International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 15, Issue 3 [March 2026] PP: 75-79

Cybersecurity Risks, Challenges, and a Multi-Layer Resilience Framework

Gaurav Singh Rana[1], Dr Amardeep Singh[2], Dr Manish Gupta[3], Dr R. Chitra[4]
[1] *Scientist C, Central Soil and Materials Research Station, New Delhi*
[2, 3] *Scientist E, Central Soil and Materials Research Station, New Delhi*
[4] *Director, Central Soil and Materials Research Station, New Delhi*

Abstract: *The rapid growth of digital technologies in India has significantly transformed operational processes and service delivery across multiple sectors. At the same time, increasing reliance on interconnected Information and Communication Technology (ICT) systems has brought greater attention to cybersecurity risk management and resilience.*

This paper examines the evolving cybersecurity risk landscape and key implementation considerations in complex digital environments. Using the 2022 cyber incident at the All India Institute of Medical Sciences (AIIMS), New Delhi as an illustrative case, the study highlights the importance of preparedness, response coordination, and recovery capabilities in ensuring continuity of critical services. The study demonstrates that multi-layer resilience frameworks improve preparedness and service continuity.

The paper identifies key categories of cybersecurity risks, discusses implementation considerations, and proposes a multi-layer resilience framework comprising governance, protection, detection and response, resilience, and assurance. The study also highlights national-level progress and initiatives undertaken between 2023 and 2025 to strengthen cybersecurity capacity, monitoring, and institutional readiness.

Keywords: *Cybersecurity Risks, Cybersecurity Challenges, Cyber Resilience, ICT Security, Digital Infrastructure Protection*

Disclaimer: The views expressed in the paper are those of the authors and do not in any way represent the views of the organisation where they are presently working.

I. Introduction

Digital transformation has become a central pillar of modern governance and institutional development. In India, the expansion of digital infrastructure across sectors has enabled improved accessibility, efficiency, and scalability.

By 2025, internet connectivity in India exceeded 100 crore users, accompanied by substantial growth in digital service adoption (PIB 2025). The digital economy is projected to contribute approximately 20% of GDP by 2026 (MeitY 2025). However, this rapid digital expansion also amplifies exposure to cyber threats, making resilient security mechanisms essential.

Recognising the need for secure digital ecosystems, the Government of India has implemented various cybersecurity initiatives via CERT-In, including operational guidelines, audit frameworks, and incident response mechanisms (CERT-In 2022; CERT-In 2023a).

Between 2023 and 2025, notable progress was observed in monitoring systems, audit capacity, and cybersecurity awareness.

II. Literature Review

Cybersecurity research has evolved from technical safeguards to integrated governance and resilience-based approaches. Early research focused on firewalls and encryption, while modern studies emphasize governance frameworks, adaptive resilience strategies, layered defence, continuous monitoring, and adaptive response mechanisms.

Frameworks such as:

- **NIST Cybersecurity Framework (CSF 2.0) –** Structured risk-based approach including Govern, Identify, Protect, Detect, Respond, Recover.
- **Zero Trust Architecture (ZTA) –** Principle of "never trust, always verify," focusing on identity authentication, least-privileged access, and cloud-centric security.

Recent studies define cyber resilience as the capacity to anticipate, withstand, recover, and adapt to cyber incidents (ENISA 2024; IBM Security 2025). In India, institutional reports highlight progress in governance, monitoring, and capacity building (CERT-In 2024; CERT-In 2025a).

III. Cybersecurity Risk Landscape

Cybersecurity risks are multi-dimensional and influenced by increasing system complexity and interconnectivity.

3.1 Data and Privacy Considerations

The growth of digital platforms has increased the volume and sensitivity of data, including personal, financial, and institutional information. Protecting such data is crucial for maintaining trust and ensuring secure operations. In 2023, a major financial data breach affected over 2 lakh customers, highlighting the need for robust encryption and access controls (CERT-In 2023a).

Data breaches can lead to financial loss and reputational impact. Global studies show that breach costs continue to rise due to increasing data volumes and system complexity (IBM Security 2025). In India, cybersecurity guidelines have strengthened practices such as encryption, access control, and secure data handling (CERT-In 2023a).

3.2 Service Continuity Considerations

Service continuity is vital in digitally dependent environments, especially for essential services. Disruptions can affect operational efficiency and accessibility.

Global assessments indicate increasing cyber incidents targeting critical infrastructure (ENISA 2024). Organisations are adopting business continuity and disaster recovery strategies, supported by institutional mechanisms that enhance service restoration (CERT-In 2024).

3.3 System Integrity Considerations

System integrity ensures that data and systems remain accurate and reliable. Ensuring system integrity is essential for effective operations.

Security measures such as access control, validation mechanisms, and configuration management support system integrity. National guidelines emphasise these controls to ensure reliable system functioning (CERT-In 2023a).

3.4 Infrastructure and Network Considerations

Modern digital environments are supported by complex ICT infrastructures, including on-premises systems, cloud platforms, data centres, and interconnected networks. While these architectures enhance scalability and efficiency, they also increase the complexity of securing digital systems.

Cyber incident trends in India reflect this expanding infrastructure landscape:

Table 1: Cyber Incident Trends in India (CERT-In 2024, 2025a)

Year	Incidents	Year-on-Year Growth (%)	Cumulative Growth (%)
2023	1,592,917	-	28
2024	2,041,360	28 %	85
2025	2,944,000+	44%	-

Source: CERT-In 2024, 2025a

As shown in Table 1, cyber incidents in India rose by 85% cumulatively from 2023 to 2025. This increase reflects both improved detection/reporting capabilities and rapid growth in ICT infrastructure, including additional endpoints, cloud services, and interconnected networks. The escalating incident trend demonstrates that as digital adoption grows, the attack surface widens, making continuous monitoring, endpoint protection, and network segmentation increasingly critical.

Key risks include misconfigured systems, unpatched software, insecure network interfaces, and limited segmentation between critical and non-critical systems. Vulnerabilities in one system can propagate to dependent systems, especially in interconnected environments. Cloud and hybrid architectures introduce additional considerations, including shared responsibility models and access configuration challenges.

Technical measures—such as network segmentation, secure configuration, endpoint protection, and real-time monitoring—help mitigate these risks and maintain operational stability. Strengthening infrastructure security is therefore fundamental to overall cybersecurity resilience and justifies the need for a multi-layer resilience framework.

3.5 Supply Chain Considerations

Reliance on third-party systems introduces additional cybersecurity risks. Risks may arise from external vendors and service providers.

Global studies highlight supply chain security as a key priority (ENISA 2024). Policy frameworks support improved oversight of third-party systems (CERT-In 2025a).

3.6 Cyber Financial Security Trends

The expansion of digital financial systems has been accompanied by increased reporting of cyber-related financial incidents. This reflects higher transaction volumes, improved reporting mechanisms, and growing user awareness.

Table 2: Cybercrime Complaints Related to Financial Frauds in India (PIB 2025)

Year	Number of complaints related to financial frauds on NCRP	YoY Growth (%)	Amount Reported (₹ In Crore)	YoY Growth (%)
2021	2,62,846	-	551	-
2022	6,94,446	164	2290	315
2023	13,10,357	89	7465	226
2024	19,18,835	46	22848	206
2025	24,02,579	25	22495	-1.5

Source: PIB 2025

The sharp rise in complaints—from 13 lakh in 2023 to over 24 lakh in 2025—reflects increased public reporting as well as growing cyber threats targeting financial systems. Despite this rise, approximately ₹8,189 crore has been safeguarded through preventive measures (PIB 2025), demonstrating the effectiveness of monitoring systems, institutional coordination, and awareness campaigns in mitigating financial cyber risks.

Common threats include phishing, identity theft, and unauthorised transactions, often originating from both technical vulnerabilities and user-related factors. These trends highlight the importance of integrating financial cybersecurity into organisational resilience frameworks, emphasizing real-time detection, incident response, and recovery mechanisms.

IV. Cybersecurity Implementation Considerations

Cybersecurity implementation involves translating policies and technical guidelines into operational practices. While national frameworks provide direction, effective implementation depends on institutional capacity, coordination, and consistent execution.

CERT-In has issued:

- 1,530+ alerts
- 390 vulnerability notes
- 65 advisories

(PIB 2025)

Over 230 empanelled audit organisations support compliance and assessments (CERT-In 2025a).

As shown in Table 1, Cyber incidents highlight implementation relevance:

In practice, implementation challenges relate to consistency, coordination, and integration. Security controls must be embedded into routine processes such as updates, access management, and incident reporting.

Building capacity through targeted training and clearly defined responsibilities enhances implementation effectiveness. Continuous monitoring, audits, and feedback mechanisms support ongoing improvement.

Cybersecurity implementation is therefore an ongoing governance and operational process, requiring alignment between policy, practice, and organisational capability.

V. A Multi-Layer Resilience Framework

The proposed framework integrates governance, protection, detection and response, resilience, and assurance layers (CERT-In 2023a; CERT-In 2025a).

Figure 1: Multi-Layer Cybersecurity Resilience Framework

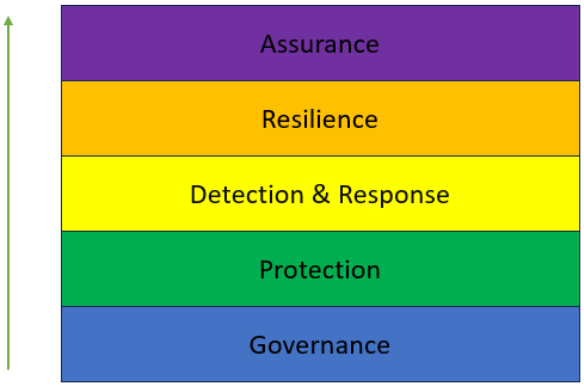

Figure 1

Figure 1: Multi-layer cybersecurity resilience framework showing governance, protection, detection & response, resilience, and assurance layers with continuous feedback loops.

Framework Explanation

- **Governance Layer:** Establishes cybersecurity policies, roles, responsibilities, and accountability structures. It aligns cybersecurity objectives with organisational goals and supports risk management and compliance (CERT-In 2023a).

- **Protection Layer:** Implements preventive controls such as access management, encryption, and secure configurations to reduce vulnerabilities.

- **Detection & Response Layer:** Enables monitoring, anomaly detection, and incident response through logging and SOC operations, ensuring timely mitigation (CERT-In 2022).

- **Resilience Layer:** Ensures continuity through backup systems, disaster recovery planning, and alternate workflows, supported by regular testing.

- **Assurance Layer:** Supports continuous improvement through audits, vulnerability assessments, and compliance reviews (CERT-In 2025a).

VI. Key Findings

- Increased cyber incident reporting reflects both expanded digital adoption and improved detection capabilities, particularly across critical ICT infrastructure (CERT-In 2024; CERT-In 2025a).
- The rise in financial cybercrime complaints underscores growing public awareness and reporting, while preventive measures demonstrate the effectiveness of institutional monitoring frameworks (PIB 2025).
- National frameworks, guidelines, and response systems contribute to structured cybersecurity management, supporting timely mitigation and recovery (CERT-In 2023a; PIB 2025).
- Effective cybersecurity requires integration of governance, technology, operational processes, and human factors, linking incident trends directly to preparedness needs.
- The AIIMS case exemplifies how disruptions in critical institutional systems can compromise service continuity; when viewed alongside national trends, it underscores the urgent need for multi-layer resilience frameworks (Lok Sabha 2022).
- A multi-layered approach strengthens overall cybersecurity preparedness, adaptability, and response capability, demonstrating the practical value of linking data trends to operational frameworks.

VII. Conclusion

The expansion of digital systems has increased the importance of cybersecurity across sectors. Between 2023 and 2025, frameworks, monitoring, and institutional capacity have strengthened. The proposed multi-layer resilience framework offers a structured, practical, and scalable approach for managing cybersecurity risks and enhancing preparedness.

References

[1]. CERT-In (2022). Directions relating to information security practices. Government of India.
[2]. CERT-In (2023a). Guidelines on information security practices for government entities. Government of India.
[3]. CERT-In (2024). Annual report 2023. Government of India.
[4]. CERT-In (2025a). Annual report 2024. Government of India.
[5]. ENISA (2024). Threat landscape 2024. European Union Agency for Cybersecurity.
[6]. Gandhi, P., and Pahwa, S. (2022). "AIIMS cyberattack study." IMIB Journal, 15(2), 45–58.
[7]. IBM Security (2025). Cost of a data breach report 2025. IBM Corporation.
[8]. IBM (n.d.). Ransomware-as-a-service (RaaS).
[9]. Lok Sabha (2022). Cyber-attack in AIIMS. Government of India.
[10]. MeitY (2025). Digital economy report. Government of India.
[11]. PIB (2025). Year-end review: Telecommunications and cybersecurity. Government of India.
[12]. The Economic Times (2023). "AIIMS breach and network segmentation."