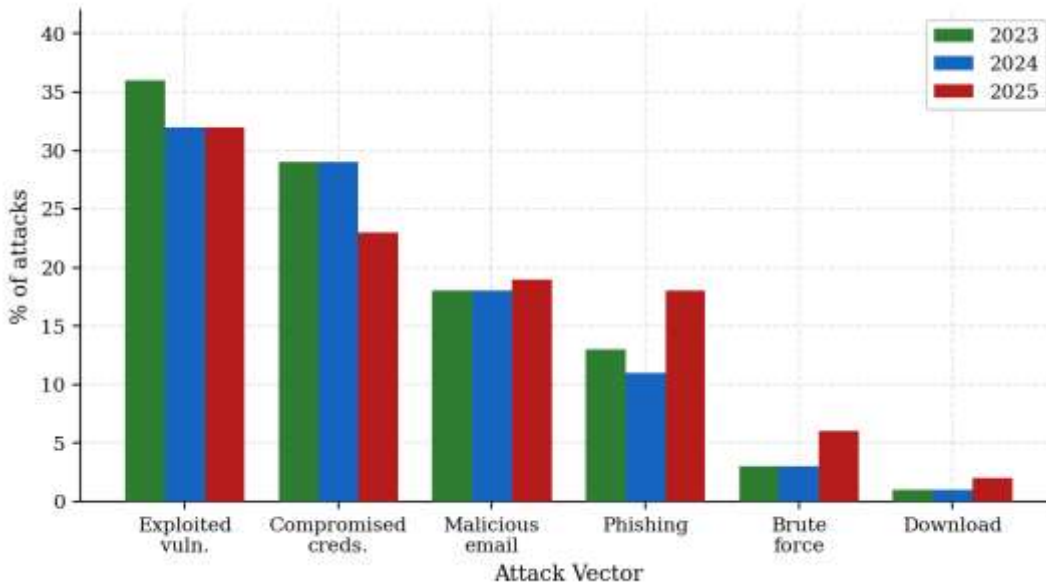


Fig. 1. Technical root cause of ransomware attacks 2023–2025, global (Source: Sophos 2025 [10])

In India, exploited vulnerabilities led at 29%, with compromised credentials at 22% and malicious email at 21% [3]. The near-parity of these three vectors in India means no single technical control provides dominant coverage. The Verizon DBIR also found that third-party involvement in breaches doubled in 2025, rising from 15% to 30% of all incidents [1].

B. Impact: Encryption, Exfiltration, and Recovery

Fig. 2 compares key outcome metrics between India and the global average. Globally, 50% of attacks resulted in data encryption in 2025—a six-year low from 70% in 2024 [10]. India's 42% figure sits below the global average. However, 28% of globally encrypted organizations also experienced data exfiltration [10]. India's recovery times are moving in the wrong direction: while 53% of global organizations recovered within a week (up from 35%), only 48% of Indian organizations achieved the same—down from 61% [3]. More Indian organizations took between one and six months to fully recover in 2025 than in 2024 [3].

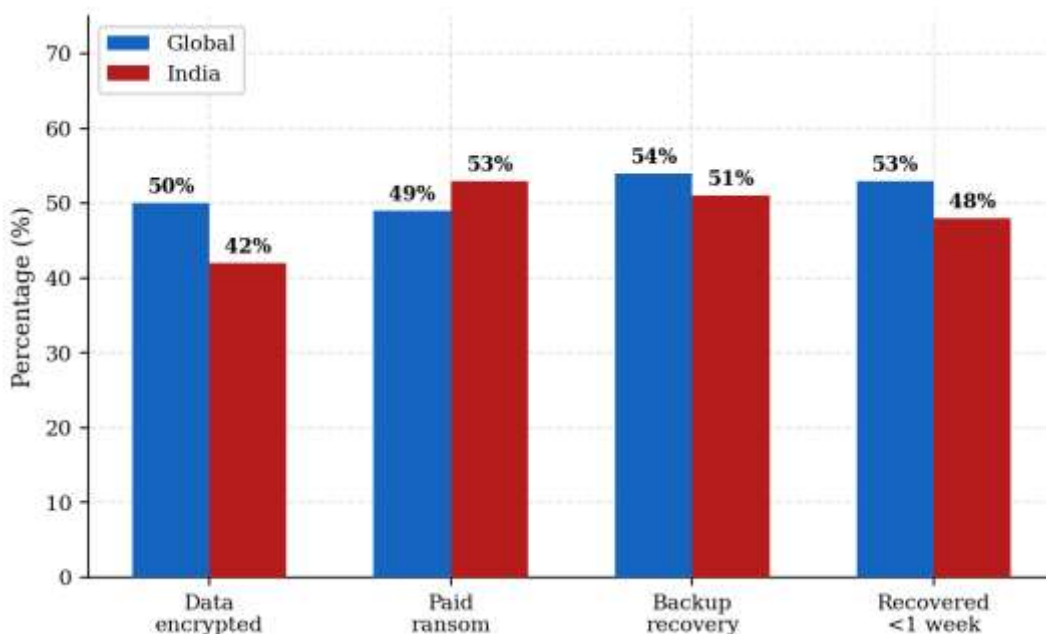


Fig. 2. Key ransomware outcome metrics: India vs. global (Source: Sophos 2025 [3][10])

C. Financial Dimensions

Globally, the median ransom demand fell 34% to \$1.32 million and the median payment fell 50% to \$1 million [10]. India showed steeper declines: a 52% drop in median demand to \$961,000 and a 79% drop in median payment to approximately \$482,000 [3]. The Chainalysis report documents over \$820 million in total on-chain payments, with the median payment rising 368% to \$59,556—indicating fewer organizations paying but larger amounts from those who do [2]. Claimed victims grew 50% year-over-year, with analysts tracking up to 85 active extortion groups operating through RaaS infrastructure [2].

V. Survey Results and Analysis

A. Awareness and Knowledge

Fig. 3 presents the six knowledge indicators measured by the survey. Seventy percent of respondents reported some prior awareness of ransomware, but only 56.7% could correctly define it as malware that encrypts files and demands payment for restoration. The remaining 43.3% selected incorrect definitions including 'a virus that slows down your computer' (23.3%), 'software that monitors your browsing activity' (10%), and 'a type of firewall' (10%).

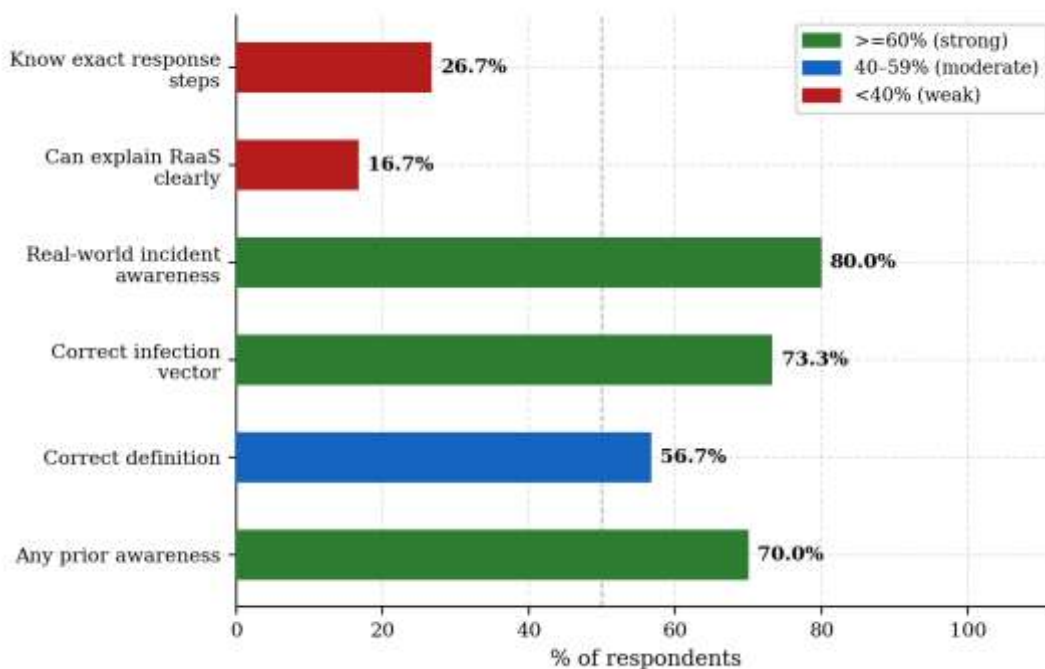


Fig. 3. Knowledge and awareness indicators, primary survey (n=30)

Incident familiarity was higher: 80% had heard of real-world events like WannaCry or Colonial Pipeline, though only 36.7% knew specific details. Awareness of the RaaS model was very limited: only 16.7% could explain it clearly, while 63.3% had heard the term without certainty of its meaning, and 20% had not encountered it at all. The sharpest finding is the incident response gap: only 26.7% knew exactly what steps to take if actively infected—the most consequential knowledge deficit the survey uncovered.

B. Cyber Hygiene Behaviours

Fig. 4 presents six behavioural indicators. MFA adoption shows 36.7% using it on all accounts, 26.7% on some accounts, and 30% not using it at all, with 6.7% unfamiliar with the concept. That means one-third of respondents have no MFA protection and are directly exposed to the compromised-credentials attack vector.

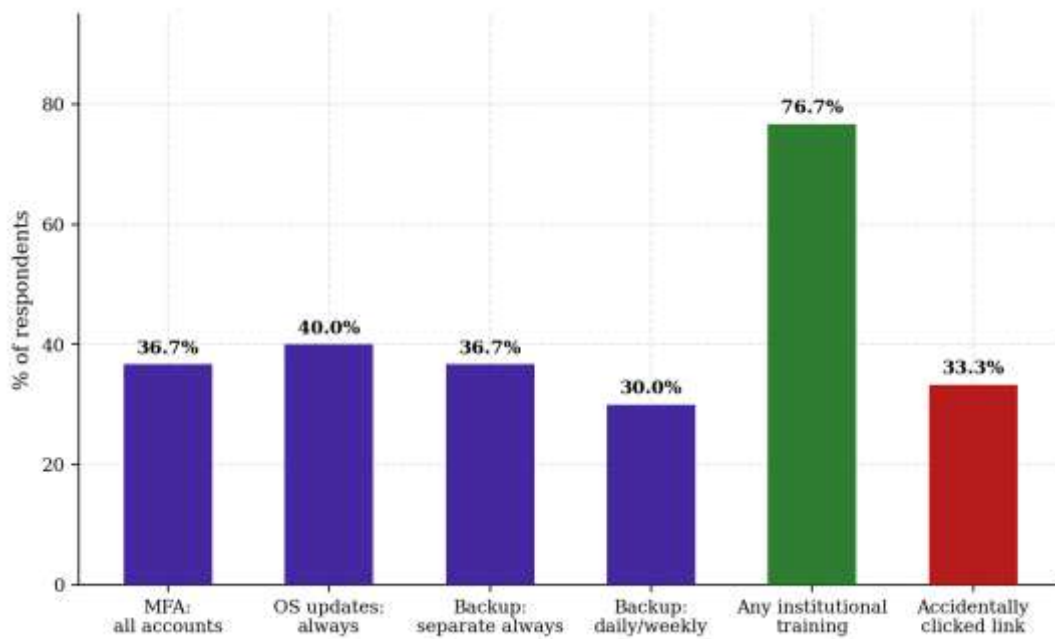


Fig. 4. Cyber hygiene behaviour rates, primary survey (n=30)

The backup data shown in Fig. 5 reveals a concerning distribution. Only 13.3% back up daily and 16.7% weekly—fewer than a third have backup habits providing meaningful recovery capability. A combined 40% back up rarely or never. When separate storage discipline is examined, only 36.7% maintain always-separate storage, 43.3% do so sometimes, 6.7% store backups on the same device (which ransomware would encrypt alongside primary data), and 13.3% do not back up at all.

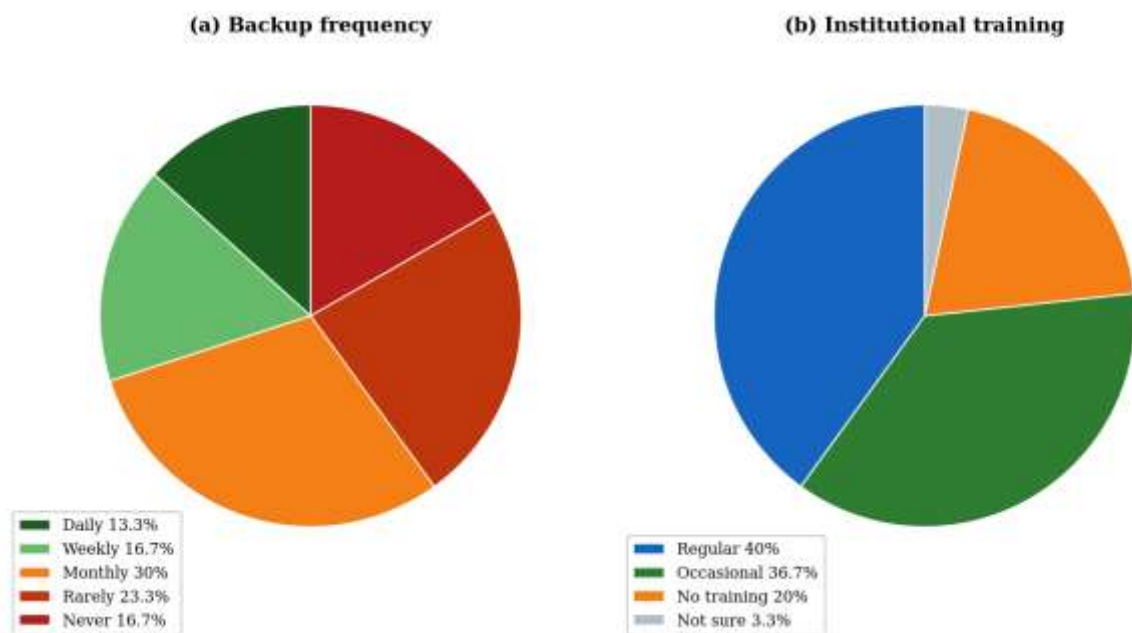


Fig. 5. Backup frequency and institutional training distribution (n=30)

Software patching showed improvement but remains incomplete: 40% always install updates promptly, 43.3% do so occasionally, and 16.7% rarely or never update. These individuals maintain exposure windows that may remain open for months, directly enabling the vulnerability exploitation vector that led global attack rankings for three consecutive years.

C. Attitudes and Self-Assessment

Forty-six percent of respondents stated they would not pay ransom, 13.3% would pay, 23.3% said it depends on data value, and 16.7% were unsure. Prevention confidence (mean=3.77) was slightly higher than threat seriousness ratings (mean=3.67)—the inverse of the pattern that effective risk perception typically follows. Individuals who feel adequately capable relative to the threat they perceive may not invest in further preparedness, a dynamic documented in [7].

A particularly notable observation concerns the two faculty/educator respondents. Both reported first-time exposure to the term 'ransomware' during the survey. One had never backed up data, did not know what MFA was, rarely updated software, and received

no institutional training. While statistically anecdotal at $n=2$, this pattern raises a pointed question: if those responsible for educating future IT users have not been exposed to basic cybersecurity concepts, the institutional knowledge deficit is reproduced and amplified with each student cohort. Seventy percent of all respondents endorsed the need for more cybersecurity education in academic institutions.

TABLE II Key Survey Findings at a Glance ($n=30$)

Category	Indicator	%
Knowledge	Any prior awareness	70.0
	Correct definition	56.7
	Correct infection vector	73.3
	Can explain RaaS	16.7
	Know exact response steps	26.7
Behaviour	MFA on all accounts	36.7
	Always updates promptly	40.0
	Separate backup (always)	36.7
	Rarely/never backs up	40.0
	Has clicked suspicious link	33.3
Institutional	Regular training available	40.0
	No training at all	20.0
Attitude	Would not pay ransom	46.7
	Threat seriousness (mean/5)	3.67
	Prevention confidence (mean/5)	3.77
	More education needed	70.0

VI. Discussion

A. The Macro-Micro Correspondence

The most significant analytical contribution of this paper is the structural correspondence between the operational root causes of ransomware victimization—documented across all four secondary sources—and the individual behavioural deficits measured by the survey. Sophos identifies lack of expertise as the top operational cause in India [3]. The survey finds 73.3% lack knowledge of incident response steps. The Sophos global report finds unknown security gaps contributed to 40.1% of victimization events [10]. The survey finds 33.3% have accidentally engaged with suspicious content they did not recognize as a threat. The Verizon DBIR documents 32-day vulnerability remediation delays [1]. The survey finds only 40% update promptly.

These are not coincidences. Individual behaviours aggregate into organizational risk profiles. Academic institutions continuously produce workers whose individual preparedness directly shapes the security posture of every organization that hires them.

B. India's Recovery Paradox

India's worsening recovery times—from 61% recovering within a week to 48%—sit in apparent contradiction with improved encryption-prevention rates. The survey data provides the plausible explanation: with only 26.7% of individuals knowing correct incident response steps, a successful attack detection is not automatically followed by efficient recovery. Containing an incident, preserving forensic evidence, restoring from backups, and coordinating stakeholder communication all require skills and pre-planned procedures that the survey population largely lacks.

C. RaaS Fragmentation and the Academic Target Profile

The Chainalysis report's documentation of 85 active extortion groups [2], combined with the explicit observation that fragmented RaaS operators increasingly target smaller organizations expected to pay faster, positions academic institutions directly in the crosshairs. Universities store valuable personal and financial data, operate with modest IT security resources relative to their attack surface, and are populated by users with inconsistent security practices. The survey finding that only 36.7% of respondents consider their institution well-protected, and that 20% receive no cybersecurity training at all, confirms this targeting risk is not matched by institutional investment.

VII. Defence Framework and Recommendations

A. Mandatory Institutional Cybersecurity Training

The 20% with no training, the 73.3% knowledge gap on incident response, and the faculty-level awareness deficit make this the highest-priority single intervention. Training must cover ransomware definition and recognition, phishing identification, MFA setup, backup discipline, and the exact steps to take during an active infection. It should be integrated into mandatory coursework for all degree programs—not only IT and computer science.

B. Universal MFA Deployment

With 30% of respondents using no MFA, and compromised credentials accounting for 22% of Indian ransomware attacks [3], MFA on all institutional accounts is a straightforward and high-impact control. Institutions should configure MFA as mandatory for all student and faculty logins to email, cloud storage, and institutional portals. The 6.7% unfamiliar with MFA as a concept indicates that deployment must be accompanied by clear onboarding guidance.

C. The 3-2-1-1-0 Backup Standard

The backup situation in the survey— 40% rarely or never backing up, 43.3% not consistently using separate storage—is too poor to address through policy alone. Table III maps each element of the 3-2-1-1-0 framework to specific evidence from the survey or threat intelligence. The critical addition to the classic 3-2-1 rule is one immutable or air-gapped copy, providing a guaranteed clean recovery source even when attackers specifically target and corrupt backup directories. The zero-errors element mandates regular tested restoration drills: a backup that has never been tested is not a backup, it is an assumption.

TABLE III 3-2-1-1-0 Backup Framework with Evidence Mapping

Rule	Requirement	Evidence anchor
3	Primary + 2 independent backups	40% rarely/never back up
2	Two distinct storage media	Single medium fails with primary device
1	One off-site or cloud copy	28% globally also suffered exfiltration [10]
1	One immutable/air-gapped copy	RaaS strains enumerate & encrypt backup dirs [2]
0	Zero restoration errors (tested)	Backup recovery at 6-yr global low [10]

D. Simulated Phishing Programs

Seventy-three percent of respondents correctly identified phishing/malicious links as the primary infection vector, yet 33.3% have still accidentally clicked on suspicious content. This is the clearest demonstration that declarative knowledge does not translate automatically to behavioural caution [6]. Simulated phishing exercises with immediate post-click feedback are the evidence-backed intervention for closing this specific gap, and should be conducted at least quarterly.

E. Structured Incident Response Planning

The 73.3% who cannot confidently execute correct incident response steps need a documented, rehearsed plan to fall back on during a real event. Every institution should develop a Cyber Incident Response Plan (CIRP) aligned with CISA guidance [8], covering: isolation of affected devices from the network; forensic image capture before any remediation; out-of-band communication (voice calls rather than institutional email, which may be monitored by the attacker); and restoration from the verified clean backup.

F. Accelerated Patch Management

Given that exploited vulnerabilities have led the global attack vector ranking for three consecutive years [10], and that only 40% of survey respondents always update promptly, institutions should implement automated OS and application update policies

for all managed devices. Faculty and students should understand explicitly that security updates are not optional maintenance—they are direct risk reduction with a measurable impact on attack exposure windows.

VIII. Conclusion

This paper has developed an integrated, dual-track analysis of ransomware as a threat that operates simultaneously at the macro level of organizational and global dynamics and at the micro level of individual knowledge, behaviour, and institutional training. The survey data makes the individual-level picture concrete: 56.7% correct on definition, 26.7% confident in incident response, 36.7% using MFA on all accounts, 40% backing up rarely or never. These are not abstract statistics—they describe the knowledge and behavioural state of individuals who will shortly enter India's IT workforce.

The threat intelligence sources paint the context they will enter: ransomware in 44% of all confirmed breaches globally [1], a 50% surge in claimed victims [2], India's recovery times worsening against global trends [3], and a criminal ecosystem of 85+ active groups increasingly targeting smaller, faster-paying organizations including academic institutions [2]. The structural argument of this paper is that these two pictures are causally connected: individual knowledge gaps aggregate into the organizational expertise deficits that threat intelligence sources document as the leading cause of victimization. Addressing the macro problem requires closing the micro gap first.

The defence framework in Section VII translates this analysis into actionable steps. Mandatory training, universal MFA, the 3-2-1-1-0 backup standard, simulated phishing programs, structured incident response planning, and automated patch management are not novel concepts—but they remain incompletely implemented in the academic settings reached by this survey. The 70% of respondents who believe more cybersecurity education is definitely needed are correct. Acting on that consensus is the most impactful step available to Indian academic institutions today.

Future research should extend this survey to a larger, geographically representative national sample; develop pre/post training assessments to measure whether interventions close the gaps identified here; and investigate whether the faculty-level awareness deficit observed is representative of a broader institutional pattern.

. References

- [1] C. D. Hylender, P. Langlois, A. Pinto, and S. Widup, "2025 Data Breach Investigations Report," Verizon Business, 2025.
- [2] Chainalysis Inc., "The 2026 Crypto Crime Report," Chainalysis, March 2026.
- [3] Sophos Ltd., "The State of Ransomware in India 2025," Sophos Whitepaper, June 2025.
- [4] A. Young and M. Yung, "Cryptovirology: Extortion-based security threats and countermeasures," in Proc. IEEE Symposium on Security and Privacy, Oakland, CA, 1996, pp. 129–140.
- [5] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, "A Survey on Ransomware: Evolution, Taxonomy, and Defence Solutions," ACM Computing Surveys, vol. 54, no. 11, pp. 1–37, 2022.
- [6] P. Rajivan and C. Gonzalez, "Creative Persuasion: A Study on Adversarial Behaviours and Strategies in Phishing Attacks," Frontiers in Psychology, vol. 9, p. 135, 2018.
- [7] J. M. Blythe, L. Coventry, and L. Little, "Unpacking Security Policy Compliance: The Motivators and Barriers of Employees' Security Behaviours," in Proc. Symposium on Usable Privacy and Security (SOUPS), Ottawa, Canada, 2015, pp. 103–122.
- [8] Cybersecurity and Infrastructure Security Agency (CISA), "#StopRansomware Guide," CISA, Washington, D.C., 2023. [Online]. Available: <https://www.cisa.gov/stopransomware/ransomware-guide>
- [9] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, 2020.
- [10] Sophos Ltd., "The State of Ransomware 2025," Sophos Whitepaper, June 2025.