The Indian Cybersecurity Landscape

Introduction

India's digital landscape is undergoing a profound transformation, characterized by rapid digital expansion and widespread adoption of technology across diverse sectors. This accelerated digitalization has significantly enhanced connectivity, yet it has concurrently broadened the attack surface, leading to an increased susceptibility to cyber threats. The current environment is marked by an unprecedented volume and sophistication of cyber threats targeting both organizations and individuals. This dynamic interplay between digital growth and escalating cyber risks means that as India continues its digital journey, the complexity and volume of cyber threats will inevitably rise, necessitating continuous adaptation of cybersecurity strategies.

This report aims to provide a foundational understanding of the Indian cybersecurity landscape for an intern. It will focus on key cyber threat patterns, outline the relevant regulatory framework specifically for Small and Medium-sized Enterprises (SMEs), detail essential general security requirements, explain incident response protocols, and identify the types of data crucial for training Artificial Intelligence (AI) models in cybersecurity.

I. Understanding India's Cyber Threat Landscape

The cyber threat landscape in India has reached a critical juncture, characterized by a significant surge in both the volume and sophistication of attacks. In 2024, India experienced a fourfold increase in cyber fraud, resulting in estimated losses of approximately $20 million. This surge positioned India as the second most targeted nation globally in terms of cyberattacks in 2024, with 95 Indian entities falling victim to data theft incidents.

Current Threat Patterns and Trends

The sheer scale of malicious activity is evident in the detection statistics. A total of 369.01 million distinct malware detections were recorded across 8.44 million endpoints nationwide. A substantial majority of these threats, 85.44%, were identified through traditional signature-based methods, which indicates a persistent vulnerability to established attack vectors. However, a notable 14.56% of detections occurred via behavior-based methods, underscoring the emergence of innovative and previously unidentified threat methodologies. This divergence in detection methods highlights a critical shift in the cybersecurity paradigm. The continued reliance on signature-based detection for a large portion of threats, while still necessary for known vulnerabilities, is increasingly challenged by the growing percentage of threats requiring behavior-based detection. This trend, coupled with the explicit rise of AI-generated threats, signals an escalating competition in cybersecurity. Traditional defenses, which rely on recognizing known patterns, are becoming increasingly insufficient against threats crafted by artificial intelligence. This pushes organizations towards more advanced, AI-powered behavioral analytics for effective threat detection, as AI itself becomes a crucial tool for defense, capable of learning and adapting to identify previously unknown malicious activities.

Predominant threat vectors include Trojans, accounting for 43.38% of all detections, and Infectors, which represent 34.23%. This indicates a strategic shift by attackers from opportunistic attacks to more targeted and sophisticated campaigns, leveraging these advanced malware types.

Ransomware attacks emerged as the most significant threat in India in 2024, impacting numerous sectors, with 108 known incidents recorded. The Lockbit group was particularly active, responsible for over 20 incidents in the country. Phishing attacks also remained a major concern, especially within sectors handling financial transactions and personal data. Cybercriminals employed deceptive emails, fake websites, and social media impersonations to steal sensitive information.

Emerging threats pose new challenges. Digital arrest scams, where cybercriminals impersonate law enforcement officials to extort money, were notably prevalent in urban centers such as Delhi, Bengaluru, and Mumbai. The advent of deepfake and AI-driven attacks represents a particularly concerning development. Cybercriminals are now leveraging AI to automate and scale their attacks, making detection significantly harder, and are using deepfake technology to impersonate trusted individuals like CEOs or government officials to carry out fraud. A striking example of this trend is that by April 2025, 51% of spam emails were generated by AI, surpassing human-written spam. These AI-generated emails often exhibit greater formality, fewer grammatical mistakes, and higher linguistic sophistication, which can help them evade detection and appear more credible to recipients.

Key Threat Vectors and Targeted Sectors

The primary threat vectors observed in India involve Trojans (43.38% of detections) and Infectors (34.23%). These malware types are central to the strategic shift towards more targeted and sophisticated campaigns by cyber attackers.

The sectors most severely affected by cyberattacks include Banking, Financial Services, and Insurance (BFSI), Healthcare, and Hospitality. These industries are consistently targeted because they manage vast amounts of sensitive financial and personal information, making them high-value targets for cybercriminals. In 2024, the finance and banking sectors recorded the highest number of victims, with 20 entities affected, followed by the government sector with 13 victims, telecommunications with 12, and the healthcare/pharma and education sectors with 10 and 9 victims, respectively. The consistent targeting of BFSI and Healthcare sectors highlights not only the immense value of data within these industries but also their critical interconnectedness. A breach in one entity within these sectors can have cascading effects across the broader economy and public trust. Attacks on these critical sectors can lead to severe disruptions to business operations, impacting national security, the economy, public health, or safety. This interconnectedness means that a successful attack on one entity, such as a bank, can have widespread consequences, affecting customers, suppliers, and other dependent services, thereby posing a systemic risk. This necessitates a strategic imperative for India to not only protect individual entities but also to build resilience across the entire critical information infrastructure to prevent widespread economic and social disruption.

Mobile Security Threats

Mobile security threats constitute a significant portion of the overall cyber landscape. Malware accounts for 42% of mobile threats, followed by Potentially Unwanted Programs (PUPs) at 32%, and Adware at 26%. The high prevalence of adware points directly to the monetization of mobile-based cyber threats. Android devices, in particular, are highly vulnerable, underscoring the urgent need for robust mobile security measures.

Geographic Distribution of Threats

Cyber threats are not uniformly distributed across India. The regions experiencing disproportionately high volumes of malware activity are Telangana, Tamil Nadu, and Delhi. This concentration may be attributed to higher levels of digital adoption and connectivity in these areas. Furthermore, emerging threats like digital arrest scams have been particularly prevalent in major urban centers such as Delhi, Bengaluru, and Mumbai.

Table 1: Key Cyber Threat Statistics and Trends in India

Category	Metric	Value	Source
Overall Threat Volume	Total Malware Detections (across 8.44M endpoints)	369.01 million	
Detection Methods	Signature-Based Detection	85.44%	
	Behavior-Based Detection	14.56%	
Predominant Malware Types	Trojans	43.38% of detections	
	Infectors	34.23% of detections	
	Ransomware Incidents (known)	108 incidents	
Cyber Fraud	Increase in Cyber Fraud (2024)	Fourfold increase	
	Losses from Cyber Fraud (2024)	~$20 million	
Global Ranking	India's Ranking (2024)	2nd most targeted nation	
	Indian Entities Attacked (2024)	95 entities	
Emerging Threats	AI-generated Spam (by April 2025)	51% of spam emails	
Most Affected Sectors	Top 3 Sectors	BFSI, Healthcare, Hospitality	
	Finance & Banking Victims (2024)	20 entities	
	Government Victims (2024)	13 entities	
Top Targeted Regions	Regions with high malware activity	Telangana, Tamil Nadu, Delhi	
	Regions with prevalent Digital Arrest Scams	Delhi, Bengaluru, Mumbai	
Mobile Threats	Mobile Malware	42%	

Category	Metric	Value	Source
	Potentially Unwanted Programs (PUPs)	32%	
	Adware	26%	

This table provides a concise overview of the most critical cyber threat statistics and trends in India, offering a quick reference for the scale and nature of the challenges. It helps in grasping the most impacted areas and types of attacks, which is crucial for understanding the overall cybersecurity posture.

II. Navigating India's Cybersecurity Regulatory Framework for SMEs

India has established a multi-layered legal and regulatory framework to address cybersecurity, with key legislation and guidelines impacting Small and Medium-sized Enterprises (SMEs).

A. The Information Technology Act, 2000 (with 2008 Amendments)

The Information Technology Act, 2000 (IT Act), represented India's foundational step towards establishing a comprehensive legal framework for the digital age. Its initial purpose was to grant legal recognition to electronic transactions and facilitate e-commerce, while also defining and addressing cybercrime. Recognizing the evolving nature of cyber threats, the Information Technology (Amendment) Act, 2008, introduced significant changes. These amendments strengthened provisions related to cybercrimes, privacy issues, and e-commerce, implementing stricter penalties and establishing clearer regulations for intermediaries. The 2008 amendment also placed a strong emphasis on data privacy and information security, formally defined terms like "cyber-café," made digital signatures technology-neutral, and redefined the roles of intermediaries and the Indian Computer Emergency Response Team (CERT-In).

Section 43A: Data Protection and Reasonable Security Practices

Section 43A of the IT Act is a cornerstone for data protection, particularly relevant to businesses handling sensitive information. It mandates that any body corporate that possesses, deals with, or handles "sensitive personal data or information" must implement and maintain "reasonable security practices and procedures". Failure to adhere to these practices, resulting in wrongful loss to any person or wrongful gain to another, renders the entity liable to pay compensation to the affected individual.

The term "sensitive personal data or information" is specifically defined to include categories such as an individual's username/passwords, financial information (e.g., bank account, credit/debit card details), health conditions, biometric information, and sexual orientation. The rules enacted under Section 43A further distinguish between "Personal information" (any information identifying a natural person) and "Sensitive personal data or information" as a specific sub-category.

Before collecting sensitive personal data, organizations must provide the information provider with an option to opt out or withdraw their consent at any time. Disclosure of sensitive personal data to any third party requires prior permission from the provider. Furthermore, body corporates are required to designate a Grievance Officer and prominently publish their name and contact

details on their website.
A critical change introduced by the 2008 Amendment was the removal of the ceiling limit for compensation under Section 43A. Previously, Section 43 had a compensation limit of one crore rupees, but for Section 43A, no such limit is prescribed, meaning the potential liability is uncapped. This removal of the compensation ceiling for data breaches signifies a strong regulatory intent to hold entities, including SMEs, fully accountable for data protection. For SMEs, this means that a single data breach, regardless of the company's size, could lead to compensation demands that far exceed their financial capacity, potentially posing an existential threat. This transforms data security from a mere compliance checkbox into a critical business risk, compelling SMEs to prioritize robust security practices even with limited resources.

Sections 66, 66C, 66D: Cybercrimes and Penalties

The IT Act penalizes various cybercrimes, providing a legal framework to deter and punish malicious online activities.

- **Section 66 (Hacking):** This section addresses the act of dishonestly or fraudulently accessing a computer resource without the owner's permission. It also covers actions that destroy, delete, alter, diminish the value or utility of, or injuriously affect information residing in a computer resource with the intent to cause wrongful loss or damage. Hacking is punishable with imprisonment for a term that may extend to three years, or a fine up to two lakh rupees, or both. The 2008 amendment notably introduced the element of *mens rea* (criminal intent) for an offense under this section, clarifying the requirement for malicious intent.
- **Section 66C (Identity Theft):** This provision targets individuals who fraudulently or dishonestly make use of another person's electronic signature, password, or any other unique identification feature. The penalty for identity theft includes imprisonment for up to three years and/or a fine that may extend to one lakh rupees.
- **Section 66D (Cheating by Personation):** This section addresses cheating by impersonation using a communication device or computer resource. Offenders can face imprisonment for up to three years and/or a fine up to one lakh rupees.

Other relevant sections introduced or strengthened by the 2008 Amendments include Section 66A, which dealt with offensive messages online but was later quashed by the Supreme Court in 2015 for infringing free speech. Section 66B penalizes receiving stolen computer resources, Section 66E addresses the violation of privacy by capturing or transmitting images of private areas without consent, and Section 66F deals with cyber terrorism, which carries a severe penalty of imprisonment for life.
For SMEs, understanding these sections is crucial not only for protecting themselves as potential victims but also for ensuring that their own operations and employee conduct do not inadvertently lead to legal violations. While the penalties for these cybercrimes might appear lower than the uncapped liability under Section 43A, they still represent significant legal and financial risks, including potential imprisonment for individuals involved.

Section 69: Government Powers for Interception and Decryption

Section 69 of the IT Act grants significant powers to the Central or State Government, or their specially authorized officers, to direct any agency to intercept, monitor, or decrypt any information transmitted through any computer resource. These powers can be invoked in the interest of India's sovereignty or integrity, defense, security of the State, friendly relations with foreign states, public order, or for preventing incitement to the commission of any cognizable offense.

A critical aspect of this section is the obligation it places on individuals and entities. Subscribers, intermediaries, or any person in charge of a computer resource are mandated to provide all necessary facilities and technical assistance, including access to the computer resource and the decryption of information, when called upon by the authorized agency. Failure to provide such assistance is a serious offense, punishable with imprisonment for a term that may extend to seven years and a fine. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, outline the specific procedures and safeguards for such actions, requiring written orders, review within seven days, and limiting the validity of directions to 60 days (renewable up to 180 days).

The broad powers for government interception and decryption under Section 69, coupled with severe penalties for non-compliance, highlight a potential tension between national security interests and user privacy or business operational autonomy. For SMEs, particularly those acting as service providers or hosting data, this means they must be technically prepared to comply with government requests for data interception or decryption. This readiness involves having the technical capability to provide such access and understanding the legal obligations to avoid severe penalties. The stringent nature of this provision implies that SMEs need to not only ensure technical readiness but also establish clear internal policies on how to handle such requests, potentially requiring legal counsel to navigate the complexities and ensure compliance while safeguarding business interests.

Sections 70, 70A, 70B: Critical Information Infrastructure and CERT-In's Role

These sections focus on the protection of critical digital assets and the role of the national cybersecurity agency.

- **Section 70 (Protected System):** This section empowers the government to declare specific computer systems as "Protected Systems" to safeguard Critical Information Infrastructure (CII). CII is defined as computer resources whose incapacitation or destruction would have a debilitating impact on national security, the economy, public health, or safety. Unauthorized access to such protected systems, or even attempts to gain access, is a serious offense, punishable with imprisonment for up to ten years and a fine.
- **Section 70A (Nodal Agency for CII Protection):** This mandates the establishment of a national nodal agency dedicated to protecting CII. The National Critical Information Infrastructure Protection Centre (NCIIPC) has been officially notified as this agency. NCIIPC is responsible for developing and enforcing a robust framework for CII protection, including launching research and development initiatives to enhance infrastructure resilience.
- **Section 70B (CERT-In's Role):** This section formally designates the Indian Computer Emergency Response Team (CERT-In) as the national cybersecurity incident response agency. CERT-In's responsibilities include collecting, analyzing, and disseminating information on cyber incidents, issuing forecasts and alerts regarding potential cybersecurity threats, and coordinating emergency actions to counter cyberattacks. Significantly, CERT-In is empowered to call for information and issue directions to a wide range of entities, including service providers, intermediaries, data centers, body corporates, and any other person.

While direct designation as Critical Information Infrastructure might be less common for smaller

SMEs, those providing services to or handling data for critical sectors (such as BFSI, Healthcare, or Government) could indirectly fall under the broader ambit of CII protection requirements or be directly subject to CERT-In's directions, especially concerning incident reporting and data retention.

Section 79: Intermediary Safe Harbour Provisions

Section 79 is pivotal for entities operating as intermediaries in the digital space, providing a "safe harbour" from liability for third-party content. This provision applies to a wide range of entities, including social media platforms, search engines, hosting providers, and telecom service providers.

However, this immunity is conditional. For the safe harbour to apply, the intermediary's function must be limited to providing access to a communication system, and they must not initiate, select, or modify the transmission of the information. Crucially, intermediaries must observe "due diligence" while discharging their duties. This includes expeditiously removing or disabling access to unlawful content upon receiving actual knowledge or a notification from the appropriate government or its agency. Failure to abide by the broader Intermediary Guidelines can lead to the withdrawal of this safe harbour protection, rendering the intermediary liable for punishment under any applicable law, including the IT Act.

The conditional "safe harbour" under Section 79 creates a significant compliance burden for SMEs that act as intermediaries. The requirement for "due diligence" and "expeditious removal" of unlawful content effectively shifts a portion of content moderation responsibility onto these entities. This necessitates that SMEs invest in monitoring and response capabilities that might strain their limited resources. For a small business, establishing robust content moderation, grievance redressal, and rapid takedown mechanisms, which can include automated filtering for significant intermediaries, requires significant investment in technology, personnel, and legal expertise. This can lead to SMEs struggling to comply, facing penalties, or even over-removing content (over-censorship) to avoid liability, potentially impacting user expression. This regulatory approach, while aiming to control online content, implicitly privatizes a significant portion of content policing, creating a complex legal and technical landscape where failure to comply can lead to severe repercussions, potentially stifling innovation or participation in the digital economy for smaller players.

B. Intermediary Guidelines & Digital Media Ethics Code Rules, 2021 (Updated 2023)

These rules, updated in 2023, elaborate on the due diligence requirements for intermediaries under Sections 79 and 87 of the IT Act. They apply broadly to social media platforms, hosting providers, and digital publishers.

Due Diligence Obligations for Intermediaries

Intermediaries are mandated to prominently publish their rules, privacy policy, and user agreement on their website or mobile application. They must also inform users about various categories of prohibited content, including obscene material, content harmful to children, information infringing intellectual property rights, misinformation, impersonation, and content threatening national security.

A key obligation is the mandatory removal or disabling of access to unlawful information within 36 hours of receiving a court order or notification from the appropriate government agency. For content specifically related to nudity, sexual acts, or impersonation, the rules stipulate even faster action, requiring resolution within 72 hours. When information is removed, the intermediary must preserve it and associated records for 180 days for investigation purposes, or longer if required by authorities. Similarly, user registration information must be retained for 180 days after cancellation of their registration.

Intermediaries are also required to take all reasonable measures to secure their computer resources and the information contained therein. They must provide information or assistance to lawfully authorized government agencies for investigative, protective, or cybersecurity activities within 72 hours, with a stricter 24-hour window for online gaming intermediaries enabling permissible online real money games. Furthermore, mandatory reporting of cybersecurity incidents and sharing related information with CERT-In is a crucial obligation.

For "Significant Social Media Intermediaries" (SSMIs), defined as those with over 50 lakh (5 million) registered users in India , additional stringent obligations apply. These include appointing a Chief Compliance Officer, a Nodal Contact Person for 24x7 coordination with law enforcement, and a Resident Grievance Officer, all of whom must be residents in India. SSMIs are also required to publish monthly compliance reports detailing complaints received and actions taken. They must also endeavor to adopt technology-based measures, including automated tools, to proactively identify certain unlawful content like child sexual abuse material. Messaging services that qualify as SSMIs are further obligated to enable the identification of the "first originator" of information for specific legal purposes, though they are not required to disclose message content.

Grievance Redressal Mechanism

The rules establish a comprehensive grievance redressal mechanism to ensure user complaints are addressed efficiently. Intermediaries must appoint a Grievance Officer and prominently publish their contact details. This officer is responsible for acknowledging complaints within 24 hours and resolving them within 15 days.

A three-tier grievance redressal structure is outlined: Level I involves self-regulation by the intermediary, Level II involves self-regulatory bodies of publishers, and Level III is an oversight mechanism under the Ministry of Information & Broadcasting. Additionally, the Central Government is empowered to establish one or more Grievance Appellate Committees to hear appeals from users who are dissatisfied with a Grievance Officer's decision or whose grievance remains unresolved within the stipulated timeframe.

Impact on SMEs as Intermediaries

SMEs operating as intermediaries must strictly adhere to these due diligence obligations. This includes implementing content takedown procedures, ensuring data preservation, and establishing a functional Grievance Officer role. While the more stringent requirements for SSMIs, such as proactive filtering and first originator identification, may not directly apply to smaller SMEs, the general obligations still represent a significant compliance burden. The emphasis on rapid content takedown (within 36-72 hours) and the requirement for a dedicated Grievance Officer place a heavy operational and financial burden on SMEs acting as intermediaries. This can disproportionately affect smaller platforms that may lack the resources for 24/7 monitoring, legal review, and the technical infrastructure needed to comply swiftly and effectively. Such pressures could lead to over-censorship to avoid liability or create significant barriers to entry for new, smaller intermediaries due to the high compliance costs involved.

C. CERT-In Directions, 2022 (Section 70B Compliance)

Issued under Section 70B(6) of the IT Act, the CERT-In Directions of 2022 are designed to significantly strengthen India's overall cybersecurity posture. These directions are broadly applicable to service providers, intermediaries, data centers, body corporates, and government organizations. Non-compliance with these directives can result in penalties, including fines and imprisonment.

Mandatory Incident Reporting

One of the most critical provisions is the mandatory reporting of all specified cyber incidents to CERT-In within **6 hours** of noticing such incidents or being brought to notice. The list of incidents requiring mandatory reporting is extensive, covering categories such as Distributed Denial of Service (DDoS) attacks, ransomware, phishing, data breaches, unauthorized access, fake mobile applications, and attacks on critical infrastructure. Reports can be submitted via email (incident@cert-in.org.in), helpdesk, or fax. The report content must be comprehensive, including the time of occurrence, information regarding affected systems/networks, observed symptoms, and relevant technical details such as deployed security systems and mitigation actions taken. This reporting obligation is mandatory and overrides any confidentiality agreements under contract.

Log Retention Requirements

Organizations are mandated to enable and securely maintain logs of all their Information and Communication Technology (ICT) systems within India for a rolling period of **180 days**. These logs are considered crucial for forensic analysis and must be provided to CERT-In upon request, whether for incident reporting or other directives. Beyond general ICT logs, specific entities such as Data Centers, Cloud Service Providers, Virtual Private Network (VPN) providers, and Virtual Private Server (VPS) providers are required to maintain validated names of subscribers/customers and Know Your Customer (KYC) records for a period of 5 years after service cancellation. Similarly, virtual asset service providers, virtual asset exchange providers, and custodian wallet providers must retain KYC details and records of financial transactions for 5 years, ensuring that individual transactions can be reconstructed with identifying elements like IP addresses, timestamps, and transaction details.

Time Synchronization Mandates

To ensure accurate incident reporting and facilitate forensic analysis, the CERT-In Directions mandate that organizations synchronize the clocks of all their ICT systems. This synchronization must be done with the Network Time Protocol (NTP) Server of the National Informatics Centre (NIC) or the National Physical Laboratory (NPL), or with NTP servers that are traceable to these national sources. For entities with operations spanning multiple geographies, the use of alternative NTP servers is permitted, provided their time source does not deviate from that of NPL or NIC. This consistency in timestamps is vital for accurately investigating cybersecurity incidents.

Applicability and Compliance Extensions for SMEs

The CERT-In Directions apply to "body corporates," which explicitly includes SMEs. Recognizing the challenges faced by smaller entities, the initial 60-day compliance deadline (June 28, 2022) was extended to September 25, 2022, specifically for Micro, Small & Medium Enterprises (MSMEs). This extension was granted to provide SMEs with additional time to "build capacity" required for implementing the cybersecurity measures , acknowledging the resource constraints many SMEs face.

Penalties for Non-Compliance

Non-compliance with the CERT-In Directions is punishable with imprisonment for up to 1 year and/or a fine up to ₹1 lakh. Furthermore, other penal provisions under the IT Act, such as the confiscation of underlying computer or computer systems, may also apply. If an offense is committed by a company, every person who, at the time of the contravention, was responsible for the conduct of its business (e.g., directors, managers) can also be held liable.

A significant development is the proposed Jan Vishwas (Amendment of Provisions) Bill, 2023, which aims to increase the fine amount under Section 70B(7) of the IT Act to a maximum of ₹1 crore. While this proposed amendment has not yet taken effect, it signals a clear intent to significantly raise the financial risk associated with non-compliance with CERT-In Directions.

The CERT-In Directions, particularly the stringent 6-hour reporting window and the 180-day log retention requirement, impose a significant operational and technical burden on SMEs. The initial compliance deadline extension for SMEs, coupled with the proposed tenfold increase in penalties, highlights a regulatory recognition of SME challenges while simultaneously increasing the stakes for non-compliance. This regulatory approach strongly encourages SMEs to make proactive investments in cybersecurity infrastructure and processes, as "building capacity" is no longer optional but a necessary cost of doing business in India's digital economy. This pushes SMEs to integrate cybersecurity into their core operations and budget planning to avoid severe legal and financial repercussions.

Table 2: Summary of Key Regulatory Requirements and Penalties for SMEs

Regulation/Guideline	Key Requirement for SMEs	Specific Implication for SMEs	Penalties for Non-Compliance	Source
IT Act, 2000 (with 2008 Amendments)				
Section 43A (Data Protection)	Implement "reasonable security practices" for Sensitive Personal Data/Information	Uncapped compensation liability for data breaches can pose an existential threat.	Uncapped compensation to affected persons.	

Regulation/Guideline	Key Requirement for SMEs	Specific Implication for SMEs	Penalties for Non-Compliance	Source
	(SPDI); appoint Grievance Officer; obtain consent for SPDI collection.			
Sections 66, 66C, 66D (Cybercrimes)	Avoid hacking, identity theft, cheating by personation; ensure internal policies prevent employee misconduct.	Significant legal and financial risks, including imprisonment for individuals.	Imprisonment up to 3 years, fines up to ₹2 lakh (Sect 66) or ₹1 lakh (Sect 66C/66D).	
Section 69 (Govt. Interception)	Provide technical assistance and access for interception/decryption upon lawful order.	Requires technical capability and clear internal policies to avoid severe penalties.	Imprisonment up to 7 years and a fine for failure to assist.	
Section 79 (Intermediary Safe Harbour)	Observe "due diligence" for third-party content; expeditiously remove unlawful content upon knowledge/notification.	Conditional immunity; significant compliance burden requiring monitoring and response capabilities.	Loss of safe harbour protection, leading to liability under relevant laws.	
Intermediary Guidelines & Digital Media Ethics Code Rules, 2021				
Due Diligence Obligations	Publish rules/policies; inform users of prohibited content; remove unlawful content within 36/72 hours; preserve data for 180 days; report incidents to CERT-In.	Heavy operational and financial burden, disproportionately affecting smaller platforms.	Loss of safe harbour (Section 79) and liability under IT Act/other laws.	
Grievance Redressal	Appoint Grievance Officer;	Requires dedicated	Loss of safe harbour (Section	

Regulation/Guideline	Key Requirement for SMEs	Specific Implication for SMEs	Penalties for Non-Compliance	Source
	acknowledge complaints within 24 hours, resolve within 15 days.	personnel and efficient processes.	79).	
CERT-In Directions, 2022				
Mandatory Incident Reporting	Report specified cyber incidents to CERT-In within 6 hours of noticing.	Demands 24/7 monitoring capabilities and skilled personnel for rapid detection and reporting.	Imprisonment up to 1 year and/or fine up to ₹1 lakh (proposed to ₹1 crore).	
Log Retention	Maintain logs of all ICT systems securely in India for 180 days.	Requires robust logging infrastructure and secure storage.	Imprisonment up to 1 year and/or fine up to ₹1 lakh (proposed to ₹1 crore).	
Time Synchronization	Synchronize ICT system clocks with NIC/NPL NTP servers.	Ensures consistent timestamps for forensic analysis.	Imprisonment up to 1 year and/or fine up to ₹1 lakh (proposed to ₹1 crore).	

This table offers a consolidated view of the most critical regulatory requirements and their associated penalties under India's cybersecurity laws, specifically highlighting their relevance and impact on SMEs. This provides a clear reference point for understanding the complex web of regulations and the potential consequences of non-compliance.

III. Essential Security Requirements and Incident Response Protocols for SMEs

Beyond merely complying with legal mandates, establishing robust general security practices and a well-defined incident response protocol is fundamental for SMEs to effectively protect their digital assets and ensure business continuity.

General Security Best Practices

Foundational security practices are crucial for any organization, including SMEs, to build a strong defense against cyber threats:

- **Access Controls:** Implementing principles of least privilege and zero trust is paramount to protect AI systems and other digital assets from unauthorized access. This involves restricting user, API, and system access based strictly on necessity and continuously verifying all interactions. API monitoring is also essential to detect and limit unusual usage patterns that could indicate abuse.

- **Data Protections:** Given the reliance on data, ensuring data integrity is a top priority to prevent modifications that could bias or corrupt system outputs. It is advisable to separate sensitive data and avoid training AI models with highly confidential or personal information unless absolutely necessary. Protecting AI prompts is also critical, as unauthorized access could expose business intelligence and decision-making strategies.
- **Patch Management:** Regularly applying security patches and updates is vital to fix exploited vulnerabilities and prevent attackers from leveraging known weaknesses.
- **Employee Training:** A significant challenge in India is the low level of cybersecurity awareness. Therefore, continuous security awareness training for employees is a non-negotiable measure to equip them with the knowledge to identify and report potential threats.
- **Network Segmentation:** Strengthening network segmentation helps restrict the lateral movement of attackers within a network, limiting the impact of a breach.
- **Multi-Factor Authentication (MFA):** Enforcing MFA adds an essential layer of security by requiring multiple forms of verification before granting access, significantly reducing the risk of unauthorized access even if passwords are compromised.
- **Regular Audits and Vulnerability Scans:** Proactively identifying weaknesses through regular security audits and vulnerability scans can help organizations discover and address vulnerabilities before they are exploited by attackers.
- **Backup and Recovery:** Maintaining clean, isolated backups of critical data and systems is crucial for rapid restoration in the event of a ransomware attack or data corruption.

The Incident Response Lifecycle

A structured approach to incident response is crucial for minimizing damage, containing threats, and ensuring a swift recovery from cybersecurity incidents. The incident response lifecycle typically comprises six interconnected phases:

- **Phase 1: Preparation:** This foundational phase involves developing a comprehensive Incident Response Plan (IRP) that clearly defines response procedures, roles, responsibilities, and escalation paths. It also includes training employees on security awareness and conducting regular cybersecurity drills, such as tabletop exercises and simulated attacks, to test the team's readiness and identify gaps.
- **Phase 2: Identification:** The first step in an actual incident is to confirm that a security event is indeed an incident. This involves analyzing security alerts, logs (e.g., SIEM logs), network traffic, and threat intelligence to validate the threat. The team must determine the type, scope, and potential impact of the incident, promptly classifying it and documenting key details such as the date, time, affected systems, and any initial actions taken.
- **Phase 3: Containment:** Once an incident is identified, the immediate priority is to limit its scope and minimize damage. Short-term containment actions include isolating affected devices from the network, disabling compromised accounts, blocking malicious IPs and domains, and revoking access privileges. Long-term containment strategies involve applying patches and updates to prevent reinfection and strengthening network segmentation to restrict lateral movement of attackers.
- **Phase 4: Eradication:** This phase focuses on fully removing the attacker's presence from the environment. Key actions include scanning for and removing all traces of malicious code, backdoors, and persistence mechanisms. It also involves applying security patches to fix exploited security gaps, eliminating attack vectors (e.g., misconfigured cloud settings), and conducting thorough forensic analysis to determine the root cause of the

attack and eliminate residual risks.

- **Phase 5: Recovery:** The goal of recovery is to restore affected systems and operations to normal. This involves restoring systems from clean backups, gradually bringing systems back online to minimize disruptions, and continuously monitoring network traffic for any signs of lingering threats. Performing penetration testing after recovery helps confirm that security gaps are closed before resuming full operations.
- **Phase 6: Lessons Learned (Post-Incident Review):** This crucial final phase involves conducting a detailed post-mortem analysis of the incident. The team documents the attack timeline, response actions taken, and identifies what worked well and what needs improvement. This review helps identify gaps in detection, response, and communication. Based on these findings, security policies are updated, and additional training is provided for security teams and employees to address weaknesses exposed during the attack.

Practical Steps for SMEs in Incident Response (aligned with CERT-In)

For SMEs, aligning incident response with CERT-In's requirements is paramount to ensure compliance and effective mitigation.

- **Initial Assessment & Documentation:** Upon detecting a potential cybersecurity event, SMEs must promptly identify and classify the incident. This involves understanding its nature and scope, including potential impacts on data, systems, or services. Crucially, key details such as the date and time of the incident, affected systems, and any initial actions taken must be thoroughly documented. This documentation serves as a vital reference throughout the entire incident response process.
- **Contacting CERT-In:** Immediate contact with CERT-In is a mandatory step upon identifying a cybersecurity incident. Timeliness is critical, as incidents must be reported within **6 hours** of noticing or being brought to notice. SMEs should utilize the designated channels for reporting, which include email (incident@cert-in.org.in) and online reporting portals.
- **Information Required for Reporting:** When reporting, SMEs must provide a comprehensive description of the incident. This includes details on the attack vector (how the attack occurred), affected assets, potential vulnerabilities exploited, and a clear articulation of the impact on the confidentiality, integrity, and availability of data or critical services.
- **Follow-up Procedures:** Collaboration with CERT-In is ongoing throughout the incident response process. SMEs should follow CERT-In's guidance and be prepared to share additional information as requested to facilitate the resolution. Internally, a thorough post-incident analysis must be conducted. This involves documenting lessons learned, identifying areas for improvement, and updating incident response plans accordingly to enhance future preparedness.

Addressing SME Challenges in Cybersecurity

SMEs face unique challenges in establishing and maintaining robust cybersecurity postures, often due to inherent limitations:

- **Resource Constraints:** Many SMEs operate with limited financial, technical, and personnel resources, which restricts their ability to invest in sophisticated cybersecurity measures and comprehensive incident response capabilities.
- **Lack of Awareness:** Despite the increasing proliferation of digital tools and security

technology, cybersecurity awareness often remains low within SMEs, making them more susceptible to common attack vectors like phishing.

- **Complexity of Reporting:** The detailed and strict reporting requirements, such as the 6-hour incident reporting window mandated by CERT-In, can be overly complex and burdensome for SMEs that lack dedicated security teams.

The recurring theme of "resource constraints" and "lack of awareness" for SMEs creates a significant gap between regulatory expectations and practical implementation. This situation suggests a critical need for government-backed initiatives or industry-specific, simplified cybersecurity frameworks and affordable solutions tailored specifically for SMEs. Such support, beyond mere extensions and penalties, is essential to genuinely uplift their security posture.

Strategies to Overcome these Challenges:

- **Prioritization:** SMEs should focus on implementing foundational security practices that offer the highest return on investment in terms of risk reduction, securing critical assets first.
- **Leveraging Managed Security Service Providers (MSSPs):** Outsourcing security functions to specialized MSSPs can help SMEs overcome their resource limitations by providing access to expertise, technology, and 24/7 monitoring that they might not be able to afford in-house.
- **Automation:** Utilizing automated tools for tasks like log analysis, vulnerability scans, and routine security functions can free up limited human resources, allowing staff to focus on more strategic or complex security issues.
- **Cybersecurity Education & Training:** Continuously fostering a culture where transparency is valued and reporting incidents is seen as a responsible and necessary act is crucial. Regular and accessible cybersecurity education and training for all employees can significantly improve an SME's defensive capabilities.
- **Collaboration:** Forging strong partnerships between government agencies, private enterprises, and cybersecurity organizations can lead to enhanced coordination in incident response, streamlined information sharing, and collective efforts to strengthen national cybersecurity.
- **Simplified Frameworks:** Adapting existing, comprehensive cybersecurity frameworks like NIST (National Institute of Standards and Technology) or SANS (SysAdmin, Audit, Network, and Security) to a scale appropriate for SMEs can provide a structured yet manageable approach to security.

IV. Data for AI Model Training in Cybersecurity

Artificial Intelligence (AI) is rapidly transforming the field of cybersecurity, offering powerful capabilities to enhance defenses against evolving threats.

Role of AI in Enhancing Cybersecurity

AI cybersecurity represents a proactive approach that leverages artificial intelligence to eliminate security blind spots, preemptively predict and prevent attacks, and significantly improve the efficiency of security operations across an organization's entire digital estate. AI models, utilizing deep learning algorithms and neural networks, can monitor, assess, and analyze enormous volumes of data at speeds far exceeding human capabilities.

The benefits of integrating AI into cybersecurity are substantial:

- **Faster and More Accurate Threat Detection and Response:** AI models can sift through vast amounts of data in real-time to detect unusual patterns of activity, identify anomalies, and respond to the first signs of potential risks or attacks more quickly and accurately than traditional methods.
- **Automation of Routine Security Tasks:** AI agents can automate many mundane or high-volume tasks previously performed by human security personnel, such as log analyses, vulnerability scans, and threat correlation. This frees security teams to focus on more critical and strategic tasks.
- **Predictive and Proactive Defense:** By learning from past attacks and identifying patterns, AI technologies can predict and anticipate new threats, enabling organizations to take preemptive steps to reduce security risks and vulnerabilities before they can be exploited.
- **User Behavior Analytics (UBA):** AI can access and analyze historical user behavior data to identify patterns and detect any unusual activity, such as logins from unusual IP addresses or devices. This capability is instrumental in determining if a user account is at risk and preventing identity fraud.
- **Incident Triage and Prioritization:** AI can assess the severity of threats, prioritizing critical issues like ransomware attacks over less urgent phishing attempts. This ensures that security teams address high-risk incidents first, reducing response times and preventing escalation of damage.

The increasing sophistication of AI-driven attacks, where cybercriminals use AI to automate and scale their malicious activities, making them harder to detect, creates a compelling and almost self-fulfilling need for AI in cybersecurity defense. This dynamic suggests an escalating "AI vs. AI" cyber arms race, where the quality and diversity of training data for defensive AI models become paramount. The effectiveness of cybersecurity increasingly depends on the sophistication of its AI models, which in turn makes the quality, volume, and diversity of the data used to train these models a critical strategic asset. The future of cybersecurity will likely be defined by continuous innovation in AI-driven defenses, fueled by comprehensive and high-quality threat intelligence and training data, to counter the ever-evolving AI-powered offensive tactics.

Types of Data for AI Training

Effective AI models in cybersecurity require vast amounts of diverse data for training. Key categories include:

- **Malware Samples:** These are fundamental for training Machine Learning (ML) models for both static and dynamic analysis. By analyzing malware samples, AI can identify malicious behaviors, code patterns, and classify malware families. Datasets can include various malware categories such as ransomware, Trojans, coin miners, spyware, backdoors, and worms.
- **Network Traffic Logs:** Used extensively for anomaly detection, network traffic logs allow AI models to identify unusual patterns or activities that deviate from normal network behavior. AI models monitor, assess, and analyze huge volumes of network traffic data, including flow records, packets, and logs, to detect anomalies in real-time. This process involves cleaning, preprocessing, and extracting relevant features from data based on protocols like TCP/IP, HTTP, FTP, and DNS.
- **Incident Reports:** Aggregated incident reports can be invaluable for automating aspects of incident response. AI can analyze past attack data, identify recurring patterns, and

predict future threats. India's initiative to develop AI incident reporting guidelines for critical infrastructure aims to create a centralized database for AI-related issues, which could serve as a rich source of training data.

- **Phishing Email Datasets:** These datasets are used to train AI models to detect phishing attacks by identifying anomalies in email content, sender addresses, and suspicious links. The increasing prevalence of AI-generated spam, which exhibits greater formality and fewer grammatical errors, makes such datasets crucial for developing more sophisticated detection mechanisms.
- **System Logs & Executable Files:** AI collects and analyzes system logs and executable files for feature extraction and subsequent model training, enabling the identification of suspicious activities and potential threats.
- **User Behavior Data:** Historical user behavior data is analyzed by AI to establish baselines of normal activity. Deviations from these patterns can signal potential threats, helping to prevent identity fraud and unauthorized access.
- **Threat Intelligence:** AI enhances and supports cyber threat management by integrating with threat intelligence platforms. This allows AI to correlate attack data from various sources, identify emerging trends, and provide actionable insights for proactive security measures.

Sources of Indian Cybersecurity Datasets

Several sources provide publicly available Indian data that can be valuable for cybersecurity research and AI model training:

- **Data Security Council of India (DSCI):** Organizations like DSCI publish comprehensive reports, such as the "India Cyber Threat Report 2025." These reports leverage extensive telemetry data from millions of endpoints, offering valuable insights into malware detections, predominant threat vectors, and sectoral impacts within India. While raw data may not always be publicly accessible, the summarized findings and trends are highly informative.
- **Kaggle:** This platform hosts various datasets, including "Cybersecurity Cases India," which provides granular views of cybersecurity incidents in India. This dataset offers details on financial impact, geographic distribution, and different incident types, making it a valuable resource for trend analysis.
- **Open Government Data Portal India (data.gov.in):** This official portal provides year-wise and state/Union Territory-wise statistics on cybercrime cases reported on the National Cyber Crime Reporting Portal. This includes data on digital arrest scams, various cyber fraud cases, and cybersecurity incidents tracked by CERT-In, offering a broad overview of the national threat landscape.
- **Research Institutions:** Universities and research bodies globally, such as York University's BCCC, actively generate and release cybersecurity datasets for AI-powered model training. These datasets cover a wide range of areas, including encrypted traffic, large-scale malware analysis, DDoS attacks, and smart contract vulnerabilities. While not exclusively Indian, these contribute to the global pool of relevant data that can be applied to the Indian context.
- **Malware Repositories:** Large-scale datasets from malware repositories and collections of labeled samples are crucial for training robust ML models capable of detecting previously unseen malware strains.

Importance of Data Quality and AI Governance

The effectiveness of AI in cybersecurity is directly proportional to the quality of the data it is trained on. If the training data contains "noise" or "garbage," the AI's output and reliability will be compromised. This means that protecting the integrity of AI training data, and ensuring its representativeness and cleanliness, becomes a new frontier in cybersecurity. It is not just about collecting data, but actively defending against adversarial data poisoning or manipulation, which could turn defensive AI into a vulnerability. The growing reliance on AI for cybersecurity, coupled with the increasing prevalence of AI-generated threats, creates a critical dependency on the integrity and quality of AI training data. This implies that "data integrity" for AI models is not merely about preventing accidental corruption, but about actively defending against sophisticated adversarial data poisoning or manipulation attacks, which could effectively turn defensive AI systems into exploitable vulnerabilities.

Furthermore, AI systems themselves must be protected from various threats, including adversarial attacks, model poisoning or theft, and ensuring the data integrity of machine learning pipelines. It is imperative that AI tools are developed and utilized in full compliance with all applicable laws and company policies. Implementing robust AI Risk Management Frameworks, such as NIST's AI Risk Management Framework (RMF), and maintaining an AI Bill of Materials (AIBOM) are crucial steps for secure and ethical AI deployment. These measures help document AI supply chain dependencies and track model lifecycles for version control and risk assessment, ensuring transparency and accountability in AI-driven cybersecurity solutions.

Conclusion

India's journey of rapid digital transformation, while offering immense opportunities, has simultaneously created an expanding attack surface and an increasingly sophisticated cyber threat landscape. This report has highlighted the critical inflection point at which India's cybersecurity stands, marked by a significant volume of malware detections, a surge in cyber fraud, and its position as the second most targeted nation globally. The prevalence of traditional threats like Trojans and Infectors, alongside the alarming rise of AI-driven attacks and deepfakes, underscores a dynamic and evolving threat environment. The consistent targeting of critical sectors such as BFSI and Healthcare further emphasizes the systemic risks posed by cyber incidents, necessitating a holistic approach to national cybersecurity.

Navigating this landscape requires a robust understanding of India's regulatory framework. The Information Technology Act, 2000, with its 2008 amendments, lays the legal foundation, particularly Section 43A, which imposes uncapped compensation liability for data breaches, making data protection a critical business risk for SMEs. Sections related to cybercrimes (66, 66C, 66D) and government powers for interception (69) demand both legal awareness and technical readiness from SMEs. The conditional "safe harbour" under Section 79 and the comprehensive Intermediary Guidelines of 2021 impose significant due diligence, content moderation, and grievance redressal burdens on SMEs acting as intermediaries, potentially straining their limited resources. Furthermore, the CERT-In Directions of 2022, with their stringent 6-hour incident reporting window and 180-day log retention requirements, present a substantial operational and technical challenge for SMEs, despite compliance deadline extensions. The proposed increase in penalties for non-compliance signals a strong regulatory push towards greater accountability.

To overcome these challenges, SMEs must move beyond mere compliance. Implementing foundational security practices, such as strong access controls, robust data protections, regular patching, and comprehensive employee training, is paramount. A structured incident response lifecycle, from preparation and identification to containment, eradication, recovery, and lessons learned, is essential for minimizing damage and ensuring resilience. Addressing the inherent resource constraints and lack of awareness within the SME sector requires not only internal prioritization but also leveraging external support, such as Managed Security Service Providers (MSSPs), and advocating for simplified, tailored cybersecurity frameworks and government-backed initiatives.

Finally, Artificial Intelligence is rapidly becoming indispensable in cybersecurity defense, enabling faster threat detection, automation of tasks, and predictive analysis. However, the effectiveness of AI is entirely dependent on the quality and integrity of its training data. The increasing use of AI by adversaries to create sophisticated attacks necessitates a proactive defense against data poisoning and model manipulation, making AI governance and data integrity critical components of future cybersecurity strategies.

For aspiring cybersecurity professionals, these dynamics underscore a fundamental truth: the cyber threat landscape is in a state of perpetual evolution. New attack vectors, AI-driven threats, and regulatory shifts will continue to emerge. Therefore, continuous learning and adaptation are not merely advantageous but are absolute imperatives. Professionals must commit to staying abreast of technological advancements, understanding the intricate legal frameworks, and fostering collaborative efforts between government, industry, and academia to collectively strengthen national cybersecurity.

Works cited

1. India Cyber Threat Report 2025 | Data Security Council of India - DSCI, https://www.dsci.in/resource/content/india-cyber-threat-report-2025

2. Understanding India's Cyber Threat Landscape in 2025 | Security Quotient, https://securityquotient.io/understanding-indias-cyber-threat-landscape-in-2025

3. India second most targeted nation in terms of cyber attacks: CloudSEK, https://m.economictimes.com/tech/technology/india-second-most-targeted-nation-in-terms-of-cyber-attacks-cloudsek/articleshow/116890873.cms

4. Over half of spam emails now generated by AI, new study finds - SecurityBrief Australia, https://securitybrief.com.au/story/over-half-of-spam-emails-now-generated-by-ai-new-study-finds
5. Section 70 Of The IT Act, 2000: All About Critical Infrastructure Protection - ApniLaw, https://www.apnilaw.com/acts/section-70-of-the-it-act-2000-all-about-infrastructure-protection/

6. Government Taking Measures to Strengthen National Preparedness Against Cybersecurity Threats - PIB, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2115416

7. Cyber Law and Data Privacy in the 21 st Century: Emerging Legal Issues and Challenges, https://www.researchgate.net/publication/391738972_Cyber_Law_and_Data_Privacy_in_the_21_st_Century_Emerging_Legal_Issues_and_Challenges

8. Information Technology (Amendment) Act,2008,

https://www.bcasonline.org/Referencer2015-16/Other%20Laws/information_technology_act_000.html

9. Revised Information Technology Act to strengthen security and privacy of data - PIB, https://www.pib.gov.in/newsite/erelcontent.aspx?relid=50088

10. Difference Between IT Act 2000 and IT Act 2008: A Comprehensive Overview, https://www.advocatepriyapaul.com/blog/difference-between-it-act-2000-and-it-act-2008.php

11. Information Technology (amendment) Act, 2008 : An Overview - Articles – Manupatra, https://articles.manupatra.com/article-details/Information-Technology-amendment-Act-2008-An-Overview

12. Offences and Penalties under Technology Act - IndiaFilings, https://www.indiafilings.com/learn/offences-and-penalties-under-technology-act/

13. Data Privacy Protection in India - Institute of Law - NIRMA UNIVERSITY, https://law.nirmauni.ac.in/data-privacy-protection-in-india-technology-vis-a-vis-law/

14. Information Technology Amendment Bill 2008 - Seth Associates, https://www.sethassociates.com/information-technology-amendment-bill-2008.html

15. Cybercrime Against Women - PIB, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1881404

16. Compliance as Per IT Act - Finlaw Associates, https://finlawassociates.com/it-compliance-litigation-lawyer.php

17. Untitled - Ministry of Electronics and Information Technology, https://www.meity.gov.in/static/uploads/2024/03/ITbill_2000.pdf

18. Sections 66C-66D - UNODC's Sherloc, https://sherloc.unodc.org/cld/en/legislation/ind/the_information_technology_act_2000/chapter_xi/sections_66c66d/sections_66c-66d.html

19. Implementation of S.66A IT Act - Supreme Court Observer, https://www.scobserver.in/cases/peoples-union-for-civil-liberties-implementation-of-s-66a-it-act-case-background/

20. S. 69 of the Information Technology Act and the Decryption Rules : Absence of adequate procedural safeguards - Software Freedom Law Center, India, https://sflc.in/s-69-information-technology-act-and-decryption-rules-absence-adequate-procedural-safeguards/

21. Section 69 - India Code, https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=88

22. Understanding CERT-IN Directions for Cybersecurity in India - Securityium, https://www.securityium.com/understanding-cert-in-directions-for-cybersecurity-in-india/

23. Incident Reporting to Indian Computer Emergency Response Team [CERT-In] in 2024, https://www.neumetric.com/incident-reporting-indian-cert-in-2024/

24. How Do Organizations Comply With the 2022 CERT-In Directions? - InfoSec Brigade - Information and Cyber Security Solution, https://infosecbrigade.com/how-do-organizations-comply-with-the-2022-cert-in-directions/

25. CERT-IN Directions - AZB & Partners, https://www.azbpartners.com/bank/cert-in-directions/

26. Section 79 of the IT Act 2000, Legal Framework, Latest News - Vajiram & Ravi, https://vajiramandravi.com/current-affairs/section-79-of-it-act/

27. Navigating New Digital Frontiers: The IT Rules 2021 and Their Impact on Intermediaries,

https://www.khuranaandkhurana.com/2024/08/20/navigating-new-digital-frontiers-the-it-rules-2021-and-their-impact-on-intermediaries/
28. Section 79 and the IT Rules: Privatising censorship in India - Internet Democracy Project, https://internetdemocracy.in/laws/the-information-technology-amendment-act-2008/section-79-and-the-it-rules/
29. Information Technology Act 2000, as amended by the Information Technology (Amendment) Act 2008 | wilmap, https://wilmap.stanford.edu/entries/information-technology-act-2000-amended-information-technology-amendment-act-2008
30. The Information Technology (Intermediary Guidelines and Digital ..., https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf
31. Intermediary Guidelines 2021 - Treelife, https://treelife.in/legal/intermediary-guidelines-2021/ 32. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 & Grievance Redressal - Law Community, https://lawcommunity.co.in/articles/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021-grievance-redressal/
33. Directions issued by CERT-In on April 28, 2022 - Sangeeta Rana Law Practice, https://www.srlawpractice.in/directions-issued-by-cert-in-on-april-28-2022/
34. CERT-In 2022 Guidelines – Cyber security advisory - Positka, https://positka.com/services/cert-in
35. CERT-In Cyber Security Direction 2022 - Varutra Consulting, https://www.varutra.com/cert-in-cyber-security-direction-2022
36. Understanding CERT-In's Cybersecurity Directions, 2022 | The CCG Blog, https://ccgnludelhi.wordpress.com/2022/06/15/understanding-cert-ins-cybersecurity-directions-2022/
37. India extends deadline for compliance with infosec logging rules by 90 days - The Register, https://www.theregister.com/2022/06/28/india_directions_deadline_logging/
38. Increased Penalties for Failure to Comply with the 2022 CERT-in Directions, https://ksandk.com/newsletter/increased-penalties-for-failure-to-comply-with-2022-cert/
39. Regulators, Enforcement Priorities and Penalties | India | Global Data and Cyber Handbook, https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/asia-pacific/india/topics/regulators-enforcement-priorities-and-penalties 40. Securing AI in 2025: A Risk-Based Approach to AI Controls and Governance | SANS Institute, https://www.sans.org/blog/securing-ai-in-2025-a-risk-based-approach-to-ai-controls-and-governance/
41. What is Incident Response? Process, Plan, and Complete Guide (2025) - Sygnia, https://www.sygnia.co/blog/what-is-incident-response-process-plan-and-complete-guide/
42. What Is AI Cybersecurity | Trend Micro (US), https://www.trendmicro.com/en_us/what-is/ai/ai-cybersecurity.html
43. AI and Cybersecurity: Automating Incident Response Processes to Minimize Downtime and Damage - TEAM International, https://www.teaminternational.com/en/blog/ai-cybersecurity
44. AI in Cybersecurity Incident Response: Automating Crisis Management - Akitra, https://akitra.com/ai-in-cybersecurity-incident-response/
45. Automated Malware Detection and Classification using Machine Learning, https://journals.mriindia.com/index.php/ijacect/article/view/130

46. AI-Powered Malware Analysis | How Artificial Intelligence Detects and Prevents Malware Attacks - Web Asha Technologies, https://www.webasha.com/blog/ai-powered-malware-analysis-how-artificial-intelligence-detects-and-prevents-malware-attacks

47. AI in Malware Analysis - ramsac Ltd, https://www.ramsac.com/blog/ai-in-malware-analysis/

48. Cybersecurity Datasets (Intelligence-led Security) - Behaviour-Centric Cybersecurity Center (BCCC) - York University, https://www.yorku.ca/research/bccc/ucs-technical/cybersecurity-datasets-cds/

49. Network Anomaly Detection: A Comprehensive Guide - Kentik, https://www.kentik.com/kentipedia/network-anomaly-detection/

50. Network Traffic Anomaly Detection with Machine Learning - Eyer.ai, https://www.eyer.ai/blog/network-traffic-anomaly-detection-with-machine-learning/

51. India unveils AI incident reporting guidelines for critical infrastructure, https://dig.watch/updates/india-unveils-ai-incident-reporting-guidelines-for-critical-infrastructure

52. Cybersecurity Incidents in India (2020–2024) - Kaggle, https://www.kaggle.com/datasets/saisimha203/cybersecurity-cases-india

53. Cyber |Open Government Data (OGD) Platform India, https://www.data.gov.in/keywords/Cyber