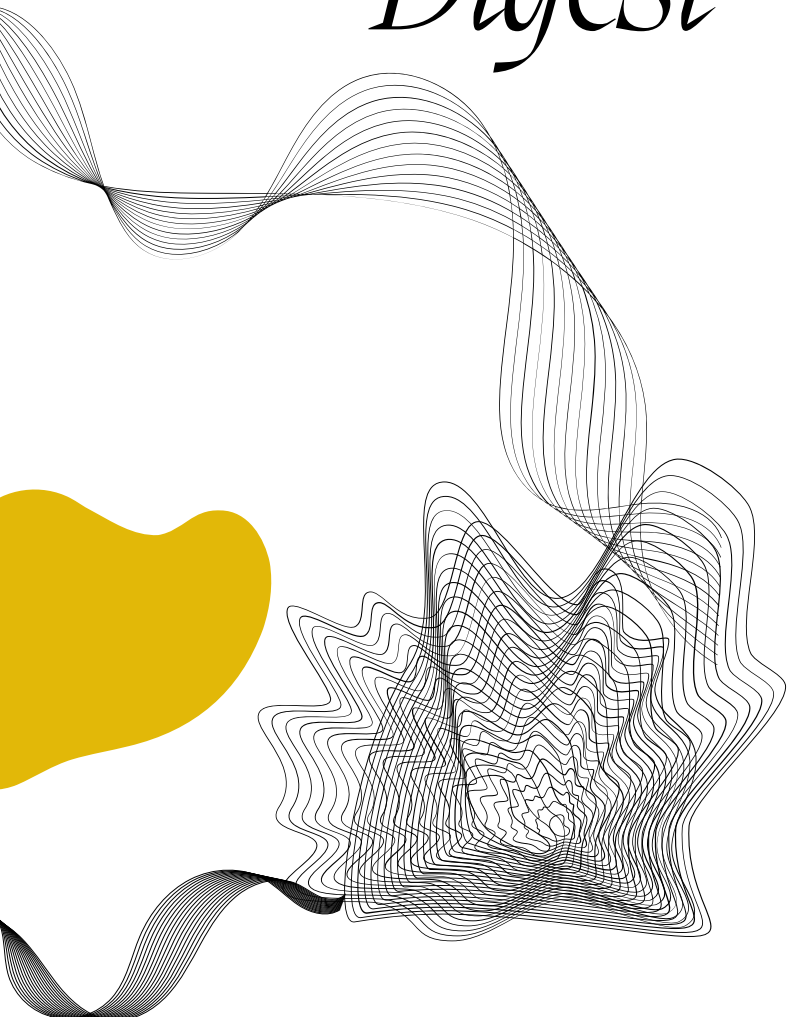
DSCI
PROMOTING DATA PROTECTION

DSCI Digest

March 2025



DSCI Digest

The DSCI Digest is brought to you for a peripheral understanding of the industry-relevant studies conducted by DSCI. It aims to help you learn and understand the subjects in discussion in a succinct composition.

Table of Contents

Reimagining Security: An Era Powered by Generative AI

In the era powered by Generative AI, a comprehensive analysis of the current state of the cybersecurity landscape, with a particular focus on the integration of Generative AI technologies, is important. Cyber threats continue to evolve and escalate, making it imperative for organizations to adapt their security strategies and safeguard their assets to maintain trust in the digital age.

This report aims to highlight the challenges and opportunities presented by Generative AI in enhancing cybersecurity measures while also examining the emerging trends within the Indian security landscape, as India's cybersecurity market is expected to account for 5% of the global market by 2028. Furthermore, the adoption of Generative AI in user organizations is gradually gaining momentum, as businesses recognize the potential of AI-powered solutions to enhance threat detection and incident response. Generative AI is a promising technology, with nearly 35-40% of security providers already integrating it into their offerings within just two years.

Integrating AI and automation will play a crucial role in enhancing the organizations' ability to combat cyber threats effectively as they continue to prioritize security.

However, technological advancements and growing reliance on them have accelerated the risk of cyber threats. From data breaches and identity theft to critical infrastructure attacks and geopolitical espionage, the average cost of a data breach has jumped to $4.88 million, pointing out that globally the stakes have never been higher. Notably, 88% of cybersecurity breaches are due to addressable human error.

Expanded digital footprint, increased interconnectedness of critical infrastructure, and the widespread adoption of Generative AI have unlocked new opportunities for cyberattacks,

as malicious actors exploit these tools to launch sophisticated attacks.

Some of the common cyberattack pathways include:

- Email
- Third-party and open-source software
- Web applications
- End-point devices
- Cloud-based pathways
- Software supply chain
- Mobile devices
- Operating systems

These often lead to vulnerabilities such as misconfigurations, unsecured APIs, outdated/unpatched software, zero-day vulnerabilities, weak or stolen user credentials, unauthorized access, and more.

This calls for greater attention to AI penetration and its impact on cybersecurity. Until 2023, its use was limited to summarization, accessibility to security information, and decomposition of complex problems. But the tide changed in 2024, Generative AI was now used to achieve complex security goals, adapt to evolving threats, and learn from past experiences. Therefore, accuracy and trust-building have emerged as key goals with the usage.

Expanding its delivery, Generative AI can now assist with:

- Dynamic protocol updates
- Continuous hardening
- Automated enforcement of security policies
- Security posture adjustment
- Prioritization of incidents based on severity
- Autonomous threat detection
- Precise risk identification
- Vulnerability prediction

Despite the potential, there remains a global shortage of 4 million cybersecurity professionals. Organizations are trying to bridge this gap by building their talent pool and increasing productivity with Generative AI. However, ethical concerns over privacy, bias, accountability, sensitive data exposure, AI-powered malware, and deepfake threats hold back its effective leverage.

India, however, shows promise with over 400 companies in its cybersecurity ecosystem, making it an emerging hub for cybersecurity services. There has been a significant increase in product startups and expansion of managed security services and system integrators with growing demand. A notable trend is that global end-user enterprises are embracing Generative AI-led shifts in cybersecurity strategies by:

- Increasing cybersecurity spending.
- Making Generative AI a top investment priority after the cloud.
- Evaluating data privacy concerns of incorporating Generative AI.
- Prioritizing regular audits and model testing to mitigate associated risks.

Current security measures include data loss prevention strategies, online risk management policies, digital asset security plans, and information breach response protocols. Best practices being exercised by organizations include regular security awareness training, continuous monitoring and patching, and robust access controls.

Security technology providers are also innovating by incorporating Generative AI into their solutions portfolio, particularly in AI/ML applications, by:

- Advanced threat detection through data-driven pattern analysis and anomaly detection.
- Automated threat response with predefined actions like IP blocking and system isolation.
- Anomaly detection through behavioral analysis.
- Potential threat and vulnerability detection by analyzing historical data patterns.

Several security processes such as data collection, aggregation, analysis, and behavioral pattern segmentation are likely to be automated as Generative AI adoption grows. This will enable security professionals to focus on advanced threat assessments requiring human intuition and expertise. Adoption has surged across BFSI and manufacturing sectors, followed by healthcare and retail. More hi-tech and telecom SMEs are also embracing Generative AI-enabled security services.

However, the top challenges remain:

- Data quality and bias.
- Model interpretability and explainability.
- Security risks involving sensitive data usage.

To overcome these challenges, security providers prefer partnerships and industry collaborations to kick-start their Generative AI journey. Combined resources and knowledge in data sharing, compute optimization and expertise access enable the creation of robust and innovative solutions. In-house Generative AI development, while time-

-consuming allows firms to build custom solutions, ensure smooth integration with existing systems, and establish early-mover advantages. Co-creation with clients and R&D partnerships with academia also hold the potential for unlocking innovation and IP creation over time.

Security organizations are focusing on training existing non-AI tech workforces and hiring external specialists to prepare for the AI-led cybersecurity transformation. According to ISC2, 88% of its members believe AI influences their current jobs, primarily in a positive way through increased efficiency, though concerns about job redundancy persist. Partnerships have gained importance due to the complex nature of Generative AI solutions.

The scenario can improve if end-user enterprises adopt a comprehensive cybersecurity framework, enabling them to proactively protect valuable assets, maintain business continuity, and build stakeholder trust. For service providers, the recommended security playbook would include:

- Assessment and planning
- Architecture design and implementation
- Verification and validation
- Monitoring and detection
- Risk management and compliance
- Incident response and recovery

However, different stakeholders have varying recommendations for better security. Service providers should invest in AI expertise and prioritize data security. User organizations must evaluate AI solutions critically and foster AI literacy. Startups can focus on niche applications and collaborate with established players while governments should establish clear AI regulations and promote AI research and development.

For a deeper understanding including case studies, explore the detailed report on "Reimagining Security: An Era Powered by Generative AI" at: https://www.dsci.in/resource/content/reimagining-security-in-gen-ai-era

India Cyber Threat Report 2025

India's economy remains robust, driven by strong government investments in infrastructure, local manufacturing, and consistent service industry performance. The digital economy is therefore projected to contribute 20% of GDP by 2026 and has also become a prime target for cyberattacks, accounting for 13.7% of global incidents.

This report, in collaboration with Seqrite, has been developed after covering data from nearly 85 lakh endpoints, thus providing a comprehensive analysis of cyber threats and India-specific recommendations to help businesses strengthen their defenses in the coming day and age.

When we talk about the past year, it saw significantly escalated threats and advances in detection capabilities. The detection of over 369.01 million security incidents across 8.44 million endpoints means that, on average, every minute saw 702 potential security threats. This volume of attacks demonstrates the relentless nature of modern cyber threats and the constant pressure on security systems.

A noteworthy observation has been the increase in malware detection (extending to Android-based security detections) and how it has changed. The collected data highlights the scale of cyber threats and the gaps in protection. The majority of detections, 85.44%, relied on signature-based methods, underscoring the persistence of known threats.

However, 14.56% of detections came through behavior-based detection (increased from 12.5%), emphasizing the growing need for adaptive security to identify emerging, unknown threats as they become more sophisticated.

The subcategory detections that dominated the malware landscape were Trojans (about 43%), followed by Infector, Worm, PUA (Potentially Unwanted Applications),

Exploit, Adware, Cryptojacking, and, Ransomware. Another important finding has been increased attacks on cloud environments as enterprise migration to the cloud is leading to an expansion of the attack surface. Geographically speaking, out of all the nation-states, the India malware landscape experienced the highest detections across the states of:

- Telangana (highest around 15.03% detections)
- Tamil Nadu (second highest around 11.97% detections)
- Delhi (third highest around 11.79% detections)

These were followed by the states of Karnataka, Rajasthan, Uttar Pradesh, Gujarat, Maharashtra, Madhya Pradesh, and West Bengal, where 51.13% of total national security detections are concentrated. The cities that recorded the top 34.06% of detections include New Delhi, Jaipur, Ahmedabad, Surat, Mumbai, Pune, Hyderabad, Bengaluru, Chennai, and Kolkata.

On the other hand, industries like Healthcare (highest around 21.82%), Hospitality (19.57%), BFSI (17.38%), Education (15.64%), MSME (7.52%), Manufacturing (6.88%), Government (6.10%), and IT/ITES (5.09%) experienced the most cybersecurity incidents. The study reveals critical insights into India's cybersecurity landscape, identifying key threats including: prominent hacktivist groups targeting Indian networks, high impact threat actors, commonly exploited driver vulnerabilities, frequently abused Living-Off-the Land Binaries (LOLBins), prevalent malicious file types, widely misused file-sharing platforms, dominant MITRE ATT&CK techniques, and the most active ransomware groups operating in the region.

This evolving threat landscape underscores the increasing importance of the intersection of geopolitics and cybersecurity which is more critical than ever, both in global and local contexts. Nations are leveraging cyber capabilities to advance their strategic objectives while facing the growing challenge of defending against sophisticated and coordinated cyberattacks.

If we look into the long-term projections (2026-2030), there can be:

- Emergence of quantum warfare
- Autonomy of AI in cyber operations
- Targeting of space infrastructure
- Battles for digital sovereignty

The Indian Cyber Crime Coordination Centre (I4C), established by the Ministry of Home Affairs, has also taken a proactive stance in responding to the hacktivist threats. The Indian government has enhanced cybersecurity measures, launched public awareness campaigns, and ramped up collaborations with international cybersecurity organizations to strengthen defense capabilities.

However, the speed and scale of hacktivist attacks have already tested India's cyber defense infrastructure, highlighting the need for more robust and agile responses to politically motivated cyber incidents.

India's position within the broader geopolitical context further complicates its cybersecurity challenges. As a key ally of Israel in the Middle East and a member of the Quad (with the US, Japan, and Australia), India faces mounting pressure from hostile state-sponsored actors and hacktivists.

Therefore, key areas of focus for India's cybersecurity strategy in the coming years should include:

- Enhancing critical infrastructure protection.
- Developing a strong national cyber defense framework.
- Fostering international cooperation.

Apart from this, the survey was conducted to understand the industry's cybersecurity preparedness, which helped identify the top five investment priorities for 2025. These are threat detection and response, data protection, endpoint security, cloud security, and employee training.

This also serves as a strong reminder to be wary of the next wave of threats, which are predicted to be:

- Ransomware evolution: Complex extortion and physical sabotage
- Cloud & API vulnerabilities: Expanding attack surfaces
- Supply chain attacks: Amplified cybersecurity risks
- IoT & edge device exploitation: The next botnet frontier
- AI-driven attacks: Enhanced social engineering & data poisoning
- Hacktivist shifts: Migration to secure platforms
- Targeted attacks on critical infrastructure: Increasing sophistication
- Convergence of AI-driven TTPs and supply chain attack vectors
- AR malware: Emerging threats

in augmented reality
- AI-powered adaptive malware: Real-time evasion tactics
- Cloud-controlled malware on Android: Evading detection

Emerging financial application threats: Government and investment platform exploitation
- Deepfake-enabled malware: Enhanced deception techniques
- Zero-day exploits in emerging technologies
- Mobile malware sophistication: Beyond traditional threats
- Cryptojacking and resource exploitation attacks
- Biometric data exploitation: Targeting authentication systems
- Insider threats enhanced by malware
- AI-driven offensive capabilities: Enhanced attack automation
- Cyber warfare & geopolitical tensions

The evolving threat landscape of 2025 demands a fundamental shift in how CISOs approach cybersecurity. Traditional security models are becoming obsolete against quantum-enabled threats, AI-powered attacks, and state sponsored operations. The recommendations, therefore, are suggested on the lines of:
- Embrace artificial intelligence (AI) and machine learning (ML) for threat detection and response
- Adopt a zero-trust security framework
- Prepare for cloud-native security challenges
- Focus on cyber resilience, not just prevention
- Invest in threat intelligence and collaboration

These recommendations and predictions are dealt with in detail, with a special emphasis on featured stories to present the cybersecurity scenario we as an industry have experienced. Gain comprehensive first-hand learning with the report on "India Cyber Threat Report 2025": https://www.dsci.in/resource/content/india-cyber-threat-report-2025

Cyber Resilience in Hospitals

Today, the average Indian household spends about 5.9% of its annual expenditure on health. This number has doubled since 2012. Therefore, consumer awareness and commitment to health have increased in the last 10 years. Correspondingly, there has been increased investment in both public and private healthcare.

Over the past five years, there has been an unprecedented adoption of digital technologies in the healthcare system. Key areas of transformation include patient engagement and experience, clinical data lakes, clinical decision support systems, operational efficiency, and new care models such as telemedicine.

This transformation is delivered via the cloud, contributing to the higher adoption of cloud technology in healthcare compared with the life sciences sector. As a result of the increased digital footprint, cyberattacks on the healthcare sector have risen.

Today, India ranks among the world's top five most cyber-attacked healthcare systems.

The COVID-19 pandemic further accelerated the enhancement of hospitals' digital infrastructure. The pandemic prompted the release of guidelines for telemedicine, leading to a further expansion of the digital footprint in healthcare. The usage of digital technology within the healthcare sector has also been expedited, and emerging technologies are facilitating the advancement of cost-effective, superior therapeutic interventions. Subsequent strategies should therefore focus on assisting India in developing a digitally advanced and enduring healthcare infrastructure for the future.

As the trend continues, the next few years will see enhanced development in the following areas:

- Interoperable patient records, where the records can be shared with various providers based on a consent mechanism.

- Integration of HIS and EMR systems with government programs such as Ayushman Bharat Digital Health Mission.
- Integration of AI into clinical diagnosis and enhanced remote diagnosis of patients.
- Molecular biology and genomic research for personalized therapy and medicines.
- Establishment of clinical boards for all major therapeutic areas.
- Enhanced digital transformation in key areas.

The major areas of digitization will include:

- Cloud services, ePharmacy, and patient experience
- CRM (Sales and marketing)
- AI/ML-driven CDSS
- Big data analytics with a focus on Clinical Data Lake
- Robotic surgeries—Da Vinci/Mantra
- IoT applications—Wearable and sensor devices for remote patient monitoring

Moreover, healthcare's digital shift is taking place through hybrid cloud computing. Hospitals use this innovation through a private cloud-computing system, simplifying patient treatment nationwide. However, a shortage of technical expertise, operational challenges, financial strain, and cloud security risks remain. This warrants stakeholders to carefully evaluate the cloud risks, whether technical, cybersecurity, or regulatory. They should recognize the importance of thorough risk assessment to ensure the security and compliance of their cloud environments.

The ecosystem in India currently provides healthcare services to over 1.3 billion people and beyond to foreign nationals. The hospital industry in India is projected to experience significant growth driven by multiple factors like government initiatives, infrastructure investments, technology adoption via telemedicine, digital health solutions and electronic medical records, health insurance coverage, demographic trends, disease burden, and changes in the regulatory environment.

Advancements in technology and digitization have led to a greater boon in the medical industry. Hardcopy versions of patients' therapeutic records are now replaced by digital copies, and specific therapeutic records can be easily retrieved digitally. This has enhanced public healthcare by improving efficiency, accessibility, quality of care, and health outcomes, with 80% of hospitals

maintaining EMRs, and 40% having integrated EMRs into HMIS (Health Management Information Systems).

But this influx of technology has also contributed to cyberattacks. The key cybersecurity challenges that have emerged now are:

- Personal data protection
- Third-party and supply chain risks
- Stakeholder and employee awareness
- Protecting IP data
- Cloud security
- Securing remote access
- Insider threat or inadvertent leakage
- Insecure devices
- Cyber talent management (lack of budget)

Moreover, hospitals become prime targets for attackers to execute data breaches, launch active assailant attacks, harbor physical security deficiencies, leverage insider threats, and exploit systems' vulnerabilities due to legacy systems. On average, hospitals spend 8–10% of their IT budget on cybersecurity techniques, such as hiring professionals and acquiring tools to minimize cyberattacks to the maximum extent. Our survey conducted on hospitals indicates that this percentage may increase to 12–15% in the next two years.

The top priorities would then include data security and privacy, identity and access management, cyber resilience, cyber strategy risk and governance, extended enterprise security, and next-gen security operations. The focus areas to achieve this would be infrastructure, endpoint and application security, security for emerging tech, cloud security, and IoT security.

Therefore, incorporating a SOC would cultivate a round-the-clock security mindset to safeguard patient data and healthcare operations. Its crucial aid could be seen in efficient operations with SIEM integration, improved patient security through IoT security, proactive defense against phishing threats, and effective endpoint detection and response within the SOC for prompt address of threats.

Another important consideration from a strategic viewpoint is the involvement of the board and management in cyberspace. Their involvement can help in vigilant monitoring to mitigate system visibility oversight. Their in-depth review can further strengthen cybersecurity preparedness, prioritize and address patient-

related cyber concerns, include cyber tabletop exercises, make strategic budget allocations, ensure compliance with relevant regulatory requirements, and facilitate thorough discussions on cyber risks at the board level.

For hospitals, their key pillars of resilience lie in third-party risk management, crisis management plans, crisis simulation/red teaming, vulnerability and penetration testing, cyber insurance, and a zero-trust framework. Some hospitals adhere to the ISO 27001 and NIST Framework, while others lack a defined standard due to being in the planning stage or facing uncertainty surrounding the decision.

This brings us to the understanding that the pandemic may have accelerated the digital infusion, but challenges and exposures remain paramount and need effective handling with substantial investment in cybersecurity. As cloud capabilities continue to escalate annually and a 50% surge in teleconsultations is projected over the next 5–10 years, the need for heightened cybersecurity measures within hospitals becomes evident. Key priorities include fortifying data security and privacy, bolstering cyber resilience, refining cyber strategy, and enhancing TPRM protocols.

The survey also found that nearly 80% of hospitals have invested in foundational cybersecurity architecture, notably establishing Security Operations Centers (SOCs). It is therefore an important recommendation to propel the discussed board-level engagement, where discussions revolving around cyber strategies frequently can involve technology leaders in monthly or quarterly board meetings. In summary, there is a clear trajectory towards amplified investment in cybersecurity across the healthcare sector's spectrum of people, processes, and technologies. All it needs is the right and timely implementation.

A more detailed understanding of the survey can be found in the report on “Cyber Resilience in Hospitals” at: https://www.dsci.in/resource/content/cyber-resilience-in-hospitals

Assessing India's Cybersecurity Regulations in a Dynamic Environment

The rapid advancements in artificial intelligence have accelerated the global shift toward digitization, compelling governments to adopt modern technologies to match private sector services. In Asia-Pacific, governments are enhancing e-government services, improving data analytics capabilities, and implementing digital economy development plans to support the digital transformation.

Aiding this situation is cloud computing and other enterprise solution providers like resource management platforms, cyber security solutions providers, which offer flexible computing power and data storage, enabling businesses to scale operations according to their needs while ensuring cost efficiency, scalability and continuity. These advancements ease enterprises of managing complex IT systems, allowing them to focus on core objectives and digital innovation. Particularly, speaking of, cloud technologies support remote work, real-time data access, and enhanced cybersecurity through centralized management.

While benefits of employing enterprise solutions are immense, there are viable risks, such as security and privacy concerns, vendor concentration risks, third-party access management risks, and potential national security threats, as digitization through cloud services becomes a strategic priority for enterprises. In response, governments are developing comprehensive cybersecurity regulations to ensure secure, resilient, accountable, trustworthy, and transparent cyber ecosystems, maximizing the benefits of digitization for all stakeholders in society and the economy.

For enterprises, these regulations

can act as both a safeguard and a challenge. They provide guidance to protect against cyber threats and data breaches but may also require significant compliance investments, potentially hindering innovation and increasing operational complexity. Thus, creating an equilibrium between regulation and innovation is essential. Hence, the report seeks to understand how these regulations affect cloud service providers and enterprise solution providers, ultimately developing common parameters for enterprise users to assess the effectiveness of solution providers along with guidance for navigating regulations

The current wave of digitization is largely driven by the Software as a Service (SaaS) model, offering businesses flexibility, scalability, cost efficiency, and enhanced security. However, due to diverse enterprise needs, a single cloud model may not suffice for all businesses. This has led to the rise of Enterprise Service Providers (ESPs), companies specializing in IT solutions such as software development, IT infrastructure management, cloud computing, cybersecurity, and strategic consulting. They also integrate technologies like Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and Supply Chain Management (SCM) into cohesive systems that align with a company's operational and strategic objectives.

However, transitioning enterprises to cloud environments presents unique regulatory and security challenges, making compliance with cybersecurity frameworks a top priority.

Therefore, understanding the frameworks becomes important. In the context of India, the cybersecurity landscape consists of national, institutional, sectoral, and state-level regulations. Key national-level regulations include:

- Information Technology Act, 2000 (IT Act)
- CERT-In directions under Section 70B (April 2022)
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, also referred to as SPDI rules
- Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018
- The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code Rules, 2021)
- The Digital Personal Data Protection Act, 2023

- National Cyber Security Policy 2013
- The Aadhaar (Data Security) Regulations, 2016
- Meghraj Policy – Cloud Security Best Practices
- National Information Security Policy and Guidelines (2019) Version

Important regulatory bodies include CERT-In, the National Critical Information Infrastructure Protection Centre (NCIIPC), and the National Cyber Security Coordinator (NCSC). Additionally, various sectoral regulations govern cybersecurity practices across industries, such as banking, telecommunications, insurance, and power. These are:

- CEA (Cyber Security in Power Sector) Guidelines 2021
- Draft CEA's Regulation Measures on Cyber Security in the Power Sector, 2024
- The Reserve Bank of India (RBI) Cyber Security Framework in Banks, 2016
- RBI Master Direction on Outsourcing of Information Technology Services (April 10, 2023)
- Draft Telecommunication Cyber Security Rules 2024
- Draft Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024 (CTI) Rules
- MeitY Cloud Empanelment Guidelines
- SEBI Framework for Adoption of Cloud Services
- SEBI Cyber Security and Cyber Resilience Framework
- IRDAI Information Security and Cyber Security Guidelines 2023
- PFRDA: Circular on Information and Cyber Security Policy Guidelines - 2024 for Intermediaries/Regulated Entities

State-wise policies, such as the Maharashtra Cloud Computing Policy 2018, Assam Cyber Security Policy 2020, Uttar Pradesh Information Security Policy, Assam Cyber Security Policy 2020, Telangana's Cyber Security Policy 2016 and Madhya Pradesh's Cloud Adoption Framework 2022 further add layers of compliance requirements.

To align with evolving cybersecurity regulations, ESPs in general need to adhere to fundamental security standards, including:

- Identity and access management (IAM) solutions
- Network segmentation and secure connection protocols
- High availability and business continuity measures
- Multi-compliance and

reporting capabilities
- Robust data protection mechanisms

Given the complexities of compliance, a shared responsibility model between enterprises and service providers is essential. This model clarifies security responsibilities, ensuring accountability in managing cybersecurity risks. However, inconsistencies in regulatory frameworks, such as varying data localization requirements and incident reporting mandates, pose significant operational challenges for ESPs and enterprises alike.

To address these challenges, it is required that the regulations governing cybersecurity requirements work in harmony and do not prescribe diverse requirements for the same set of requirements. For enterprises, it may be required to ensure the demonstration of proactive compliance to the existing regulations and set industry benchmarks to devise a proactive cybersecurity strategy to drift away from the ever-emerging cyber security threats in the age of AI which the existing regulations may not have thought of. In that backdrop, the key recommendations for strengthening cyber resilience include:

- Promoting industry-driven best practices
- Harmonizing regulations across sectors
- Adopting a risk-based approach to cybersecurity
- Ensuring alignment with global security standards
- Encouraging stakeholder collaboration
- Investing in capacity-building initiatives

This report further provides a comprehensive analysis of India's cybersecurity regulatory landscape and its impact on ESPs and cloud service providers. It also offers insights into global regulatory trends, covering the US, Europe, Asia-Pacific, and Australia. By understanding these evolving frameworks, enterprises can better navigate the regulatory environment, enhance security resilience, and drive innovation in the digital economy. For further details access the report on "Assessing India's Cybersecurity Regulations in a Dynamic Environment" at: https://www.dsci.in/resource/content/assessing-india-cybersecurity-regulations

What to Expect in the Next Edition

The DSCI Digest offers a condensed version of all our publications, giving you a quick overview to help you decide on your next read.

The subjects catered here enable you to gain first-hand information on the volumes we bring out for the industry. The information shared is a brief account of the conducted studies, you are requested to visit the reports on our website for better understanding.

https://www.dsci.in/knowledge-center/study-and-reports

Authors

- Reimagining Security: An Era Powered by Generative AI by Niharika Singh
- India Cyber Threat Report 2025 by Neha Mishra
- Cyber Resilience in Hospitals by Ankit Bhadola
- Assessing India's Cybersecurity Regulations in a Dynamic Environment by Deepa Ojha

Compiler and Editor

Mridushi Bose, Content Marketing Manager

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in

DATA SECURITY COUNCIL OF INDIA

NASSCOM CAMPUS, FOURTH FLOOR, PLOT. NO. 7-10, SECTOR 126,
NOIDA, UP - 201303
+91-120-4990253 | INFO@DSCI.IN | WWW.DSCI.IN

fdsci.connect dsci.connect dscivideo data-security-council-of-india DSCI_Connect