Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

# Divergent Paths to Cyber Resilience: A Comparative Technical and Legal Study of Cybersecurity Governance, Incident Response Frameworks, and Neuro-Symbolic Auditing in Bangladesh and India

**MD Shamsad Hossain**

253-26-048@diu.edu.bd

Daffodil International University https://orcid.org/0009-0006-1896-8468

**Humaira Tausif Surovi**

surovi.law0110.c@diu.edu.bd

Daffodil International University

**Ahsanul Haque Shawon**

253-26-075@diu.edu.bd

Daffodil International University

**Research Article**

**Keywords:** Cyber resilience, cybersecurity governance, incident response, legal-to-technical mapping, neuro-symbolic AI, digital forensics, Bangladesh, India

**Posted Date:** November 24th, 2026

**DOI:** https://doi.org/10.21203/rs.3.rs-11815590/v1

**License:** This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

**Additional Declarations:** The authors declare no competing interests.

# Divergent Paths to Cyber Resilience: A Comparative Technical and Legal Study of Cybersecurity Governance, Incident Response Frameworks, and Neuro-Symbolic Auditing in Bangladesh and India

Humaira Tausif Surovi*, MD Shamsad Hossain†, and Ahsanul Haque Shawon‡
*†‡Department of Law, Daffodil International University, Dhaka, Bangladesh
Email: *surovi.law0110.c@diu.edu.bd, †253-26-048@diu.edu.bd, ‡253-26-075@diu.edu.bd
ORCID: †0009-0006-1896-8468

***Abstract*—National cyber resilience extends beyond statutory criminalization or perimeter software deployment; it requires institutional capacity to anticipate threats, detect intrusions within strict time windows, coordinate multi-agency containment, preserve admissible digital evidence, and restore critical services. This paper presents a comparative technical and legal evaluation of cybersecurity governance, incident-reporting mandates, critical information infrastructure (CII) protection, and data privacy in Bangladesh and India. Analyzing time-sensitive instruments—including Bangladesh's Cyber Security Act 2026 (replacing the Cyber Security Ordinance 2025) alongside India's Information Technology Act 2000, CERT-In Directions 2022, and Digital Personal Data Protection (DPDP) Act 2023 and Rules 2025—we map statutory mandates directly to ISO/IEC 27001:2022, NIST SP 800-53, and CIS Controls v8. To bridge cross-border operational delays, we propose the Cross-Border Cyber Resilience Interoperability Architecture (CRIA) and formulate a quantitative Operational Cyber Resilience Index ($R_{\text{ops}}$). Furthermore, we implement and validate *LexCyber-Engine*, a Neuro-Symbolic AI prototype combining RDF/SHACL rule validation with Retrieval-Augmented Generation (RAG), to automate legal gap detection and digital evidence integrity auditing.**

***Index Terms*—Cyber resilience, cybersecurity governance, incident response, legal-to-technical mapping, neuro-symbolic AI, digital forensics, Bangladesh, India.**

## I. Introduction

Modern public administration, financial clearing systems, healthcare networks, and utilities rely heavily on interconnected digital infrastructure. While digital transformation improves service delivery, it expands the attack surface for ransomware syndicates, supply-chain compromises, and autonomous threats. Consequently, cybersecurity is no longer solely a technical engineering problem; it sits at the intersection of statutory governance, operational readiness, digital forensics, and constitutional accountability.

Preventing perimeter intrusions is insufficient for national security. True cyber resilience requires institutions to detect anomalies rapidly, contain lateral movement, preserve forensically sound evidence, restore trusted operations, and institutionalize post-incident lessons. The NIST Cybersecurity Framework (CSF) 2.0 formalizes this lifecycle across six core functions: *Govern, Identify, Protect, Detect, Respond,* and *Recover* [1]. Similarly, the International Telecommunication Union (ITU) Global Cybersecurity Index (GCI) evaluates national commitment across legal, technical, organizational, capacity-building, and cooperative pillars [2].

Bangladesh and India present a compelling comparative case study. As neighboring South Asian economies with shared financial and digital dependencies, both face overlapping regional threat vectors while exhibiting distinct regulatory scales and operational maturity. A persistent challenge in both jurisdictions is the gap between statutory law on paper and real-world technical execution. Statutory instruments evolve rapidly: Bangladesh enacted the Cyber Security Act 2026 on April 10, 2026, repealing the Cyber Security Ordinance 2025 [3], whereas India enforces the Information Technology Act 2000 [4] alongside the binding CERT-In Directions 2022 [5] and the DPDP Act 2023 and Rules 2025 [6], [7].

This paper makes four primary contributions:

1) **Lifecycle Governance Comparison:** Evaluates formal cybersecurity governance and statutory duties across Bangladesh and India throughout the full incident lifecycle.
2) **Legal-to-Technical Control Mapping:** Translates statutory reporting, logging, and CII mandates into actionable engineering controls under ISO/IEC 27001:2022 [9], NIST SP 800-53 Rev. 5 [10], and CIS Controls v8 [11].
3) **CRIA Architecture & Resilience Modeling:** Proposes the Cross-Border Cyber Resilience Interoperability Architecture (CRIA) and an Operational Cyber Resilience Index ($R_{\text{ops}}$) to measure practical recovery performance.
4) **Automated Neuro-Symbolic Legal Auditing:** Implements an open-source prototype (*LexCyber-Engine*) using RDFlib, pySHACL [12], and ChromaDB to deterministically detect evidentiary chain-of-custody flaws and statutory reporting gaps.

## II. Theoretical Framework and Related Work

### A. Dimensions of Cyber Resilience

Traditional information security focuses on confidentiality, integrity, and availability (CIA). Cyber resilience extends this

baseline by asking how rapidly an organization can absorb shock, contain compromise, and recover verified services under active adversarial pressure [1]. In the 2024 ITU Global Cybersecurity Index, both Bangladesh and India achieved placement in the top "Role-Modelling" tier [2]. However, high-level policy scores measure formal legislative existence rather than sector-wide operational readiness across small enterprises, hospitals, and municipal utilities.

### B. National CERTs and Operational Lessons

National Computer Emergency Response Teams (CERTs)—specifically BGD e-GOV CIRT in Bangladesh and CERT-In in India—serve as central threat intelligence and incident coordination hubs [5], [8]. Historical incidents underscore the necessity of layered technical and procedural defenses. For example, the 2016 Bangladesh Bank cyber heist, which resulted in approximately US$81 million in fraudulent transfers, demonstrated how attackers exploit gaps between financial messaging controls, network segmentation, anomaly detection, and cross-border response coordination [8].

## III. Methodology

This study employs a mixed qualitative doctrinal and technical systems-engineering methodology:

- **Primary Legal Corpus:** Analyzes current statutory texts, including Bangladesh's Cyber Security Act 2026 [3] and national CII guidelines [8], alongside India's IT Act 2000 [4], CERT-In Directions 2022 [5], DPDP Act 2023 [6], and DPDP Rules 2025 [7].
- **Control Mapping Synthesis:** Cross-references statutory obligations against international technical standards (NIST CSF 2.0 [1], ISO/IEC 27001:2022 [9], NIST SP 800-53 Rev. 5 [10], and CIS Controls v8 [11]).
- **Empirical & Prototype Validation:** Evaluates sector-level operational resilience metrics ($R_{\text{ops}}$) and validates statutory gap detection via a Python-based Neuro-Symbolic AI prototype.

## IV. Governance and Legal Control Mapping

### A. Institutional Governance Structures

In Bangladesh, the National Cyber Security Agency (NCSA) and BGD e-GOV CIRT oversee national cyber posture, CII protection guidelines, and digital forensics capacity under the Cyber Security Act 2026 [3], [8]. In India, the Ministry of Electronics and Information Technology (MeitY) and CERT-In exercise statutory authority under Section 70B of the IT Act 2000 [4], [5], supported by the National Critical Information Infrastructure Protection Centre (NCIIPC) and the Data Protection Board under the DPDP framework [6], [7].

### B. Mapping Statutory Rules to Technical Controls

To bridge the gap between legal compliance and Security Operations Center (SOC) engineering, Table I maps key statutory provisions in India and Bangladesh directly to technical control frameworks.

As illustrated in Table I, India's CERT-In Directions 2022 impose explicit quantitative operational benchmarks (a 6-hour reporting window, 180-day log retention, and mandatory NTP synchronization) [5]. Conversely, while Bangladesh's Cyber Security Act 2026 [3] and CII guidelines [8] establish institutional mandates, the lack of a unified, statutory hourly reporting threshold creates compliance ambiguity across sectors.

## V. Emerging Threat Vectors and Forensic Integrity

### A. Ransomware-as-a-Service (RaaS) and Extortion

Modern RaaS campaigns employ double and triple extortion—exfiltrating sensitive data prior to encryption and threatening downstream partners. Statutory frameworks in both jurisdictions criminalize unauthorized access and system disruption [3], [4], but neither provides comprehensive regulatory clarity regarding ransom payment prohibitions or safe-harbor protections for organizations sharing threat telemetry in good faith.

### B. Supply-Chain Compromises and AI-Driven Threats

Third-party API vulnerabilities and compromised software dependencies allow attackers to pivot across national borders into healthcare and financial networks. Simultaneously, adversaries utilize generative AI for polymorphic malware obfuscation and deepfake voice/video social engineering. Static signature-based Intrusion Detection Systems (IDS) are insufficient against dynamic AI threats; SOCs must deploy Extended Detection and Response (XDR) with behavioral telemetry (NIST SP 800-53 AU-6) [10].

### C. Digital Evidence Admissibility

Cross-border cyber prosecutions frequently fail due to evidentiary defects rather than substantive legal gaps. Volatile cloud logs, unverified chain-of-custody records, deprecated hashing algorithms (such as MD5), and unsynchronized system clocks allow defense counsel to challenge the integrity of digital exhibits under domestic evidence laws.

## VI. Proposed Cross-Border Architecture (CRIA) and Resilience Index

### A. Cross-Border Cyber Resilience Interoperability Architecture

Because full statutory harmonization between sovereign states is slow, we propose the **Cross-Border Cyber Resilience Interoperability Architecture (CRIA)** to enable real-time technical cooperation between BGD e-GOV CIRT and CERT-In without altering domestic constitutional safeguards:

1) **Tier 1 — Automated Threat Intelligence Exchange Protocol (ATIX-P):** Exchanges machine-readable STIX 2.1 / TAXII 2.1 JSON feeds containing sanitized Indicators of Compromise (malicious IP pools, file hashes, YARA rules).

TABLE I
MAPPING OF STATUTORY CYBERSECURITY MANDATES IN BANGLADESH AND INDIA TO TECHNICAL CONTROL FRAMEWORKS

| Statutory Provision | Jurisdiction & Source | ISO/IEC 27001:2022 [9] | NIST SP 800-53 Rev. 5 [10] | CIS Controls v8 [11] | Required Technical Implementation |
|---|---|---|---|---|---|
| **6-Hour Incident Reporting Window** | India: CERT-In Dir. 2022 (Sec. 70B) [5] | A.5.24 (Incident planning) | IR-6 (Incident Reporting) | Control 17.5 (Automate alerts) | Automated SIEM Severity-1 rule triggers connected via SOAR playbooks to national CERT portals. |
| **180-Day Domestic Log Retention** | India: CERT-In Dir. 2022 [5] | A.8.15 (Logging) | AU-11 (Audit Retention) | Control 8.3 (Audit log storage) | Write-Once-Read-Many (WORM) centralized SIEM cold storage with cryptographic hash chaining. |
| **NTP System Clock Synchronization** | India: CERT-In Dir. 2022 [5] | A.8.17 (Clock sync) | AU-8 (Time Stamps) | Control 8.4 (Standardize NTP) | Mandatory endpoint and gateway synchronization with NPLI/NIC official NTP time sources ($\leq$ 1000 ms drift). |
| **CII Protection & Continuity** | Bangladesh: CSA 2026 & CII Guide [3], [8] | A.8.20 (Network security) | CP-2 (Contingency Plan) | Control 11 (Data Recovery) | OT/IT network micro-segmentation, Zero-Trust Architecture (ZTA), and offline immutable backups. |
| **Personal Data Breach Safeguards** | India: DPDP 2023/2025 [6], [7]; BGD Law [3] | A.5.34 (Privacy of PII) | SC-28 (Protection at Rest) | Control 3 (Data Protection) | AES-256 encryption at rest, TLS 1.3 in transit, automated Data Loss Prevention (DLP), and pseudonymization. |

2) **Tier 2 — Bilateral Incident Escalation Taxonomy (BIET):** Aligns severity thresholds so Severity-1 critical infrastructure disruptions trigger immediate bilateral SOC escalation.
3) **Tier 3 — Mutual Evidence Preservation Protocol (MEPP):** Enforces RFC 6962-compliant Merkle Tree log hashing and digital signatures at initial acquisition to preserve evidentiary admissibility pending formal Mutual Legal Assistance Treaty (MLAT) execution.

### B. Operational Cyber Resilience Index ($R_{ops}$)

To move beyond static policy rankings, we formulate the Operational Cyber Resilience Index ($R_{\text{ops}}$) to measure practical institutional performance:

$$R_{\text{ops}} = \frac{(E_{\text{int}} \times T_{\text{idx}})}{(T_{\text{detect}} \cdot W_1) + (T_{\text{contain}} \cdot W_2) + (T_{\text{restore}} \cdot W_3)} \times 100 \tag{1}$$

where $T_{\text{detect}}$, $T_{\text{contain}}$, and $T_{\text{restore}}$ denote Mean Time to Detect, Contain, and Restore (in hours) weighted by criticality $(W_1, W_2, W_3)$, $E_{\text{int}} \in [0, 1]$ represents cryptographic evidence integrity compliance, and $T_{\text{idx}} \in [0, 1]$ denotes post-incident transparency reporting.

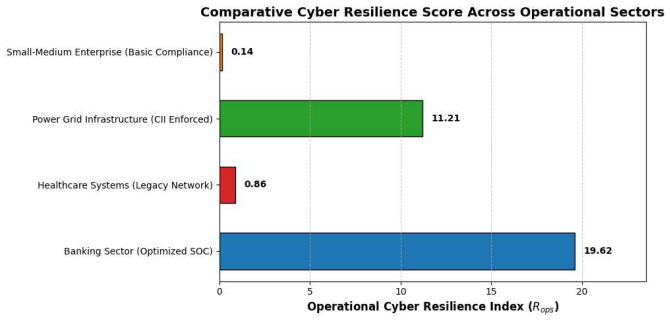



Fig. 1. Comparative Operational Cyber Resilience Index ($R_{\text{ops}}$) across operational sectors calculated using Equation (1), illustrating the disparity between optimized SOC banking infrastructure and under-resourced SMEs.

As shown in Fig. 1, banking infrastructure with automated SOC workflows achieves an $R_{\text{ops}}$ score of 19.62, whereas small and medium enterprises (SMEs) with basic compliance score 0.14 due to prolonged detection and recovery latencies.

## VII. PROTOTYPE IMPLEMENTATION: LEXCYBER-ENGINE

To operationalize the legal-to-technical audit principles of CRIA, we developed an open-source Neuro-Symbolic AI prototype named **LexCyber-Engine**. Pure LLMs frequently hallucinate statutory section numbers when analyzing complex legal scenarios. LexCyber-Engine eliminates citation hallucination by coupling deterministic symbolic logic with dense vector retrieval [14].

### A. System Architecture and Open-Source Stack

The prototype was implemented in Python and validated in a Google Colab environment using three core modules:

- **Symbolic Knowledge Graph & Rule Validator:** Constructed using `RDFlib` and `pySHACL` [12] to encode statutory rules as Shapes Constraint Language (SHACL) graphs. The engine deterministically validates forensic telemetry—flagging NTP clock drift ($>$ 1000 ms), weak cryptographic hash functions (MD5/SHA-1), and missing chain-of-custody logs.
- **Dense Vector Retrieval (RAG):** Legislative texts from Bangladesh (Cyber Security Act 2026 [3]) and India (IT Act 2000 [4], CERT-In Directions 2022 [5], DPDP Act 2023 [6]) were embedded via `BAAI/bge-small-en-v1.5` [13] and stored in `ChromaDB`.
- **Constrained Explanation Generator:** Verified SHACL violation triples and top-$k$ retrieved statutory clauses are injected into an open-source LLM (`openai/gpt-oss-120b`) constrained strictly to citing retrieved graph nodes.

### B. Experimental Case Validation Results

We evaluated *LexCyber-Engine* on a simulated double-extortion ransomware scenario targeting a commercial bank in

Dhaka involving 500 GB of exfiltrated financial data, delayed regulatory notification ($> 6$ hours), MD5 log hashing, and an NTP clock drift of $4,200$ ms.

TABLE II
LEXCYBER-ENGINE AUTOMATED VULNERABILITY AUDIT OUTPUT

| Audit Dimension | Input Telemetry / Fact | Deterministic AI Finding |
|---|---|---|
| **Applicable Statutes** | CII bank intrusion & data breach | BGD CSA 2026 (Sec. 17) [3]; IND CERT-In Dir. 2022 (Sec. 70B) [5] |
| **Clock Synchronization** | $4,200$ ms NTP drift | **SHACL Violation:** Exceeds 1000 ms limit (ISO 27001 A.8.17) [9] |
| **Cryptographic Integrity** | MD5 log hash algorithm | **SHACL Violation:** Collision-prone; inadmissible in court |
| **Custody Chain** | Unrecorded seizure log | **SHACL Violation:** Missing written chain-of-custody record |
| **Statutory Lacuna** | Delayed breach disclosure | BGD CSA 2026 lacks IND's explicit 6-hour reporting deadline [5] |

As documented in Table II, the symbolic SHACL engine deterministically detected all three evidentiary admissibility defects prior to neural text generation, demonstrating how technical telemetry failures compromise judicial accountability even when substantive cybercrime statutes apply.

## VIII. CONCLUSION AND FUTURE RESEARCH

This paper compared cybersecurity governance, statutory frameworks, and incident response readiness across Bangladesh and India. While both countries demonstrate strong formal policy commitments, operational resilience depends on translating statutory mandates into verifiable technical controls, enforceable reporting timelines, and forensically sound evidence preservation. Our proposed CRIA architecture, $R_{\text{ops}}$ metric, and *LexCyber-Engine* Neuro-Symbolic prototype provide an actionable blueprint for bridging statutory design and operational execution. Future work will expand the RDF Legal Knowledge Graph to cover multi-sector judicial precedents and evaluate prototype performance across larger datasets of anonymized cross-border incident reports.

## REFERENCES


[1] C. Pascoe, S. Quinn, and K. Scarfone, "The NIST Cybersecurity Framework (CSF) 2.0," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST CSWP 29, Feb. 2024.

[2] International Telecommunication Union, *Global Cybersecurity Index 2024*, 5th ed. Geneva, Switzerland: ITU, 2024.

[3] Government of Bangladesh, "Cyber Security Act, 2026 (Act No. 81 of 2026)," *Bangladesh Laws*, Apr. 10, 2026. [Online]. Available: https://bdlaws.minlaw.gov.bd/act-print-1710.html

[4] Government of India, *The Information Technology Act, 2000*, Act No. 21 of 2000, Jun. 9, 2000.

[5] Indian Computer Emergency Response Team (CERT-In), "Directions under sub-section (6) of section 70B of the Information Technology Act, 2000," MeitY, Govt. of India, Apr. 28, 2022.

[6] Government of India, *The Digital Personal Data Protection Act, 2023*, Act No. 22 of 2023, Aug. 11, 2023.

[7] Ministry of Electronics and Information Technology, Govt. of India, "Digital Personal Data Protection Rules, 2025," Nov. 14, 2025.

[8] National Cyber Security Agency, Govt. of Bangladesh, "Guidelines and Strategies for Critical Information Infrastructure," official portal, 2025.

[9] ISO/IEC, "Information security, cybersecurity and privacy protection — Information security management systems — Requirements," ISO/IEC 27001:2022, Oct. 2022.

[10] Joint Task Force, "Security and Privacy Controls for Information Systems and Organizations," NIST Special Publication 800-53, Rev. 5, Sep. 2020.

[11] Center for Internet Security, "CIS Critical Security Controls Version 8," CIS, East Greenbush, NY, 2021.

[12] W3C, "Shapes Constraint Language (SHACL)," W3C Recommendation, Jul. 2017. [Online]. Available: https://www.w3.org/TR/shacl/

[13] S. Xiao, Z. Liu, P. Zhang, and N. Muennighoff, "C-Pack: Packaged Resources To Advance General Chinese Embedding," *arXiv preprint arXiv:2309.07597*, 2023.

[14] P. Lewis *et al.*, "Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks," in *Proc. Advances in Neural Information Processing Systems (NeurIPS)*, vol. 33, 2020, pp. 9459–9474.