Cybersecurity Trends in India

A Comprehensive Analysis for 2024-2025

1. Executive Summary

India stands at a pivotal point in its digital journey, witnessing rapid advancements across numerous sectors. This transformation, while bringing significant economic and societal benefits, has also ushered in an era of heightened cybersecurity challenges. The cybersecurity landscape in India for 2024 and 2025 is characterized by an increasing volume and sophistication of cyberattacks, driven by factors such as the proliferation of AI-powered threats and the expanding digital footprint of organizations and individuals. Despite a decrease in the overall number of incidents in 2024, the complexity of attacks has grown, demanding more advanced and adaptive security measures. The Indian government has responded with strategic initiatives and regulatory frameworks, including the Digital Personal Data Protection Act 2023, aimed at fortifying the nation's digital defenses. Adoption of advanced security solutions like zero-trust architecture and Extended Detection and Response (XDR) is on the rise, although challenges related to implementation and the persistent cybersecurity skills gap remain. Geopolitical events continue to exert influence, further emphasizing the need for a robust and resilient cybersecurity posture. Predictions for the near future point towards an intensification of AI-driven threats and the continued targeting of critical sectors. Recent major cybersecurity incidents underscore the tangible risks and the importance of proactive security measures.

2. Introduction

India is undergoing a significant digital revolution, marked by the widespread adoption of new technologies and the digitalization of essential services. This transformation spans across vital sectors including finance, where innovative systems like UPI process billions of transactions monthly [1], as well as governance, healthcare, and critical infrastructure.[1] The nation's ambitious goal to achieve a USD 1 trillion digital economy by 2030, with digital services projected to contribute a substantial portion of its GDP by 2026 [1], highlights the scale and pace of this change. However, this rapid digitalization presents a dual challenge. While it offers unprecedented opportunities for growth and efficiency, it simultaneously expands the nation's cyber frontier, making it increasingly attractive to malicious actors.[1] Consequently, India now accounts for a notable percentage of global cyber incidents.[1] The government's proactive push to digitalize various facets of governance and critical infrastructure has undeniably enhanced accessibility and efficiency for a vast population. Nevertheless, it has also exposed inherent systemic fragilities, including a population still navigating the nuances of digital literacy and organizations that are yet to fully mature their cyber hygiene practices. Sectors crucial to the digital economy, such as healthcare and finance, are emerging as primary targets for sophisticated ransomware and data extortion attacks.[1] Furthermore, the rise of artificial intelligence introduces a new layer of complexity, presenting both ethical dilemmas and the emergence of sophisticated malware capable of evading conventional security defenses.[1] The cybersecurity landscape in India for 2025 is therefore defined by an ongoing contest between the relentless advancement of technology and the ever-evolving sophistication of cyber threats. While progressive legislation and

strategic national policies aim to strengthen defenses, persistent gaps necessitate a continuous and adaptive approach to cybersecurity.

3. Cybersecurity Threat Landscape in India (2024-2025)

3.1 Analysis of Recent Reports and Key Findings

Several key reports provide valuable insights into the cybersecurity trends in India for 2024 and 2025. The India Cyber Threat Report 2025 by the Data Security Council of India (DSCI) in collaboration with Seqrite [3, 4, 5], Check Point's 2025 Security Report [6, 7, 8], and Palo Alto Networks' Unit 42 Incident Response Report 2025 [9, 10] are particularly noteworthy. These reports collectively highlight the dynamic and challenging nature of the threat landscape. Check Point's 2025 Security Report, analyzing data from 170 countries, reveals an alarming 44% increase in global cyberattacks year-over-year.[6, 7, 8] This surge underscores the escalating threat environment that India is also contending with. Notably, Check Point's findings indicate that organizations in India face a significantly higher average of weekly attacks compared to the global average. Over the past six months leading up to their report, Indian organizations experienced an average of 3,291 attacks per week, substantially exceeding the global average of 1,847.[6] This consistently higher attack rate in India suggests that the nation is a particularly attractive target for cybercriminals. This could be attributed to India's large and rapidly growing digital footprint, coupled with varying levels of cybersecurity maturity across different sectors and organizations. A larger user base and potentially less mature security practices in some segments might present more lucrative opportunities for malicious actors. The fact that multiple prominent cybersecurity vendors are independently reporting on these trends lends further credence to the severity and breadth of the observed increase in cyber threats. The consensus across these reports from different vantage points reinforces the validity of the findings and provides a comprehensive understanding of the evolving threat landscape in India.

3.2 Detailed Breakdown of the Most Common Cybersecurity Threats Observed

India's cybersecurity landscape in 2024 and 2025 is marked by a variety of persistent and evolving threats. **Malware** continues to be a significant concern, with the India Cyber Threat Report 2025 indicating a high volume of detections, totaling 369.01 million across 8.44 million endpoints in 2024.[3, 4, 5] While this represents a slight reduction from the previous year, the sheer volume underscores the scale of the threat. Trojans and Infectors remain the most prevalent types of malware detected.[3, 4, 5] Notably, there has been an increase in behavior-based malware detections, rising from 12.5% in 2023 to 14.5% in 2024.[1, 3, 4] This shift indicates that attackers are employing more sophisticated malware capable of evading traditional signature-based detection by altering their code or concealing themselves within legitimate processes.

Ransomware also continues to pose a major threat to Indian organizations.[1, 4, 6, 11] While traditional ransomware attacks involving data encryption persist, there is a growing trend towards data extortion tactics.[1, 4, 6, 11] In this approach, attackers steal sensitive data but may not necessarily

encrypt it, leveraging the threat of public disclosure to pressure victims into paying a ransom. Sectors such as healthcare, hospitality, and BFSI (Banking, Financial Services, and Insurance) are particularly targeted due to the high value and sensitivity of the data they handle.[1, 2, 3, 5]

The rise of **AI-Powered Attacks** presents a growing challenge in India's cybersecurity landscape.[1, 4, 6, 12] These threats are characterized by their scalability and ability to evade traditional security measures. Attackers are increasingly leveraging open-source AI tools and low-cost cloud computing resources to execute more advanced attacks. This includes the use of AI to craft hyper-personalized phishing emails by analyzing publicly available data, as well as AI-simulated voices mimicking executives to authorize fraudulent transactions. Furthermore, AI-enhanced malware, such as BlackMamba which can dynamically rewrite its code, and polymorphic ransomware, which alters its behavior in real-time, are becoming more prevalent.[1, 4] The emergence of data-centric ransomware, where the focus is on identifying and exfiltrating high-value information rather than just encryption, also signifies the evolving tactics of cybercriminals.[1]

With the increasing adoption of cloud services by Indian businesses, **Cloud-Based Threats** are also on the rise. Reports indicate a significant increase in cloud-based malware detections, accounting for as much as 62% of all detections in one report.[1, 4] Cybercriminals are also misusing popular cloud platforms like Google Drive, Dropbox, and OneDrive, as well as enterprise-focused platforms, to spread malware and conduct phishing schemes.[5] The targeting of collaboration tools like Microsoft Teams further highlights the trend of exploiting trusted digital workspaces for malicious purposes.[5]

Mobile Malware poses a growing threat, particularly to the large base of Android users in India.[3, 5] These threats can lead to the theft of sensitive information, disruption of device functions, and provide hackers with access for further attacks. **Social Engineering** continues to be a significant and effective attack vector, with cybercriminals manipulating human psychology to gain unauthorized access to systems and data.[4, 6, 11] Finally, **Supply Chain Attacks** are an increasing concern, with attackers targeting third-party vendors and open-source libraries to inject malicious code and compromise larger organizations.[1, 4, 12]

4. Government Initiatives and Regulatory Framework

4.1 Investigation of Specific Government Initiatives and Regulations

The Indian government has actively undertaken several initiatives and implemented regulations to bolster the nation's cybersecurity framework. A key piece of legislation is the **Digital Personal Data Protection Act 2023 (DPDPA)**.[1, 12, 13] This act mandates stringent safeguards for AI training datasets, requiring explicit consent for the collection and processing of personal data. It also imposes significant penalties for non-compliance, potentially reaching up to USD 30 million.[1] The DPDPA establishes comprehensive guidelines for data controllers, enforces the implementation of organizational and technical security safeguards, and sets standards aimed at addressing the growing concerns surrounding data security in India's increasingly digital economy.[1] These

measures reflect the government's commitment to aligning India's cybersecurity governance with evolving global standards.

In addition to the DPDPA, the **National Cybersecurity Strategy** has been updated, although specific details of this updated strategy are not extensively covered in the provided snippets.[1, 12, 14, 15, 16, 17] The National Cyber Security Policy 2013 serves as an existing framework, outlining the government's approach to creating a secure cyber ecosystem, enhancing capabilities, strengthening regulatory frameworks, and promoting research and development in cybersecurity.[15, 16, 17, 18] The government's growing prioritization of cybersecurity is further evidenced by the increased budgetary allocation for cybersecurity initiatives and projects in the Union Budget 2025, which has exceeded 1,900 crores, marking an 18% increase compared to the previous budget.[9] This significant financial commitment underscores the government's recognition of the escalating cyber threats and the urgent need to strengthen national cyber defenses.

4.2 Role of CERT-In and the Impact of the Digital Personal Data Protection Act (DPDPA)

The **Indian Computer Emergency Response Team (CERT-In)** serves as the national nodal agency for all matters related to cybersecurity in India.[1, 19, 20, 21, 22] Established in 2004 under the Information Technology Act, CERT-In plays a crucial role in safeguarding India's digital infrastructure, coordinating responses to cybersecurity incidents, and fostering a secure cyber ecosystem.[1, 19, 20, 21] Its responsibilities encompass a wide range of functions, including threat analysis, vulnerability management, and collaboration with both domestic and international stakeholders.[1, 19, 20, 21]

CERT-In mandates the reporting of specific types of high-severity cybersecurity incidents within a strict six-hour timeframe.[1, 11, 23] This requirement is critical for enhancing national situational awareness and enabling timely responses to mitigate the impact of attacks. CERT-In also provides comprehensive incident management support, offering technical assistance, recommending remedial measures, and providing follow-up actions to help organizations contain and recover from cyber incidents.[1, 19, 20] Furthermore, CERT-In actively collaborates with law enforcement agencies to investigate incidents and dismantle malicious infrastructure, as well as with sector-specific regulators to ensure a coordinated approach to cybersecurity across critical sectors.[1, 20] Recognizing the evolving threat landscape, CERT-In has also issued an AI Security Advisory, recommending measures to mitigate the specific risks associated with artificial intelligence.[1]

The **Digital Personal Data Protection Act (DPDPA)** significantly complements CERT-In's operational role by establishing a robust legal framework for data protection, which is a fundamental pillar of cybersecurity.[1] The DPDPA mandates stringent safeguards for AI training datasets, requiring explicit consent for the collection and processing of personal data.[1] It also establishes clear guidelines for data controllers, enforcing the implementation of appropriate organizational and technical safeguards to ensure the security and privacy of personal information.[1] By setting these standards and imposing penalties for non-compliance, the DPDPA drives organizations to prioritize data protection and implement effective security controls, thereby contributing to a more secure digital environment in India.

5. Adoption of Cybersecurity Solutions

5.1 Research on the Adoption Rate of Specific Solutions

The adoption of advanced cybersecurity solutions is gaining momentum in India as organizations recognize the need to enhance their defenses against increasingly sophisticated threats. **Zero-Trust Architecture** is one such model that is gaining traction across Indian organizations.[12] This security paradigm operates on the principle of "never trust, always verify," mandating continuous authentication and authorization for every user and device attempting to access the network, regardless of their location.[12] By implementing zero-trust principles, Indian companies aim to mitigate the risks associated with insider threats, compromised credentials, and the growing prevalence of remote work.[12] A recent PwC India report indicates that 55% of respondents prioritized software-defined perimeter and networking and software-defined access, which are key components of a zero-trust approach.[24] However, the same report notes that only 26% of organizations focused on securing endpoints and identities within their zero-trust strategies.[24] This suggests that while the adoption of zero-trust is increasing, the focus on different aspects of the architecture may vary across organizations.

XDR (Extended Detection and Response) is another category of cybersecurity solutions witnessing growing market traction in India, as highlighted in a DSCI report.[25] Over 60% of surveyed organizations in India have either already invested in or plan to invest in XDR solutions to significantly enhance their overall cybersecurity resilience.[25] This strong interest in XDR reflects the increasing recognition of its value in providing comprehensive threat detection and response capabilities by integrating security data from various sources across the IT environment. Globally, the XDR market is projected to experience substantial growth, with compound annual growth rates (CAGR) estimated at 39.20% between 2025 and 2034 [26], and 38.4% during the forecast period of 2021-2028.[27] This global trend, coupled with the specific adoption interest in India, underscores the growing importance of XDR in the cybersecurity strategies of Indian organizations.

5.2 Factors Driving or Hindering Adoption

Several factors are driving the adoption of advanced cybersecurity solutions like zero-trust and XDR in India. The increasing sophistication of cyber threats is a primary driver, compelling organizations to seek more effective ways to protect their digital assets.[26] The need for enhanced visibility across increasingly complex IT environments is also a significant factor.[28, 29] Additionally, the automation capabilities offered by solutions like XDR are attractive to organizations facing shortages of skilled cybersecurity personnel.[28, 29] The continuous evolution of threats necessitates the adoption of sophisticated solutions that can adapt and respond effectively.[28, 29] The growing adoption of cloud services by Indian businesses is further fueling the demand for cloud-centric security solutions like zero-trust and XDR.[2] Finally, regulatory requirements, such as those outlined in the DPDPA, are also driving organizations to invest in more robust security measures.[30]

Despite these strong drivers, several factors can hinder the adoption of these advanced cybersecurity solutions. The complexity of integrating various existing security tools and data sources into a unified platform can be a significant challenge.[31] The persistent cybersecurity skills gap in India also makes it difficult for organizations to find professionals with the expertise needed to implement and manage these solutions effectively.[31] Cost concerns related to the initial investment and ongoing maintenance can also be a barrier.[32] The inherent complexity of some of these tools and potential integration issues with existing IT infrastructure can further impede adoption.[32] Additionally, there might be a lack of complete understanding among some cybersecurity professionals regarding the fundamental principles and advantages of solutions like XDR, which can slow down their adoption.[33] Overcoming these hurdles will be crucial for Indian organizations to fully leverage the benefits of zero-trust and XDR in strengthening their cybersecurity posture.

6. The Cybersecurity Skills Gap in India

6.1 Exploring the Extent of the Skills Gap and Its Impact

India's cybersecurity sector is currently grappling with a significant cybersecurity skills gap, which poses a considerable challenge to the nation's digital security. Projections indicate a substantial talent shortage, with an estimated 1.5 million unfilled cybersecurity positions expected by 2025.[34] This shortage is not unique to India; a recent World Economic Forum (WEF) report highlighted that the global cybersecurity skills gap expanded by 8% in the past year.[35] The impact of this gap is being felt across organizations, with a significant majority, nearly 60%, of respondents in an ISC2 study agreeing that skills gaps have considerably affected their ability to secure their organization.[36] This lack of skilled professionals can lead to increased operational risks, as organizations struggle to acquire individuals with the necessary defensive capabilities to effectively counter cyber threats.[37, 38] Alarmingly, the ISC2 study also found that organizations experiencing critical cybersecurity skills gaps are almost twice as likely to suffer a material data breach compared to those with no such gaps.[36] This statistic underscores the direct correlation between the skills shortage and the increased risk of successful cyberattacks. Small businesses in India are particularly vulnerable, often facing challenges in affording proper security measures and expertise.[2, 34] Furthermore, reports suggest that only a small percentage of Indian companies allocate more than 10% of their IT budget to cybersecurity, which might be insufficient given the escalating sophistication of threats.[34] The combination of a significant skills gap and potentially underfunded cybersecurity budgets creates a challenging environment for organizations striving to protect their digital assets in India.

6.2 Analysis of Initiatives and Programs Aimed at Addressing the Gap

Recognizing the critical nature of the cybersecurity skills gap, various initiatives and programs are underway in India to address this challenge. Companies across the country are increasingly investing in cybersecurity training and development programs to upskill their existing workforce and prepare for future threats.[34, 38] Industry bodies like NASSCOM project the creation of over a million cybersecurity job opportunities by 2025, indicating a growing focus on building a robust talent

pipeline.[34] Furthermore, there are collaborations between industry and educational institutions to develop specialized training programs aimed at equipping individuals with the specific skills needed in the cybersecurity domain.[1, 34, 38] The government is also playing a role in supporting these efforts, with initiatives focused on capacity building and skill development in cybersecurity. There is also a growing emphasis on skill-based hiring within the cybersecurity industry, with companies increasingly prioritizing practical skills and certifications over traditional academic degrees.[37] This shift can help tap into a wider pool of talent, including individuals with diverse backgrounds and experiences who possess the specific skills required for cybersecurity roles. Upskilling the current IT workforce is also emerging as a popular and effective tactic for organizations to prepare for future cybersecurity challenges.[39] These multifaceted efforts, involving companies, industry associations, educational institutions, and the government, demonstrate a concerted approach to bridging the cybersecurity skills gap in India and building a more resilient digital ecosystem.

7. Impact of Geopolitical Events

The cybersecurity landscape in India is increasingly influenced by global geopolitical events. Recent reports indicate that global geopolitical tensions have significantly impacted the demand for cybersecurity solutions in India.[40, 41] Conflicts involving major global players have led to a heightened sense of cyber threat, prompting Indian businesses and government entities to enhance their cybersecurity frameworks and increase investments in protective measures.[40, 41] This is because geopolitical tensions can often spill over into cyberspace, with nation-states and state-sponsored actors potentially engaging in cyber espionage, sabotage, or influence operations.[42] Critical infrastructure and public utility services can become prime targets in such scenarios.[1, 42]

Furthermore, India's strategic geopolitical location and its involvement in various regional issues can make it an attractive target for state-sponsored cyber operations, mirroring the experiences of other nations in Southeast Asia facing similar geopolitical dynamics.[43] The interconnected nature of the global digital landscape means that geopolitical conflicts occurring in one part of the world can have far-reaching implications for the cybersecurity posture of other nations, including India. Threat actors may exploit global events as opportunities to launch attacks or to obfuscate their origins and activities. Therefore, the ongoing geopolitical climate necessitates a heightened state of vigilance and the development of robust cyber defense mechanisms within India to protect its national interests and digital assets.

8. Future of Cybersecurity in India (Predictions)

The future of cybersecurity in India is projected to be a dynamic and challenging landscape, characterized by a continuous interplay between technological advancements and the evolving tactics of cyber adversaries.[1] Several key trends and predictions are shaping the outlook for 2025 and beyond. The increasing sophistication of threats, particularly those leveraging artificial intelligence, is expected to be a defining characteristic.[1, 12, 34] This includes a rise in AI-driven attacks, with more prevalent use of AI-enhanced malware capable of evading traditional defenses, as well as sophisticated deepfake technologies for social engineering and disinformation campaigns.[1, 12, 34] Data-centric ransomware, where attackers prioritize the exfiltration of high-value information, and supply chain compromises targeting

third-party vendors and open-source components are also anticipated to persist and potentially increase.[1, 12] The healthcare, hospitality, and banking sectors, due to the sensitive and valuable data they handle, are likely to remain prime targets for cybercriminals.[1, 12, 34] With the continued rapid adoption of cloud services across Indian organizations, cloud-based malware detections are expected to rise, accounting for an even larger share of overall threats.[1, 12, 34]

The Zero Trust Architecture security model is predicted to gain more traction as organizations seek to enhance their defenses against both insider and external threats.[12, 34] Biometric authentication methods are also expected to become more integral to cybersecurity strategies, offering a stronger alternative to traditional passwords.[12] Looking further into the future, the potential threat posed by quantum computing to current encryption methods necessitates a proactive approach to developing and implementing quantum-resistant cryptographic algorithms.[12]

Data privacy and regulatory compliance will continue to be a major focus, driven by increasing consumer awareness and evolving legislation like the DPDPA.[12, 34] Finally, the emergence of autonomous systems and the proliferation of IoT devices will likely introduce new vulnerabilities that cybercriminals may exploit, requiring specialized security frameworks.[12] The Indian cybersecurity market itself is projected to experience substantial growth in the coming years, with forecasts suggesting a market size of USD 13.6 billion by 2025 according to one report [12], and another projecting USD 10.90 billion by 2029.[34] This growth reflects the increasing recognition of the importance of cybersecurity in safeguarding India's digital future.

9. Major Cybersecurity Incidents and Breaches

India has experienced several significant cybersecurity incidents and data breaches recently, underscoring the persistent threats facing the nation's digital infrastructure. In May 2024, a major data breach exposed a massive 500 GB of biometric data, including sensitive information such as fingerprints and facial scans.[6] This breach affected a wide range of individuals, including police, military personnel, and public workers involved in the election process. The incident was traced back to unsecured databases managed by ThoughtGreen Technologies and Timing Technologies, highlighting the critical need for robust security measures to protect sensitive biometric data.[6] Furthermore, government reports revealed a concerning four-fold jump in cyber fraud cases in India during FY2024, resulting in substantial financial losses amounting to US$ 20 million (177 crores).[9]

These fraudulent activities encompassed various sophisticated techniques, including deepfake scams, voice cloning scams, and traditional phishing attacks, leading to both financial damage and the loss of important personal data.[9] Looking back slightly further, a notable incident in 2020 involved a ransomware attack that targeted the Maharashtra State Electricity Distribution Company, causing disruptions to their operations.[14] Additionally, over 1.39 million cybersecurity incidents were reported in India during the year 2022, indicating a consistently high level of cyber threat activity.[14]

These recent major incidents serve as stark reminders of the vulnerabilities that exist within India's digital ecosystem and emphasize the urgent need for organizations and government bodies to prioritize and strengthen their cybersecurity defenses.

10. Conclusion

The cybersecurity landscape in India for 2024 and 2025 presents a complex and evolving picture. The analysis reveals several critical trends shaping this environment, most notably the increasing sophistication of cyber threats, particularly those leveraging artificial intelligence, and the persistent challenge of the cybersecurity skills gap. The Indian government has demonstrated a strong commitment to addressing these issues through strategic initiatives and regulatory frameworks, such as the Digital Personal Data Protection Act 2023. Simultaneously, Indian organizations are increasingly adopting advanced security solutions like zero-trust architecture and Extended Detection and Response (XDR) to enhance their defenses, although implementation challenges remain. Geopolitical events continue to exert a significant influence, underscoring the need for a robust national cybersecurity posture. Future predictions point towards an intensification of AI-driven attacks and the continued targeting of critical sectors, while recent major cybersecurity incidents serve as tangible reminders of the risks involved. Addressing these multifaceted challenges requires a systemic and collaborative approach involving organizations, the government, and individuals to build a more resilient and secure digital India.

11. Recommendations

To effectively navigate the evolving cybersecurity landscape in India, the following recommendations are crucial.

For Organizations

- Prioritize the comprehensive implementation of **Zero Trust Architecture** across all IT environments to minimize implicit trust and enhance security.[12]
- Invest in and strategically adopt **XDR (Extended Detection and Response)** solutions to gain unified visibility, improve threat detection accuracy, and accelerate incident response capabilities.[25, 26]
- Develop and rigorously enforce robust **cloud security strategies** that address the unique challenges of securing data and workloads in cloud environments.[1, 4]
- Implement comprehensive and continuous **cybersecurity training and awareness programs** for all employees to address the persistent skills gap and mitigate the risk of social engineering attacks.[34, 44]
- Establish and maintain strong **vendor risk management processes** to thoroughly assess and mitigate cybersecurity risks associated with third-party suppliers and partners.[1, 12]
- Proactively invest in **AI-powered security tools and technologies** to effectively counter the growing threat of AI-driven cyberattacks and enhance overall threat detection capabilities.[1, 12]
- Develop, regularly test, and refine comprehensive **incident response plans** to ensure swift and effective action in the event of a security breach.[12, 34]
- Enhance **data protection measures** in strict adherence to the guidelines and requirements outlined in the Digital Personal Data Protection Act 2023.[1, 13]c
- Increase **cybersecurity budgets** and strategically allocate resources to support the implementation of necessary security controls and the hiring or training of skilled personnel.[9, 45]

For Policymakers and Government Bodies

- Continue to strengthen the existing **regulatory framework** and ensure the effective enforcement of cybersecurity laws and data protection regulations, including the DPDPA.[1, 13]
- Further increase **investment in CERT-In's capabilities and resources** to enhance its ability to respond to national-level cyber incidents, provide timely advisories, and coordinate with various stakeholders.[19, 20]
- Promote and actively support **initiatives aimed at bridging the cybersecurity skills gap** through collaborations with educational institutions, industry associations, and the private sector to develop specialized training programs and certifications.[34, 44]
- Foster greater **public-private partnerships** to facilitate the sharing of threat intelligence, best practices, and resources to collectively strengthen the nation's cyber defenses.[1, 15]
- Enhance **international cooperation** with other nations and cybersecurity agencies to share threat information, coordinate responses to cross-border cyberattacks, and establish global best practices.[1, 20]
- Develop and implement specific **cybersecurity standards and guidelines** tailored to the unique needs and vulnerabilities of critical infrastructure sectors such as energy, finance, and healthcare.[1, 15]
- Launch and support comprehensive **public awareness campaigns** to educate citizens and organizations about prevalent cyber threats, safe online practices, and the importance of cyber hygiene.[19]

Table 1: Common Cybersecurity Threats in India (2024-2025)

Threat Type	Description	Prevalence in India (2024-2025)	Targeted Sectors
Malware	Malicious software designed to harm systems; includes Trojans, Infectors, Worms, Adware, Exploits, Ransomware	High volume of detections (369.01 million in 2024) [3]; Increase in sophisticated, behavior-based malware [1]; Trojans and Infectors most prevalent.[3]	Healthcare, Hospitality, BFSI [1]
Ransomware	Malware that encrypts data or threatens to publish it unless a ransom is paid; increasingly using extortion.	Continued significant threat [1]; Shift towards data extortion tactics.[1]	Healthcare, Hospitality, BFSI [1]
AI-Powered Attacks	Attacks leveraging artificial intelligence for automation, evasion, and sophistication.	Growing challenge [1]; Includes AI-enhanced malware, polymorphic ransomware, and AI-driven phishing/BEC.[1]	Various sectors
Cloud-Based Threats	Threats targeting cloud environments and services.	Rising prevalence; 62% of detections in cloud environments (one report) [1]; Misuse of cloud platforms for malware and phishing.[5]	Businesses increasingly using cloud services
Mobile Malware	Malicious software targeting mobile devices, particularly Android.	Increasing threat [3]; Accounts for a significant percentage of cyberattack detections.[3]	Android users
Social Engineering	Attacks manipulating human behavior to gain access or information.	Remains a significant attack vector [4]; Increasingly sophisticated with AI-driven phishing and deepfakes.[1]	All sectors
Supply Chain Attacks	Attacks targeting organizations through their third-party vendors and suppliers.	Growing concern [1]; Attackers inject malicious code via compromised updates or dependencies.[1]	Organizations with complex supply chains

Table 2: Key Government Initiatives and Regulations Related to Cybersecurity in India

Initiative/Regulation	Description	Key Objectives/Provisions	Impact on Cybersecurity
Digital Personal Data Protection Act 2023 (DPDPA)	Legislation focused on protecting personal data.	Mandates safeguards for AI training data, requires explicit consent for data collection, imposes penalties for non-compliance, establishes guidelines for data controllers.	Strengthens data protection and privacy, drives compliance and investment in security measures.
National Cybersecurity Strategy	Updated government strategy for enhancing national cyber resilience.	Aims to create a secure cyber ecosystem, enhance capabilities, strengthen regulatory frameworks, and promote R&D.	Provides a framework for national-level cybersecurity efforts and coordination.
National Cyber Security Policy 2013	Existing policy framework for cybersecurity.	Emphasizes creating a secure cyber ecosystem, enhancing capacities, strengthening regulations, and promoting R&D.	Provides foundational guidance for cybersecurity efforts in India.
CERT-In (Indian Computer Emergency Response Team)	National nodal agency for responding to cybersecurity incidents.	Safeguarding digital infrastructure, coordinating incident responses, threat analysis, vulnerability management, mandatory incident reporting within 6 hours, provides incident management support.	Central coordinating body for cybersecurity incidents, enhances national cyber resilience.
Union Budget 2025 Allocation	Increased budgetary allocation for cybersecurity initiatives.	Over 1,900 crores allocated, an 18% increase from the previous budget.	Demonstrates government prioritization of cybersecurity and provides funding for initiatives.

Table 3: Adoption Rate of Specific Cybersecurity Solutions in Indian Organizations

Solution Type	Adoption Rate	Key Drivers for Adoption	Key Hindrances to Adoption
Zero-Trust Architecture	55% prioritize network aspects; 26% focus on endpoints [24])	Increasing sophistication of threats [26]; Need for visibility across complex environments [28]; Mitigating insider threats and remote work risks.[12]	Complexity of integration [31]; Skills gap for implementation [31]; Cost concerns.[32]
XDR (Extended Detection and Response)	Over 60% invested or plan to invest [25])	Need for sophisticated solutions [28]; Automation to alleviate personnel shortages [28]; Growing cloud adoption [2]; Regulatory requirements.[30]	Complexity of integration [31]; Skills gap for management [31]; Potential lack of understanding.[33]

Table 4: Cybersecurity Skills Gap in India | Statistics and Initiatives

Metric/Initiative	Details	Source/Context
Projected Unfilled Positions (2025)	1.5 million	[34]
Global Skills Gap Increase (2024)	8%	WEF report [35]
Impact of Skills Gaps on Security	Nearly 60% agree significant impact	ISC2 study [36]
Increased Risk of Material Breach	Twice as likely for enterprises with skills gaps	ISC2 study [36]
Investment in Training	Companies heavily investing	[34]
Projected Job Openings (2025)	Over a million	NASSCOM projections [34]
Skill-Based Hiring	Increasing emphasis	[37]
Upskilling Current Workforce	Popular tactic	[39]

WORKS CITED

1. Chambers and Partners. (2025). *Cybersecurity 2025 – India: Trends and developments.* Retrieved March 31, 2025, from https://practiceguides.chambers.com/practice-guides/cybersecurity-2025/india/trends-and-developments
2. Mordor Intelligence. (2025). *Cybersecurity market in India – Size & growth.* Retrieved March 31, 2025, from https://www.mordorintelligence.com/industry-reports/india-cybersecurity-market
3. Data Security Council of India (DSCI). (2025). *India Cyber Threat Report 2025.* Retrieved March 31, 2025, from https://www.dsci.in/resource/content/india-cyber-threat-report-2025
4. Seqrite. (2025). *India Cyber Threat Report 2025.* Retrieved March 31, 2025, from https://www.seqrite.com/india-cyber-threat-report-2025/
5. Entrepreneur India. (2025). *Malware on the rise: India's cybersecurity outlook for 2025.* Retrieved March 31, 2025, from https://www.entrepreneur.com/en-in/news-and-trends/malware-on-the-rise-indias-cybersecurity-outlook-for-2025/483901
6. Economic Times – CISO. (2025). *Check Point's 2025 security report shows 44% rise in cyberattacks.* Retrieved March 31, 2025, from https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/check-point-softwares-2025-security-report-finds-alarming-44-increase-in-cyber-attacks-amid-maturing-cyber-threat-ecosystem/117508679
7. GlobeNewswire. (2025). *Check Point Software's 2025 security report finds alarming 44% increase in cyber-attacks.* Retrieved March 31, 2025, from https://www.globenewswire.com/news-release/2025/01/14/3009378/0/en/Check-Point-Software-s-2025-Security-Report-Finds-Alarming-44-Increase-in-Cyber-Attacks-Amid-Maturing-Cyber-Threat-Ecosystem.html
8. SecurityBrief Australia. (2025). *Check Point report reveals 44% rise in cyber-attacks.* Retrieved March 31, 2025, from https://securitybrief.com.au/story/check-point-report-reveals-44-rise-in-cyber-attacks
9. SMEStreet. (2025). *Palo Alto Networks releases 2025 Unit 42 Cybersecurity Report.* Retrieved March 31, 2025, from https://smestreet.in/technology/palo-alto-networks-releases-2025-unit-42-cybersecurity-report-8896243
10. Palo Alto Networks. (2025). *2025 Unit 42 Global Incident Response Report.* Retrieved March 31, 2025, from https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report
11. Cybersecurity Asia. (2024). *Indian industry cybersecurity report 2024: Trends and insights.* Retrieved March 31, 2025, from https://cybersecurityasia.net/indian-cybersecurity-report-2024/
12. Sattrix. (2025). *13 game-changing cybersecurity trends in India for 2025.* Retrieved March 31, 2025, from https://www.sattrix.com/blog/2025-cybersecurity-trends-india-to-watch/
13. KPMG International. (2025). *Cyber security – India.* Retrieved March 31, 2025, from https://kpmg.com/in/en/services/advisory/consulting/cyber-security.html
14. NASSCOM. (2025). *Cybersecurity strategies for India with Vinayak Godse, CEO DSCI.* Retrieved March 31, 2025, from https://nasscom.in/voices/cybersecurity-strategies-india-vinayak-godse-ceo-dsci
15. RSM Global. (2025). *India's cybersecurity policy frameworks: Key strategies and initiatives.* Retrieved March 31, 2025, from https://www.rsm.global/india/insights/consulting-insights/cybersecurity-policy-frameworks
16. Ministry of Electronics & Information Technology (MeitY). (2013). *National Cyber Security Policy 2013.* Retrieved March 31, 2025, from https://www.meity.gov.in/static/uploads/2024/02/National_cyber_security_policy-2013_0.pdf
17. Centre for International Governance Innovation (CIGI). (2025). *India can be a pivotal player in stronger cybersecurity.* Retrieved March 31, 2025, from https://www.cigionline.org/articles/india-can-be-a-pivotal-player-in-stonger-cybersecurity/
18. NPS Trust. (2023). *Information and cyber security policy 2023.* Retrieved March 31, 2025, from https://npstrust.org.in/sites/default/files/inline-files/ICS_Policy_2023-NPS_Trust.pdf
19. Press Information Bureau (PIB). (2025). *The Indian Computer Emergency Response Team (CERT-In).* Retrieved March 31, 2025, from https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2109192
20. India Law. (2025). *CERT-In: India's cybersecurity response framework explained.* Retrieved March 31, 2025, from https://www.indialaw.in/blog/civil/cert-in-india-cybersecurity-framework/
21. PwC India. (2025). *Navigating the cyber pass.* Retrieved March 31, 2025, from https://www.pwc.in/research-and-insights-hub/navigating-the-cyber-pass.html
22. PwC India. (2024). *Digital Trust Insights 2024.* Retrieved March 31, 2025, from https://www.pwc.in/press-releases/2023/99-of-organisations-will-increase-their-cyber-budgets-out-of-which-50-envisaged-an-increase-between-6-and-15-in-the-next-12-months-pwcs-2024-digital-trust-insights.html
23. BreachRx. (2025). *India's CERT-In directive.* Retrieved March 31, 2025, from https://www.breachrx.com/global-regulations-data-privacy-laws/india-cert-in-directive/
24. PwC India. (2024). *Cybersecurity in India: Global Digital Trust Insights Survey.* Retrieved March 31, 2025, from https://www.pwc.in/digital-trust-insights-india.html
25. Data Security Council of India (DSCI). (2023). *India cybersecurity domestic market 2023 report.* Retrieved March 31, 2025, from https://www.dsci.in/files/content/knowledge-centre/2023/India%20Cybersecurity%20Domestic%20Market%202023%20Report.pdf
26. Market Research Future. (2025). *Extended detection and response market size and trends – 2034.* Retrieved March 31, 2025, from https://www.marketresearchfuture.com/reports/extended-detection-response-market-12210
27. Adroit Market Research. (2025). *XDR market trends and growth drivers.* Retrieved March 31, 2025, from https://www.adroitmarketresearch.com/industry-reports/xdr-market
28. GlobeNewswire. (2025). *Extended detection and response (XDR) global markets 2024–2027.* Retrieved March 31, 2025, from https://www.globenewswire.com/news-release/2025/02/26/3033119/28124/en/Extended-Detection-and-Response-XDR-Global-Markets-2024-2027-Leveraging-New-Capabilities-to-Expand-Across-Regions-and-Maturity-Levels-Developing-New-Technology-Detections-and-Intel.html

29. Business Wire. (2025). *Extended detection and response (XDR) global market forecasts 2024–2027.* Retrieved March 31, 2025, from https://www.businesswire.com/news/home/20250303595398/en/Extended-Detection-and-Response-XDR-Global-Market-Forecasts-2024-2025-2027-AI-Advancements-Third-party-Integration-and-a-Proactive-Approach-to-Security-Fueling-Opportunities---ResearchAndMarkets.com
30. PwC India. (2024). *Digital Trust Insights 2025.* Retrieved March 31, 2025, from https://www.pwc.in/press-releases/2024/93-of-indian-executives-anticipate-a-cyber-budget-increase-next-year-74-of-cxos-strengthening-their-cybersecurity-posture-due-to-regulatory-expectations-pwc-india-digital-trust-insights-2025.html
31. SecuritySenses. (2024). *2024 outlook for XDR: Emerging trends and key challenges.* Retrieved March 31, 2025, from https://securitysenses.com/posts/2024-outlook-xdr-emerging-trends-and-key-challenges
32. Rossum.ai. (2025). *2025 automation statistics that'll upset the finance applecart.* Retrieved March 31, 2025, from https://rossum.ai/blog/automation-statistics-that-will-upset-the-finance-applecart/
33. MarketsandMarkets. (2025). *Extended detection and response market size, latest trends & growth drivers.* Retrieved March 31, 2025, from https://www.marketsandmarkets.com/Market-Reports/extended-detection-response-market-52119574.html
34. Nucamp. (2025). *India cybersecurity job market: Trends and growth areas for 2025.* Retrieved March 31, 2025, from https://www.nucamp.co/blog/coding-bootcamp-india-ind-india-cybersecurity-job-market-trends-and-growth-areas-for-2025
35. Barracuda Networks Blog. (2025). *Cybersecurity skills gap widens again.* Retrieved March 31, 2025, from https://blog.barracuda.com/2025/01/27/cybersecurity-skills-gap-widens-again
36. ISC2. (2024). *2024 ISC2 cybersecurity workforce study.* Retrieved March 31, 2025, from https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study
37. Hack The Box. (2025). *5 critical cybersecurity skills gap trends for 2025.* Retrieved March 31, 2025, from https://www.hackthebox.com/blog/cybersecurity-skills-gap-trends-2025
38. Nucamp. (2025). *Thailand cybersecurity job market: Trends and growth areas for 2025.* Retrieved March 31, 2025, from https://www.nucamp.co/blog/coding-bootcamp-thailand-tha-thailand-cybersecurity-job-market-trends-and-growth-areas-for-2025
39. EY India. (2025). *Cyber and privacy leaders' agenda.* Retrieved March 31, 2025, from https://www.ey.com/en_in/ciso
40. ReportLinker. (2024). *India cybersecurity market report – Q4 2024.* Retrieved March 31, 2025, from https://www.reportlinker.com/dlp/6527f4f82d6f765d670c882b363dc80d
41. World Economic Forum. (2025). *Biggest cybersecurity threats of 2025.* Retrieved March 31, 2025, from https://www.weforum.org/stories/2025/02/biggest-cybersecurity-threats-2025/
42. Threat Intelligence. (2025). *Beyond the horizon: What lies ahead in 2025 for cybersecurity?* Retrieved March 31, 2025, from https://www.threatintelligence.com/blog/2025-cybersecurity-trends
43. Cyfirma. (2025). *The changing cyber threat landscape – Southeast Asia.* Retrieved March 31, 2025, from https://www.cyfirma.com/research/the-changing-cyber-threat-landscape-southeast-asia-2/
44. EY India. (2025). *Cybersecurity.* Retrieved March 31, 2025, from https://www.ey.com/en_in/industries/tmt/cybersecurity
45. MediaBrief. (2025). *Palo Alto Networks survey: 75% of Indian organizations increased cybersecurity budgets in 2023 compared to 2022.* Retrieved March 31, 2025, from https://mediabrief.com/palo-alto-networks-survey-75-of-indian-organizations-increased-cybersecurity-budgets-in-2023-compared-to-2022/