

Evaluation of the IT Act, Data Protection Bill, CERT-in Guidelines, and their Effectiveness in Addressing New-Age Cyber Threats

Dr. Purkha Ram*

Assistant Sub Inspector, Border Security Force.

*Corresponding Author: huddapr123@gmail.com

Citation: Ram, P. (2026). Evaluation of the IT Act, Data Protection Bill, CERT-in Guidelines, and their Effectiveness in Addressing New-Age Cyber Threats. International Journal of Global Research Innovations & Technology, 04(03), 225–234. <https://doi.org/10.62823/ijgrit/04.03.9563>

ABSTRACT

The explosive growth of digital technologies in India has made the country extensively dependent upon cyberspace for communication, trade, governance, and the operation of critical infrastructure. While this has propelled economic growth and digital inclusion, it has also made people, organizations, and the state vulnerable to an extensive range of cyber threats from ransomware and phishing to AI-generated deepfake scams, vulnerabilities in IoT, and cross-border cyberattacks. Comprehensive legal and regulatory regimes backed by effective enforcement tools are needed to counter such threats. In this research, the three significant pillars of India's cybersecurity governance are assessed: the Information Technology (IT) Act, the developing Data Protection Bill, and guidelines provided by the Indian Computer Emergency Response Team (CERT-In). The IT Act, 2000, and subsequent amendments formed the cornerstone of India's cyber law regime, mainly aimed at electronic transactions, digital signatures, and cybercrime. Nevertheless, there are gaps in addressing new-age threats and the complexities of jurisdiction relating to such trans-boundary crimes. The Data Protection Bill that is set to be legislated is expected to ensure data protection, promote accountability among data fiduciaries, and safeguard individual privacy. Nonetheless, the bill faces opposition due to extensive exemptions available to government bodies and the challenge of balancing innovation and regulation. CERT-In guidelines provide technical guidance, reporting requirements for any cyber security threats, and coordinate the national response in case of a cyber disaster. There are nevertheless issues pertaining to enforcement, compliance, and institutional capability. This paper through the analysis of the merits, demerits, and complementarities of these measures has revealed some of the progress and gaps in the Indian cyber security framework. It is clear that whereas much has been achieved, future cyber threats require a more flexible, dynamic, and globalized approach. Recommendations have been made to ensure legal provisions are updated with emerging technologies, enhancing the institutional capabilities of CERT-In, and finding the right balance in the Data Protection Bill.

Keywords: IT Act, Data Protection Bill, CERT-In, Cyber-Attacks, Cybersecurity Policy, Data Privacy, Cross-Border Cybercrime, Ransomware, AI-Facilitated Cybercrime, National Security.

Introduction

India's economy and governance have been digitalizing at a pace that has never been seen before, opening up unprecedented opportunities for growth, inclusion, and efficiency. With efforts like Digital India, e-governance portals, fintech, and deep internet penetration, the world of cyberspace is now an integral part of national development. But the same ecosystem has at the same time also generated mounting cyber threats. India has also seen an increase in ransomware attacks, financial scams, identity thefts, phishing, and cross-border intrusions into critical infrastructure. The sophistication and global scale of such threats require effective and dynamic cybersecurity law.¹

¹ Singh, A. (2025). *The Evolution of India's Cyber Law: A Legislative Analysis of the Information Technology Act, 2000 and its Amendments*. DME Journal of Law, 6(01), 17–26. <https://doi.org/10.53361/dmejl.v6i01.03> dmejournals.com

Three frameworks are particularly prominent in India's cybersecurity governance: the Information Technology (IT) Act, 2000, the proposed Data Protection Bill, and guidelines issued by the Indian Computer Emergency Response Team (CERT-In).¹ The IT Act, which was enacted more than two decades ago, was the nation's first all-encompassing cyber law, dealing with electronic records, digital signatures, and cybercrime. Although its 2008 amendments introduced provisions for cyber terrorism, data protection, and punishment for cybercrime, the law is said to be outdated in dealing with current-day challenges such as AI-facilitated fraud, ransomware-as-a-service, and crypto-based crime.

The Data Protection Bill, which is being debated in its new version, aims to bridge gaps in protection of personal data by putting more robust accountability measures on data fiduciaries, making obligations of data processing, and strengthening user privacy rights. The implementation of such legislation can change the digital scenario of India completely; however, there are certain apprehensions regarding the possibility of governmental overreach, regulatory ambiguity, and the right balance between innovation and cost of compliance.

CERT-In acts as the nodal agency for cyber incident management in India. The guidelines issued by CERT-In provide for mandatory reporting of cyber incidents, information sharing, and advisories to the government as well as private sectors. Despite the crucial role played by CERT-In in handling the issue of cyber crisis, its effectiveness is generally hampered due to the constraints of capability, compliance, and lack of international cooperation.

This research thoroughly evaluates these three legal regimes in the context of their ability to address modern cyber threats.

Background of Cybersecurity Legislation in India

The Indian cyber laws have their foundation on the enactment of the Information Technology Act, 2000, which is based on UNCITRAL Model Law on Electronic Commerce. The IT Act was passed to provide for legal validity for the transaction done electronically and the use of digital signatures. However, later as there were fast-growing incidences of cybercrimes and increased reliance on digital media, there was a need to introduce further changes. The amendment in 2008 introduced substantial features including the legalization of electronic contracts, punishment for cyber terrorism, and duties of intermediaries for safeguarding the information of the users.

Despite these advancements, the IT Act was seen as reactive rather than proactive in nature. As newer technologies including cloud computing, artificial intelligence, and blockchain technology emerged, the IT Act failed to match the threat level. Moreover, issues related to jurisdiction in cross-border crimes and enforcement became an issue of deterrence.

In order to deal with the problem of inadequate data security and privacy policies, the Indian government proposed Personal Data Protection Bill (2019), which was later updated to Digital Personal Data Protection Bill 2022, and recently renamed to the Digital Personal Data Protection Act, 2023. It aims to regulate the storing, collecting and processing of personal data through providing people with the right to access, rectify, or erase their data. However, some fears were expressed about the fact that the state institutions may get blanket exemptions from it.³

At the same time, the government expanded its organizational structure by establishing CERT-In under the IT Act. This agency deals with incident response, issuing advisories, and national readiness in cybersecurity issues. In 2022, its new guidelines established a six-hour deadline to report cyber incidents by the organizations, which is another step towards responsibility and promptness in solving them. Unfortunately, this process has limitations because many organizations cannot comply with these guidelines due to insufficient technological skills.⁴

The cybersecurity legislation of India has evolved significantly over the past two decades from enabling e-commerce to cyber governance and securing data. Nonetheless, rapid advancements in technology and rising levels of cyber threats necessitate flexible and coordinated international laws to address these challenges. In view of this, it is pertinent to assess the adequacy and effectiveness of IT Act, Data Protection Bill, and CERT-In guidelines in the present scenario.²

¹ "A Critical Study on Legal Framework of Cyber Law in India." (2025). *International Journal for Multidisciplinary Research (IJFMR)*. <https://www.ijfmr.com/papers/2025/2/41779.pdf> IJFMR

² "Comprehensive Analysis of Data Protection Laws in India." (2024). *IJRAR*. <https://ijrar.org/papers/IJRAR24A2484.pdf> IJRAR

Reason behind Assessing Legal and Regulatory Mechanisms

Cybersecurity in today's world can no longer be associated with just technology; it is a part of national security, economy, as well as human rights. Being one of the fastest-growing digital economies, India remains vulnerable to cyber-attacks due to gaps in current legal framework and regulatory mechanism. There is a number of reasons why it is important to conduct an analysis of the existing framework.

First of all, the IT Act is about two decades old and thus formulated in a completely different technological environment. Even though there are amendments, the Act cannot cover all the risks and dangers connected with cyber-attacks, including artificial intelligence-based attacks, ransomware-as-a-service, cryptocurrency frauds and digital espionage. Not being able to update itself frequently, it will soon lose relevance in protecting the national interests.

Second, the Data Protection Bill means a revolutionary change in India's digital privacy and personal data regulation strategy. Analyzing it for both flaws and strengths is essential to understand whether it not only ensures the citizens' rights, but also promotes innovations and helps India reach its goal of becoming a global digital hub. Fears about exemptions for state surveillance and burden on small businesses should be taken into account closely.

Thirdly, CERT-In guidelines are the practical backbone of India's cyber security strategy. As effective as they might be in improving accountability and response capabilities, enforcement of the guidelines has been inconsistent. Evaluation of the efficacy of these guidelines will help recognize the areas of non-compliance, capability issues and international collaboration.⁴

Fourthly, the rapidly evolving cyber threat environment involving ransomware, vulnerabilities of Internet of Things and disinformation based on deepfakes needs future-oriented frameworks rather than reactive measures. The evaluation of the existing framework will assist policymakers, industry and civil society in identifying weaknesses and recommending revisions.

Thus, this evaluation is not only an academic exercise but a strategic necessity in making sure that the Indian legal and regulatory regime is resilient and flexible.⁵

Objectives

- Analyzing the principal provisions of the IT Act, Data Protection Bill, and CERT-In guidelines.
- Assessing their efficiency in countering new-age cyber threats.
- Identifying areas of overlap, complementarity, and legislative gaps among the given frameworks.
- Evaluating the perception of stakeholders on implementation and enforcement.
- Comparing India's frameworks with international best practices.
- Suggesting recommendations for India's cyber governance regime strengthening.

Study Scope and Limitations

Scope

- Maintains focus on three major frameworks namely; IT Act, Data Protection Bill and guidelines provided by CERT-In.
- Includes dangers such as ransomware, phishing, artificial intelligence-based offenses, Internet of Things (IoT) vulnerabilities, and cross-border threats.
- Legal, institutional, as well as policy viewpoints, are incorporated in analysis.
- Utilizes case studies of recent cyberattacks to assess effectiveness.¹

Limitations

- The study excludes in-depth technical analysis of cyberattack mechanisms.
- Restricted to publicly available data, reports, and case studies.
- Regional and sectoral differences may not be fully covered.
- Fast-paced nature of the evolving cyber threats can restrict long-term relevance of results.

¹ "India's Legislative Framework for Data Protection in the Digital Era." (2024). *IJFMR*. <https://www.ijfmr.com/papers/2024/1/11933.pdf> [IJFMR](#)

Overview of India's Cybersecurity Framework

India's framework for cybersecurity is built on three key aspects that include legal aspect, IT Act, 2000, draft personal data protection law, Data Protection Bill/DPDP Act, 2023, and institutional guidelines, CERT-In. However, all these attempts to regulate cybercrimes, protect personal data, and readiness against cybercrimes have been challenged due to ransomware, artificial intelligence fraud, and cross-border cybercrimes.

- **Evolution of Cyber Laws in India**
 - 2000: IT Act enacted to legalize e-commerce as well as digital signatures.
 - 2008 Amendment: Inserted cyber terrorism, intermediary liability, as well as data protection provisions.
 - 2019-2023: Data Protection Bill proposals evolved into the Digital Personal Data Protection Act, 2023.
 - Strengthening of Institutions: Introduction of CERT-In through the IT Act for managing cybersecurity threats.
 - This step reflects a gradual move from transactional security towards privacy and data protection.
- **Role of IT Act, Data Protection Bill, and CERT-In in Cybersecurity Ecosystem**
 - IT Act: Gives the legal framework to prosecute cybercrime and control intermediaries.
 - Data Protection Bill/DPDP Act: Enforces personal data regulation, user consent, and responsibility.
 - CERT-In: National incident response agency, issuing guidelines and advisories.
 - All three together constitute a complementary framework counterbalancing crime control, privacy, and technical preparedness.
- **International Comparisons (brief contextualization)**
 - GDPR (EU): Robust on privacy, individual rights, and cross-border restrictions of data flow.
 - US Framework: Sectoral legislation with focus on private sector innovation.
 - India: Hybrid model—hitting a balance of security, state interests, and user privacy, but weaker in terms of enforcement than the EU.

The Information Technology (IT) Act, 2000 and Amendments

Objectives and Scope

- To validate electronic contracts and signatures.
- To control cybercrime, digital transactions, and intermediary accountability.
- Key Provisions Relating to Cybercrime and Data Security
- Hacking, data theft, identity theft, and cyber terrorism sections.
- Rules for reasonable security practices and intermediary liability.

Strengths of the IT Act

- First holistic legal framework for cyberspace in India.
- Prescribes penalties and legal support for cyber offences.
- Dynamic enough for several amendments.

Limitation

- Stale with regard to AI-based fraud, ransomware-as-a-service, crypto-crimes.
- Weak international cooperation provisions.
- Ambiguities in enforcing intermediary liability.

The Data Protection Bill (latest version/DPDP Act, 2023)

• Background and Evolution

Drafts since 2017 are transformed into Personal Data Protection Bill, 2019, subsequently amended to Digital Personal Data Protection Act, 2023.

Principal Provisions

- Consent-based data processing.
- Regulations for data storage, cross-border flow.
- Rights of users (access, correction, erasure).
- Penalties for breach.

Impact

- Individuals: Greater control over personal data, privacy protection.
- Businesses: Cost of compliance, data storage regulations, liability issues
- National Security: Increased state power to access data under exemptions

Strengths

- Sets robust data governance standards
- Introduces accountability of data fiduciaries.
- Gets closer to GDPR-level protection

Weaknesses

- Widespread government exemptions weaken privacy protections.
- Uncertainty over regulation and enforcement power.
- Potential for small business and startup compliance burden.

Review of Literature

Pawar, O. P. (2019). Cyber Crime and Cyber Security with regard to Indian Cyber Laws. Finds persistent gaps in enforcement and awareness under the IT Act in spite of increase in capacity of policing; identifies jurisdictional challenges and evidentiary issues.

Deshmukh, Y. B. (2019). Critical Analysis of Cyber Crime in India. Traces offence trends and contends the IT Act & IPC continue to wrestle with rapidly evolving crimes (phishing, identity theft, darknet).

Pujari, A., & Singh, M. (2021). Critical Assessment of the Information Technology Act, 2000. Identifies loopholes after 2008 amendments and demands greater clarity and capability building on intermediary liability.

Ajmeri R. Ansari, A. (2023). IT Act, 2000 & Informational Privacy. Interprets privacy protections using Puttaswamy; criticizes weak security measures and surveillance exceptions under current IT regulations.

Lata, D., & RajVardhan, R. (2025). Analytical Study of Cyber Law & Legal Framework in India. Synthesizes case law + policy; calls for modernization to tackle ransomware, cross-border data access, and DPDP alignment.

Dalei, P. (2025). The Digital Personal Data Protection Act, 2023: Legal Analysis. Compares DPDP to GDPR; faults sweeping government exemptions and enforcement design.¹

Dey, S., & Kumar, A. (2025). Comprehensive Analysis of the DPDP Act, 2023. Describes rights/obligations, cross-border transfer model, and burden of compliance; mentions accountability through the DP Board.

IndusLaw (Indian authorship) (2022). Unwinding CERT-In Directions (2022). Practitioner analysis of 70B directions—log retention, 6-hour incident reporting—highlighting compliance frictions for VPN/hosting providers.

MeitY (Govt. of India) groups including Indian researchers (2023). Ransomware Attack: An Emerging Targeted Malware. Indian insights on attack trends and response actions; informs sectoral readiness in comparison to CERT-In setup.

IJLMH authors (2023). Cybercrime & Legal Implications: Challenges & Evidence. Highlights digital-evidence admissibility and jurisdictional snag points; suggests MLAT streamlining.²

¹ "Cyber Laws in India: Issues and Challenges." (2025). *IJLR*. <https://ijlr.iledu.in/wp-content/uploads/2025/04/V5I734.pdf> *IJLR*

² "Legal Aspects of Cyber Security in India with special reference to Data Protection." (2022). *IJISAR*. <https://ijisar.com/wp-content/uploads/2022/06/Simran-Agarwal.pdf> *IJISAR*

Koushik, G., & Saxena, J. (2025). Law of Cybercrime Legislation & Global Cooperation in India. Surveys India's cooperation stance (INTERPOL, MoUs), and non-accession to Budapest; recommends diplomacy + capacity enhancements

IJLMH authors (2021). A Study on Cyber Crime and its Legal Framework in India. Examines IT Act + IPC interaction; flags training gaps in cyber cells and public-private collaboration requirements.

LawJournals authors (2023/2024). Comparative Examination of Cybersecurity/Data-privacy Laws (GDPR v. India/DPDP). Describes divergences in cross-border transfers and consent, to guide DPDP rule-making.¹

International Journal of Law (2023). Comparative review of cyber security laws of India, US & UK. Observes ransomware explosion and policy initiatives; highlights necessity to review IT Act for contemporary threats.

IJOSS authors (2025). Cyber Jurisprudence in India—Comparative Analysis. Highlights India's cyber regime gaps against global best practices; advocates harmonization with international cooperation instruments.

IJRAR (2024). Cyber Terrorism in India. Compiles recent threat-intel (state-sponsored attacks spike) and reveals implications for national security and CERT-In incident taxonomy.

IJRAR (2025). Cyber Crime in India: Legal Provisions, Enforcement, and Judicial Trends. Canvasses prosecutions/jurisprudence; advocates more transparent cross-border evidence pipelines.

IOSR Journal (2023). Digital Defenders or Deficient? India's Cybercrime Legal Landscape. Criticizes conviction rates and promotes better investigation standards + international cooperation.²

Research Methodology

• Research Design

The research is descriptive and analytical in nature. It adopts both qualitative (literature review, expert views) and quantitative (responses to the survey) approaches to analyze the IT Act, the Data Protection Bill (DPDP Act, 2023), and CERT-In guidelines.

• Sample Size and Sampling Technique

- Sample Size: 100 participants
- 30 cyber law professionals and legal experts
- 30 IT and cybersecurity experts
- 20 policymakers/administrators
- 20 postgraduate law and technology students

Sampling Technique: Purposive sampling, including respondents who are directly involved in cyber governance or policy discourse.

• Data Collection Methods

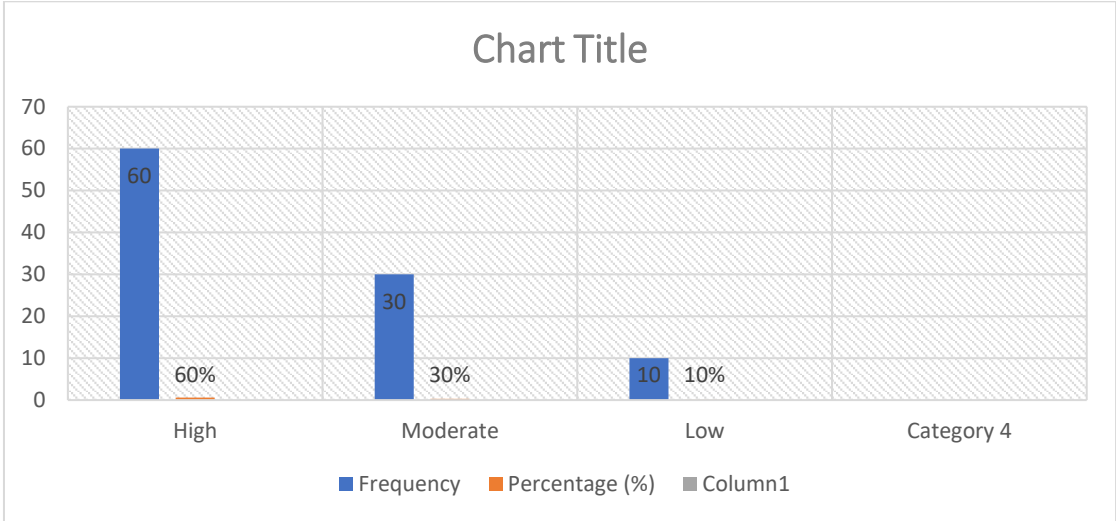
- **Primary Data:** Questionnaire survey (Likert scale + close-ended questions).
- **Secondary Data:** Government reports (CERT-In, NCRB), journal articles, and policy briefs.

Data Analysis

Table 1: Awareness of Cybersecurity Frameworks

Awareness Level	Frequency	Percentage (%)
High	60	60%
Moderate	30	30%
Low	10	10%

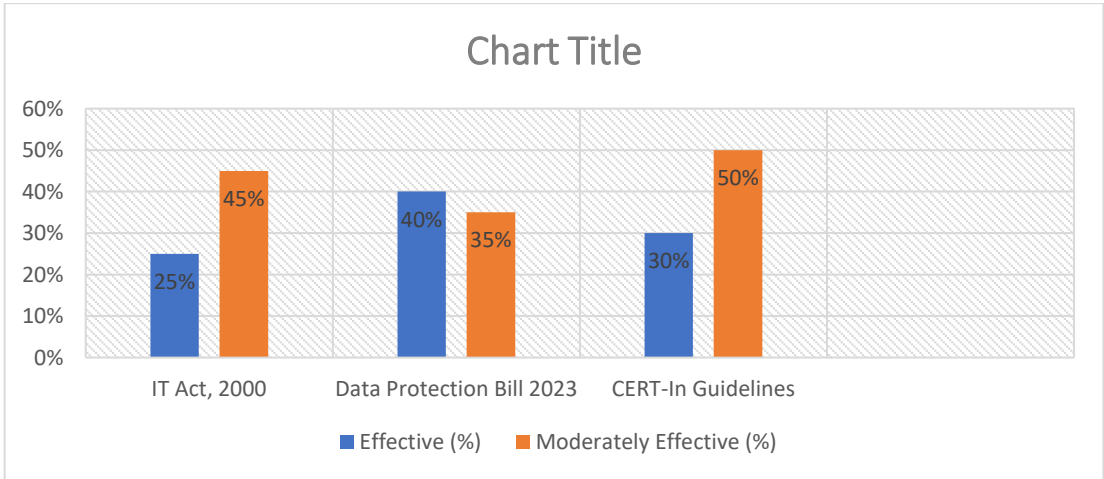
¹"Indian Cyber Act: Lacunae and Recommendations." (n.d.). IJLMH. <https://ijlmh.com/paper/indian-cyber-act-lacunae-and-recommendations/IJLMH>



Interpretation: Most respondents (60%) are highly aware of IT Act, Data Protection Bill, and CERT-In, showing good professional awareness, though a small segment still lacks clarity.

Table 2: Perceived Effectiveness of IT Act, Data Protection Bill, and CERT-In

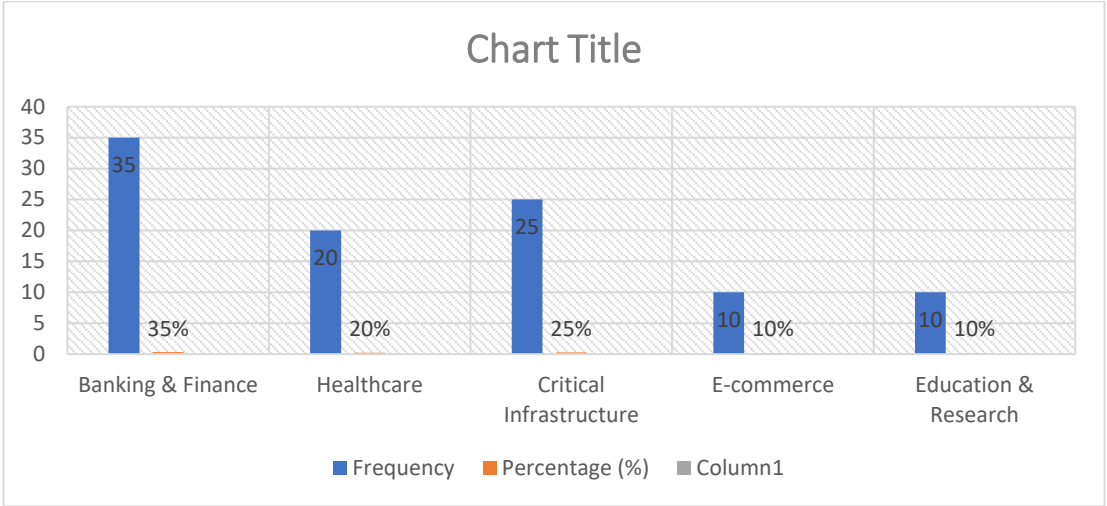
Framework	Effective (%)	Moderately Effective (%)	Ineffective (%)
IT Act, 2000	25%	45%	30%
Data Protection Bill 2023	40%	35%	25%
CERT-In Guidelines	30%	50%	20%



Interpretation: The Data Protection Bill is perceived as relatively more effective (40% support), while IT Act is considered outdated by many respondents.

Table 3: Sectors Most Vulnerable to Cyber Threats

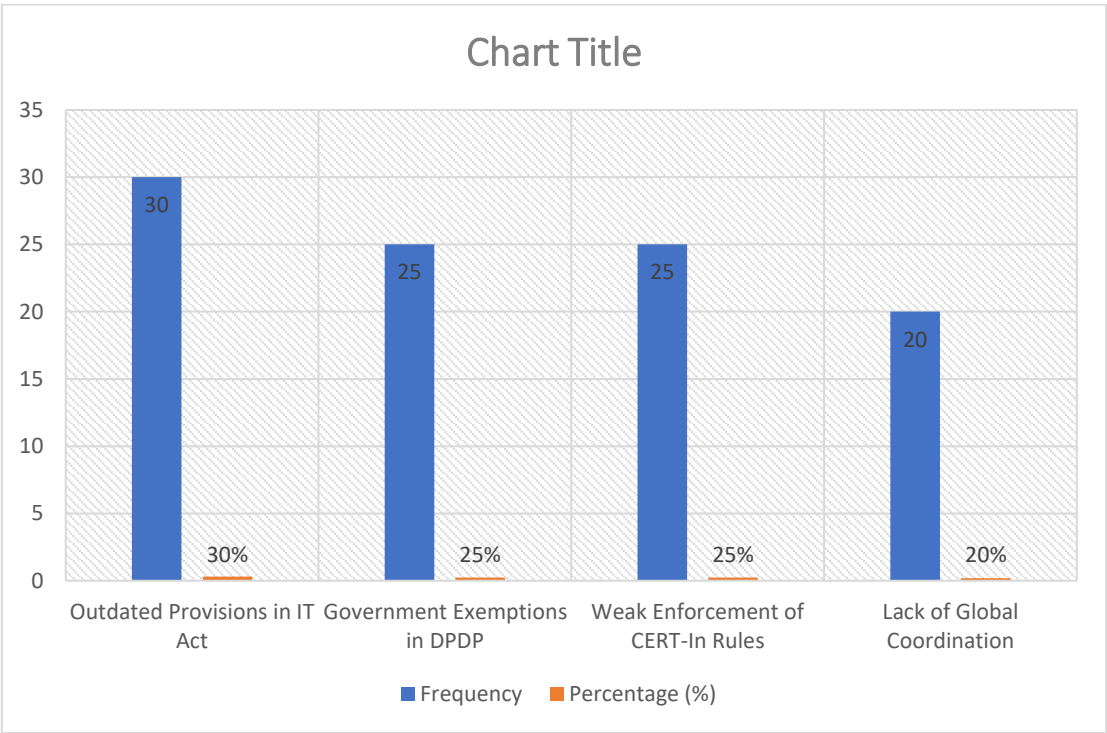
Sector	Frequency	Percentage (%)
Banking & Finance	35	35%
Healthcare	20	20%
Critical Infrastructure	25	25%
E-Commerce	10	10%
Education & Research	10	10%



Interpretation: Banking & Finance (35%) and Critical Infrastructure (25%) are seen as most exposed, consistent with global cyberattack trends.

Table 4: Key Challenges in Current Frameworks

Challenge	Frequency	Percentage (%)
Outdated Provisions in IT Act	30	30%
Government Exemptions in DPDP	25	25%
Weak Enforcement of CERT-In Rules	25	25%
Lack of Global Coordination	20	20%



Interpretation: Outdated IT Act provisions are seen as the biggest challenge, followed by gaps in enforcement and global cooperation.

Discussion

Through this research, one gets to know the merits and demerits in India's legal framework on cybersecurity. The high level of awareness indicates that the policymakers and professionals have knowledge of the IT Act, the Data Protection Bill, and CERT-In. However, the respondents are not satisfied by the effectiveness of these laws.

The IT Act is a groundbreaking legislation and it is considered to be out of touch with current technological trends due to its age and incapability in dealing with AI-related cyber-crimes, ransomware and other borderless crimes. Lack of intermediary liability and uncertainties about new technologies are the gaps identified most by the participants. On the other hand, the Data Protection Bill (DPDP Act, 2023) received more positive perceptions, particularly on user consent and accountability. However, there is concern with respect to extensive government exemptions in the bill which would dilute its privacy aspect.

Guidelines of CERT-In have been commended for timely reporting and technical advice, however, lack of enforcement and compliance issues hinder its effective functioning. Several respondents noted that it is difficult for small companies to adhere to CERT-In's guidelines of reporting within six hours.

According to the sectoral assessment, banking and finance, healthcare and critical infrastructure emerge as the most vulnerable sectors. This is in line with the global trends, where financial fraud, ransomware attacks on hospitals and intrusion at the grid level are common. According to the respondents, without proper legal framework, India can be subjected to serious economic and national security risks.

The above discussion brings to the fore the need for reforms, whereby Indian cyber laws can be brought at par with global standards.

Conclusion

As seen from the current research, the existing cyber infrastructure in India, however complex and detailed on paper, should be greatly modernized to be able to address the next generation of cyber-attacks efficiently. IT Act, 2000, being groundbreaking for India, cannot cope with the rapid evolution of technology and cybercrime in general. DPDP Act, 2023 is an innovative attempt to regulate the use of personal data but it lacks practical results because of the extensive number of exemptions. CERT-In guidelines have contributed greatly to the increase of incident reporting and coordination but weak enforcement reduces their efficiency.

It appears that the respondents value the existing guidelines highly but at the same time are not satisfied with them and emphasize their weaknesses. The respondents pointed out that Indian cyber laws have to be flexible, technologically advanced and unified globally.

This research further establishes that finance, health care, and critical infrastructures are the most susceptible areas; thus, it is essential for policy makers to give high priority to these fields in cyber security policies. Challenges faced by India in cyber governance include outdated legal framework, poor implementation, inadequate international cooperation, and governmental intervention in data management.

On the whole, this research study establishes the fact that Indian cyber governance has to move from a reactive approach to a proactive one.

Suggestions

- Alter the IT Act to include criminal activities involving AI, ransomware attacks, and misuse of cryptocurrency.
- Limit exceptions provided by the Government within the Data Protection Bill to ensure better privacy protection.
- Equip CERT-In with more power and flexibility for small enterprises in adhering to compliance norms.
- Establish cyber courts to handle cybercrimes within a short span of time.
- Further improve international cooperation through treaties and models of data sharing across countries.
- Conduct cybersecurity audit in vital infrastructure industries.
- Conduct public awareness campaigns on digital security in local languages.
- Carry out R&D activities of indigenous cybersecurity technologies to reduce dependency on imported technologies.

References

1. Singh, A. (2025). *The Evolution of India's Cyber Law: A Legislative Analysis of the Information Technology Act, 2000 and its Amendments*. DME Journal of Law, 6(01), 17–26. <https://doi.org/10.53361/dmejlv6i01.03> dmejournals.com
2. "A Critical Study on Legal Framework of Cyber Law in India." (2025). *International Journal for Multidisciplinary Research (IJFMR)*. <https://www.ijfmr.com/papers/2025/2/41779.pdf> [IJFMR](https://www.ijfmr.com)
3. "An analytical study on challenges and gaps in India's cyber security." (2024). *Criminal Law Journal*. <https://www.criminallawjournal.org/article/110/5-1-3-412.pdf> [Criminal Law Journal](https://www.criminallawjournal.org)
4. "An Analytical Study of Cyber Law & Legal Framework in India." (2025). *IJRMPS*. <https://www.ijrmips.org/papers/2025/2/232693.pdf> [IJRMPS](https://www.ijrmips.org)
5. "Digital Personal Data Protection Act, 2023: A Legal Analysis." (2025). *Law Journals*. <https://www.lawjournals.org/assets/archives/2025/vol11issue3/11064.pdf> [Law Journals](https://www.lawjournals.org)
6. "Comprehensive Analysis of Data Protection Laws in India." (2024). *IJRAR*. <https://ijrar.org/papers/IJRAR24A2484.pdf> [IJRAR](https://ijrar.org)
7. "Cybersecurity and Data Protection Laws: A Comparative Study of India and Global Perspectives." Yadav, M., & Sharma, J. (2022). *International Journal of Innovations & Research Analysis (IJIRA)*. <https://www.inspirajournals.com/issue/downloadfile/2/Volumne-Pages/Zev16rxgYBnd3YIWE5pL> [INSPIRA](https://www.inspirajournals.com)
8. "Cyber security landscape in India: Exploring Cybercrimes and Legal Responses." (2024). *IJRAR*. <https://ijrar.org/papers/IJRAR24B2474.pdf> [IJRAR](https://ijrar.org)
9. "India's Legislative Framework for Data Protection in the Digital Era." (2024). *IJFMR*. <https://www.ijfmr.com/papers/2024/1/11933.pdf> [IJFMR](https://www.ijfmr.com)
10. "Cyber Laws in India: Issues and Challenges." (2025). *IJLR*. <https://ijlr.iledu.in/wp-content/uploads/2025/04/V5I734.pdf> [IJLR](https://ijlr.iledu.in)
11. "Legal Aspects of Cyber Security in India with special reference to Data Protection." (2022). *IJISAR*. <https://ijisar.com/wp-content/uploads/2022/06/Simran-Agarwal.pdf> [IJISAR](https://ijisar.com)
12. "Indian Cyber Act: Lacunae and Recommendations." (n.d.). *IJLMH*. <https://ijlmh.com/paper/indian-cyber-act-lacunae-and-recommendations/> [IJLMH](https://ijlmh.com)
13. "Cyber Law in India: Evolution & Current Limitations." (n.d.). *IJRPR*. <https://ijrpr.com/uploads/V6ISSUE6/IJRPR49262.pdf> [IJRPR](https://ijrpr.com)

