LEX LUMEN RESEARCH JOURNAL- ISSN:3048-8702(O)
Volume 1, Issue 3, Pages:155-186, April 2025

INVESTMENT AND GROWTH OF CYBERSECURITY IN INDIA AND USA: A COMPARATIVE STUDY

By- Manas Rai[1] & Dr. Anumeha Sahai[2]

ABSTRACT

Increased cyber threats, legal frameworks, and technological breakthroughs have all contributed to the rise in cybersecurity spending brought about by our increased reliance on digital infrastructure. Globally, businesses are giving cybersecurity top priority in order to safeguard confidential information, reduce financial losses, and maintain corporate operations. By examining important investment trends, the use of artificial intelligence in threat detection, and the financial effects of cybersecurity funding, this study investigates the explosive expansion of the cybersecurity industry. In order to improve digital defences, it also looks at company strategy, industry partnerships, and government regulations. The study emphasizes how more cybersecurity investment promotes innovation in security solutions while also strengthening organizational resilience. Additionally, it emphasizes the rising demand for skilled cybersecurity professionals and the challenges in bridging the talent gap. Through an analysis of global cybersecurity investment trends, this study highlights the vital necessity of ongoing developments and calculated financial commitments to effectively combat changing cyberthreats.

KEYWORDS: Cybersecurity Investment, Digital Infrastructure Protection, Cyber Threats, Government Policies, Artificial Intelligence, and Economic Impact

[1] Student, Amity University, Noida,
[2] Assistant Professor, Amity University, Noida

METHODOLOGY

To examine investment trends, a qualitative approach is used, combining secondary data from industry white papers, government publications, and financial filings. Furthermore, statistical research and case studies shed light on the financial effects of cybersecurity investment. The report also assesses how emerging technologies, such as artificial intelligence, corporate strategies, and policy frameworks can improve cybersecurity resilience. A thorough grasp of cybersecurity investments and their effects on company and national security is ensured by this methodical approach.

1. LAWS PERMITS THE FUNDING

1.1 INDIAN LAWS

Significant legislation that establishes a strong legal framework for overseeing the Indian securities market is the Securities and Exchange Board of India (SEBI) Act, 1992. The Act, which was passed in order to protect investor interests and maintain market integrity, designates SEBI as the main regulatory body in charge of regulating stock exchanges, investment firms, and market intermediaries. The statute improves financial transparency and accountability by granting SEBI broad powers such as rule-making, investigation, and enforcement. By addressing important issues like corporate disclosures, insider trading, and fraudulent activities, the Act boosts investor confidence. India's capital markets have grown more effective and competitive on a global scale thanks in large part to SEBI's contributions over the years.

According to recent information from the Data Security Council of India, the Securities Exchange Board of India (SEBI) established a comprehensive regulatory approach to protecting digital infrastructure across SEBI-regulated entities (REs) on August 20, 2024,

by introducing the Cyber Security and Cyber Resilience Framework (CSCRF) under section 11(1) of the [3]SEBI Act. In accordance with international best practices, this framework strengthens cyber resilience by requiring strict security controls, risk assessment procedures, and incident response systems. SEBI makes sure that the framework balances the strict requirements of cyber security with the flexibility of business operations by incorporating stakeholder feedback. Understanding the increasing cyberthreats in financial markets, the framework emphasizes the necessity of ongoing monitoring, proactive defense tactics, and regular compliance reporting. Applauding SEBI's initiative, the Data Security Council of India (DSCI) highlights the agency's role in creating a robust, risk-aware financial ecosystem that can adjust to changing cyberthreats.

In order to create a framework that successfully strikes a balance between the necessity of cyber security and resilience and the operational flexibility of market participants, SEBI has actively collaborated with important stakeholders and taken industry input into consideration. SEBI's strategy has been praised by the Data Security Council of India (DSCI), which acknowledges its attempts to incorporate industry-specific issues with global best practices. Additionally, this framework emphasizes the importance of board-level oversight in cyber governance by requiring senior management to be accountable for the implementation of cyber security measures. To improve resilience, it promotes the use of blockchain-based security protocols and artificial intelligence (AI)-driven threat intelligence. SEBI's initiative strengthens India's financial sector against cyber vulnerabilities while promoting a more robust and secure digital financial ecosystem by giving priority to risk-based controls, information-sharing mechanisms, and cooperative cyber defence strategies.

[3] THE SECURITIES AND EXCHANGE BOARD OF INDIA ACT, 1992, NO. 15, Acts of Parliament, 1992 (India).

The business has also shed light on SEBI's efforts by offering regulatory forbearance and extending compliance deadlines to address industry concerns. SEBI's dedication to a balanced regulatory approach is demonstrated by these clarifications, which come in response to stakeholder inquiries following the framework's launch in August 2024. CSCRF's main goal is to make sure SEBI-regulated entities (REs) have a robust cybersecurity infrastructure that can successfully stop, identify, and lessen cyberthreats. According to SEBI's most recent circular, compliance requirements were originally scheduled to take effect on January 1, 2025, but regulatory forbearance has been granted until March 31, 2025. Furthermore, the deadline for KYC registration agencies and depository participants has been extended to April 1, 2025, in response to industry feedback on the rationalization of these entities.

Furthermore, in order to conduct additional consultations before finalizing these rules, SEBI has temporarily postponed the implementation of data localization standards within the framework. This ruling demonstrates SEBI's flexible regulatory approach, which makes sure that compliance standards match industry capacities and changing technology environments. In order to give market players more time to get ready for implementation, the data security standards—which are an essential part of the framework—will be announced later. By adopting a consultative approach, SEBI emphasizes the necessity of a systematic, risk-based approach to cyber resilience while acknowledging the complexity of cybersecurity regulation in a dynamic financial environment.

In Aug 29, 2023 the SEBI have introduced [4]Guidelines for MIIs regarding Cyber security and Cyber resilience whereby SEBI recognized the vital role that Market Infrastructure

[4] SEBI, *Guidelines for MIIS | Circular No.: SEBI/HO/MRD/TPD/P/CIR/2023/146* (Aug 29, 2023), https://www.sebi.gov.in/legal/circulars/aug-2023/guidelines-for-miis-regarding-cyber-security-and-cyber-resilience_76056.html.

Institutions (MIIs) play in preserving the integrity and stability of the securities market and sought to strengthen the cybersecurity and cyber resilience framework for MIIs. SEBI stresses the need for implementing sophisticated security measures, real-time threat monitoring, and strong incident response procedures due to the growing interconnection of MIIs. In the case of a cyberattack, MIIs make sure that preconfigured "gold images" are available to quickly restore operations, test system recovery capabilities on a regular basis, and keep encrypted offline backups. To combat possible risks like ransomware assaults, MIIs are also encouraged to keep extra hardware on hand, practice business continuity frequently, and strengthen endpoint security.

SEBI mandates that MIIs put in place a structured cybersecurity governance strategy that includes endpoint protection mechanisms, email security filters, and user awareness campaigns in order to further reduce cyber risks. To reduce their vulnerability to cyberattacks, these organizations need to implement privileged identity management systems, least privilege access controls, and multi-factor authentication. The recommendations also highlight improvements to network security, such as stringent API access controls, segmentation tactics, and DNS filtering. SEBI emphasizes the importance of regular security audits, Active Directory penetration testing, and keeping an eye out for possible dark web data leaks. In order to ensure prompt compliance with changing risks, MIIs must also connect their cybersecurity frameworks with alerts provided by CERT-In and other regulatory agencies.

1.2 UNITED STATE OF AMERICA

Investor protection, market equity, and capital formation are all ensured by the U.S. Securities and Exchange Commission (SEC), the main regulatory agency in charge of the

country's securities markets. [5]The Securities Exchange Act of 1934 created the SEC, which oversees corporate disclosures to stop insider trading and fraud, controls stock exchanges, and enforces securities laws. In order to help investors make wise judgments, it requires publicly traded corporations to submit transparent financial reports. In order to preserve market integrity, the SEC also regulates brokers, mutual funds, and investment counsellors. Emerging financial concerns, including cyber hazards, are addressed by the SEC through the implementation of cybersecurity frameworks and risk management rules. The SEC consistently adjusts to changing financial markets through enforcement actions, regulation changes, and technology breakthroughs, fostering investor confidence and economic stability.

The U.S. Securities and Exchange Commission (SEC) has established the [6]Cyber and Emerging Technologies Unit (CETU) to combat wrongdoing related to cyberspace and shield individual investors from deceptive practices in the quickly changing technology industry. Under the direction of Laura D'Allaird, CETU will take the place of the Crypto Assets and Cyber Unit. It will include about 30 fraud experts and lawyers spread throughout several SEC locations. The SEC's dedication to modifying regulatory enforcement to combat financial crimes made possible by evolving technologies is demonstrated by this endeavor. Acting Chairman Mark T. Uyeda stressed that by eradicating dishonest activities, the new unit will not only protect investors but also advance market efficiency and encourage responsible innovation. To guarantee a more thorough approach to cybersecurity and technology fraud enforcement, CETU will collaborate with the Crypto Task Force, which is chaired by Commissioner Hester Peirce.

[5] Securities Exchange Act, 15 U.S.C. (1934).
[6] Laura D'Allaird, *Cyber and Emerging Technologies Unit (CETU)* (Feb 20,2025) https://www.sec.gov/newsroom/press-releases/2025-42.

By utilizing its team's proficiency in cybersecurity and financial technology, CETU will concentrate on a wide range of cyber-related securities fraud. Cyber intrusions intended to steal material nonpublic information and fraudulent schemes that use social media, the dark web, and artificial intelligence to deceive investors are important enforcement areas. The section will also deal with fraud involving blockchain technology and cryptocurrency assets, account takeovers that impact retail investors, and regulated organizations' noncompliance with cybersecurity regulations. To provide more accountability and transparency, CETU will also closely examine public issuers for making false disclosures about cybersecurity threats. In order to preserve investor confidence and create a safe environment for technical improvements in the securities sector, CETU actively detects and mitigates cyber risks in the financial markets.

The U.S. Securities and Exchange Commission (SEC) has introduced the [7]Draft 2024 Cybersecurity Disclosure (CYD) Taxonomy as part of its larger initiatives to improve cybersecurity reporting's uniformity and openness. In accordance with recently enacted rules, registrants must report on their cybersecurity risk management, strategy, and governance every year and disclose significant cybersecurity events. In order to provide organized and machine-readable cybersecurity disclosures, the SEC requires the use of Inline extensible Business Reporting Language (XBRL). By outlining the precise components required for labeling cybersecurity-related data, the CYD taxonomy enables more uniform and effective reporting across businesses. The SEC hopes to strengthen corporate accountability in managing cyber risks within financial markets and enhance investor access to vital cybersecurity information by putting in place a uniform taxonomy.

[7] Announcement, [7]*Draft 2024 Cybersecurity Disclosure (CYD) Taxonomy* (Jun 24,2024), https://www.sec.gov/newsroom/whats-new/2406-draft-2024-cyd-taxonomy.

A public review of the CYD taxonomy draft has been released, and interested parties are urged to submit comments by the deadline of August 23, 2024. The subject line of the email that the SEC is using to solicit feedback must be "Draft 2024 CYD Taxonomy." The SEC's dedication to improving disclosure standards in cooperation with investors, industry players, and regulatory specialists is reflected in this collaborative approach. It is anticipated that the taxonomy will improve regulatory oversight, boost market efficiency, and facilitate data-driven risk management decision-making by incorporating structured data reporting into cybersecurity disclosures. Adopting XBRL tagging enhances the SEC's larger effort to match cybersecurity governance with changing financial and technical environments in addition to facilitating increased transparency.

The most propounded company of USA called "WINDHAM BRANNON" posted on 11th Oct 2023, that the Securities and Exchange Commission (SEC) has [8]proposed a new cybersecurity risk management regulation that requires investment funds and advisers to put in place thorough procedures to reduce cybersecurity risks. The rule requires written cybersecurity policies and procedures that address incident response, information protection, user access controls, and risk assessments. The SEC emphasizes the significance of strong security procedures to protect sensitive investor data and preserve market stability in view of the rising frequency of cyberattacks that target financial institutions. The plan requires companies to evaluate and reduce cybersecurity risks, put security controls in place, and notify the SEC of major cybersecurity occurrences as soon as possible—within 48 hours of confirmation. In order to ensure accountability and regulatory compliance in the ever-changing threat landscape, advisers and funds must also

[8] DEAN FLORES, *The SEC's Proposed Rule: Cybersecurity Risk Management for Investment Advisers and Funds* (Oct 11, 2023), https://windhambrannon.com/blog/sec-cybersecurity-investment-funds/.

keep thorough cybersecurity records, including incident reports and recurring risk assessments.

Investment advisers and funds handle so much sensitive financial data, cybersecurity risk management has become a top issue. The need for proactive security measures is highlighted by the fact that cyber incidents can result in identity theft, fraud, operational disruptions, and reputational harm. Formal security policies, incident response plans, risk assessments, and business continuity plans are all essential components of a strong cybersecurity program. Businesses getting ready for the proposed rule's finalization should hire cybersecurity experts to conduct assessments, implement industry-accepted frameworks such as NIST CSF, and set up explicit security procedures. Businesses can better meet regulatory requirements by putting in place a systematic remediation strategy and ongoing cybersecurity monitoring.

1.3 JUDGMENT

The Cybercrime recently enshrined by the Apex Court at para 255, [9]Rule 11 of the Protection of Children from Sexual Offences Rules, 2020 ("POCSO Rules") to report POCSO offences to the Special Juvenile Police Unit, local police, or cybercrime portal, along with pertinent information, including the source. Social media intermediaries are required to report child abuse instances under a Memorandum of Understanding (MoU) between the National Crime Records Bureau (NCRB) and the National Centre for Missing & Exploited Children (NCMEC), which is situated in the United States. These reports are sent by NCMEC to NCRB, which uses the national cybercrime reporting system to notify the appropriate State authorities.

[9] Just Rights for Children Alliance v. S. Harish, 2024 S.C.C. OnLine S.C. 2611 (India).

2. INVESTING IN NATIONAL SECURITY

2.1 INDIA

Recognizing its vital role in protecting financial institutions, digital infrastructure, and citizen data, India has taken a multifaceted approach to investing in national cybersecurity. The government has strengthened organizations like the National Critical Information Infrastructure Protection Centre (NCIIPC) and the Indian Computer Emergency Response Team (CERT-In) by greatly increasing budgetary allocations for cybersecurity activities. Enhancing resilience against cyber threats while maintaining data privacy is the goal of laws like the Digital Personal Data Protection Act and the National Cyber Security Strategy. To support national defence systems, India also encourages cybersecurity talent development, public-private collaborations, and domestic technology research. In order to safeguard its digital economy, encourage innovation, and position itself as a global leader in cyber defense, India is giving cybersecurity investments top priority in light of the mounting risks posed by financial fraud, cyberwarfare, and digital espionage.

In 2013 Ministry of electronics and information technology came up with [10]India's National Cyber Security Policy (NCSP) 2013 as an all-encompassing framework for protecting the nation's cyberspace, acknowledging the expanding complexity of digital infrastructure and the mounting dangers of cyberattacks. The strategy lays out important goals like improving cyber resilience, creating a secure IT ecosystem, and fortifying the protection of essential information infrastructure, all with the goal of creating a safe and resilient cyberspace for people, companies, and the government. It requires that a National Critical Information Infrastructure Protection Centre (NCIIPC) be established around-the-

[10] Ministry of electronics and information technology, *Policy of 2013 on national cyber security*, https://www.meity.gov.in/static/uploads/2024/02/National_cyber_security_policy-2013_0.pdf.

clock to supervise cybersecurity in vital industries. The policy also highlights capacity-building programs, incentives for companies to implement optimal security practices, and domestic cybersecurity research and development. The NCSP seeks to establish a cooperative public-private cybersecurity framework that conforms to international security norms, acknowledging the dynamic nature of cyberthreats.

Additionally, the policy places a high priority on regulatory improvements, encouraging a flexible legislative framework to handle cybersecurity issues brought on by new technologies like social media, cloud computing, and encrypted services. It emphasizes the necessity of risk assessments, cybersecurity audits, and the application of internationally accepted security standards like ISO 27001, among others. Within five years, the government wants to train 500,000 cybersecurity workers, making human resource development a top priority. Through bilateral and multinational collaborations, the policy promotes global cooperation and fortifies cybersecurity information-sharing systems. implementing open technology standards and preparing for business continuity in order to be cyber resilient.

The Business-standard articled with make cybersecurity national mission, become leader in efforts, dated 5th Dec 2024, [11]where Innovative digital public infrastructure, a flourishing technology economy, and widespread technology use have all contributed to India's rapid digital transformation during the past ten years. The nation's digital footprint has grown dramatically as digital services are becoming the foundation of economic inclusiveness, public service delivery, and national defense modernization. A strong cybersecurity framework that protects vital infrastructure, such as electricity grids, transportation

[11] Pramod Bhasin/ Vinayak Godse, *India should make cybersecurity national mission, become leader in efforts*, BUSINESS-STANDARD, Dec 05, 2024.

networks, and banking systems, is essential to the development of India's digital economy and its "Viksit Bharat" agenda. A proactive cybersecurity strategy is necessary to ensure national security in light of the growing threat of cyberattacks, which are frequently planned by both state and non-state actors. Cybersecurity is a key component of India's larger national security agenda since attackers using espionage techniques can have serious geopolitical and economic repercussions.

India has taken a mission-driven strategy similar to its National Quantum Mission, India AI Mission, and India Semiconductor Mission in recognition of the importance of cybersecurity to technological growth and economic resiliency. Enhancing cybersecurity necessitates making strategic investments in innovation, governance, and the growth of the industrial ecosystem. This will open doors for high-end service exports, cybersecurity entrepreneurship, and foreign investment. India's cybersecurity architecture has been significantly shaped over the last 20 years by the Ministry of Electronics and IT through financing for research, emergency response programs, regulatory frameworks, and policy interventions. Cybersecurity governance has been further strengthened with the creation of the Indian Cyber Crime Coordination Centre and the National Security Council Secretariat under the Ministry of Home Affairs.

The blogging platform of 'Fortune' posted on 1st Feb 2025 about the [12]Union Budget 2025 increasing dedication to cybersecurity as a cornerstone of the country's digital economy is highlighted. This budget, which includes an allocation of more than ₹1,600 crore, shows a calculated approach to bolstering India's cyber resilience against emerging threats. A proactive approach to bolstering digital infrastructure is indicated by the nearly twofold

[12] DEEPA SESHADRI, *Budget 2025: Government's Push for Cybersecurity in the Digital Economy* (Feb 1, 2025), https://www.fortuneindia.com/budget/budget-2025-governments-push-for-cybersecurity-in-the-digital-economy/120293.

rise in capital investment of ₹759 crore in cybersecurity initiatives, compared to ₹400 crore in 2023. The government's emphasis on incident response and threat mitigation is demonstrated by the ₹238 crore allotted to the Indian Computer Emergency Response Team (CERT-In), up from ₹208 crore the year before. Additionally, with ₹52.8 crore in support, specialist cybersecurity programs for women and children seek to address risks in the growing digital ecosystem, guaranteeing that cybersecurity continues to be a comprehensive and inclusive national priority.

Apart from these targeted investments, the government has increased the amount of money allocated to the National Mission on Interdisciplinary Cyber-Physical Systems from ₹435 crore in 2023 to ₹564.46 crore. This program is essential for promoting innovation at the nexus of critical infrastructure protection, artificial intelligence, and cybersecurity. India's desire to become a leader in cybersecurity research and development as well as to bolster its cyber defences is demonstrated by the increased financial commitment. Maintaining a strong cybersecurity framework is essential for protecting citizen data, national security, and economic advancement as digital adoption speeds up across industries.

The spread of articles also enshrined with one of the insights made by Businessworld posted recently on [13]12th March 2025, India's increasing emphasis on drone technology is a reflection of its strategic goal of promoting economic growth and bolstering national security. Major General CS Mann, AVSM, VSM, emphasized the revolutionary importance of drones in contemporary warfare at PHDCCI's Bharat Drone Manthan 2.0, pointing to their success in the conflict between Russia and Ukraine. Drones are essential for defense operations because of their unparalleled capabilities in targeted assaults,

[13] Sangeet Kumar Sanu, *India Must Strengthen Drone Capabilities for National Security & Development: Experts*, BW BUSINESSWORLD, March 12, 2025.

counterterrorism, and counterinsurgency. Operational concerns, however, include issues like poor battery performance in high-altitude areas. India must make investments in the indigenization of drone technologies, improving manufacturing capacities, and implementing counter-drone measures in order to allay these worries. To enhance India's drone ecosystem, cooperation between the public and business sectors is essential.

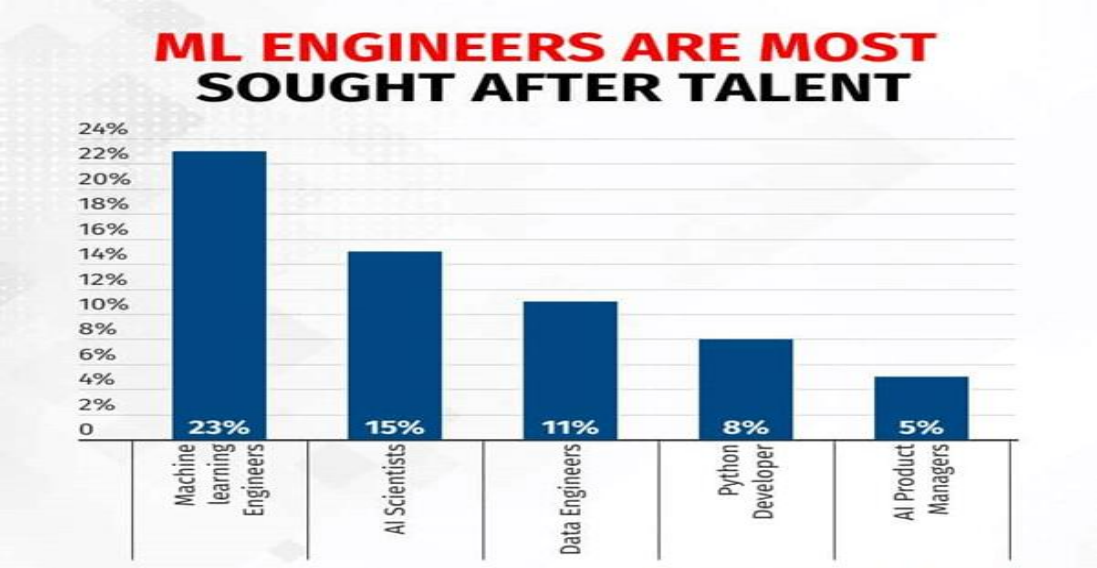
Drones have enormous potential to boost economic growth in a variety of industries outside of defense. The Ministry of Civil Aviation's Senior Economic Advisor, Piyush Srivastava, highlighted programs like "Drone Didi," which empowers women and increases agricultural productivity. Additionally, drones are essential for disaster management, infrastructure monitoring, and land mapping. Adoption in the private sector is still sluggish despite these benefits, necessitating regulatory clarification and assistance with compliance. Manish Pande of the Quality Council of India emphasized the significance of cybersecurity frameworks and quality standards, while former Defense Secretary Shekhar Dutt emphasized the necessity for stronger controls on tiny drones to prevent misuse. The CEO of PHDCCI, Ranjeet Mehta, emphasized the use of drones in precision agriculture, logistics, and India's startup ecosystem.

Also, the Boston Institute of Analytics, USA encumbered the [14]India’s The Union Budget 2025 highlights the government's dedication to technological innovation and marks a revolutionary turn toward bolstering the nation's artificial intelligence (AI) and data science ecosystem. The India AI Mission, which intends to improve AI infrastructure, speed up research and development, and promote AI applications across many industries, is a major focus of this budget. The need for qualified workers is growing along with AI

[14] Boston Institute of Analytics February, *Budget 2025: How India’s AI and Data Science Push is Defining the Future of Technology* (February 7, 2025), https://bostoninstituteofanalytics.org/blog/budget-2025-how-indias-ai-and-data-science-push-is-defining-the-future-of-technology/.

use; in India, job postings for AI and machine learning (ML) have increased by 38%. With 4.1% of AI/ML-related job postings, India notably leads the world, highlighting its developing position as a major participant in the global AI ecosystem.

The need for AI and data science professionals is on the rise.



Specialized education and training programs are becoming crucial to address the growing demand for data science and AI competence. With courses in machine learning, statistical analysis, and data visualization that are relevant to the business, organizations like the Boston Institute of Analytics (BIA) are essential in training workers for careers in artificial intelligence. Learners are given the tools they need to succeed in an AI-driven economy through practical instruction and real-world case studies. The future of AI and data science will be greatly influenced by the cooperation of government regulations, business partnerships, and academic institutions as India establishes itself as a global leader in technology. This strategic effort strengthens India's competitiveness in the rapidly changing digital landscape while also advancing the country's technological capabilities.

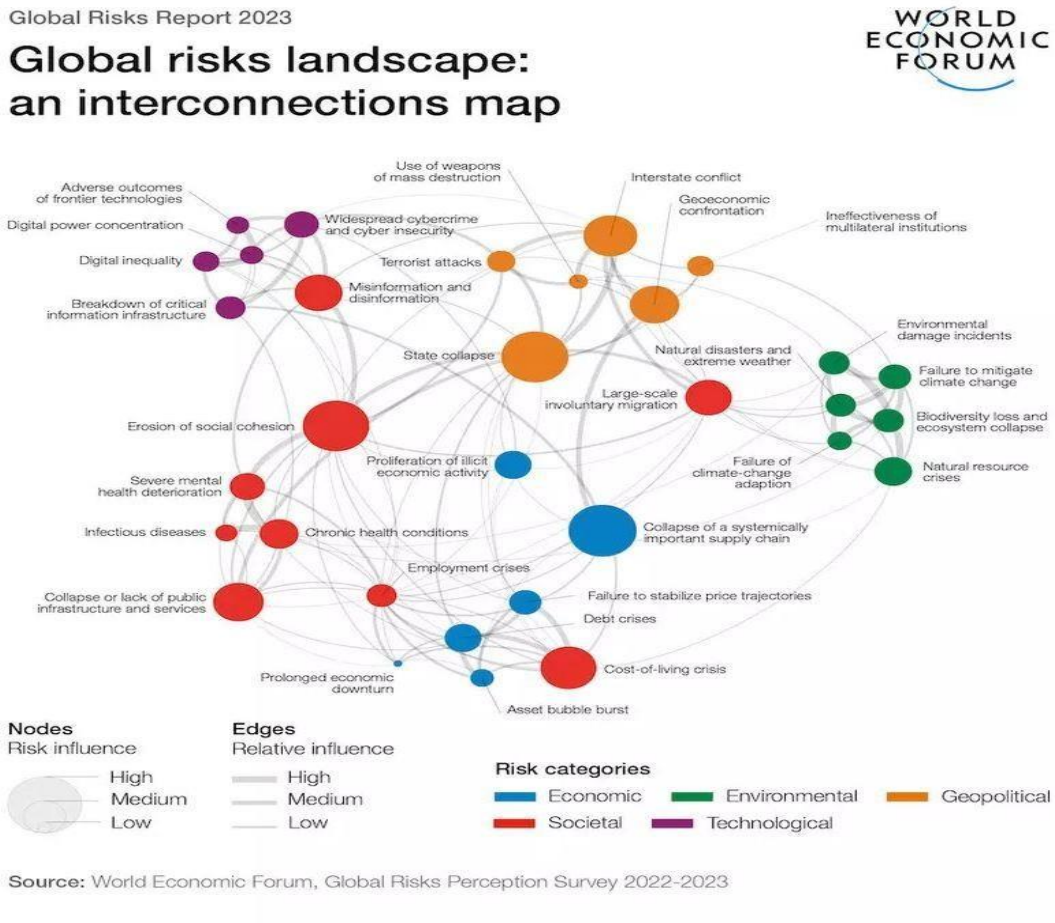
2.2 UNITED STATES OF AMERICA

The United States has established a comprehensive International Cyberspace & Digital Policy Strategy to promote a secure, open, and resilient digital ecosystem while strengthening global partnerships in cyberspace. [15]The order to confront cyber threats, improve digital governance, and combat cybercrime, the plan emphasizes cooperation with allies, private sector players, and civil society. It is in line with the National Security plan (NSS) and the 2023 National Cybersecurity Strategy (NCS). Digital solidarity, which encourages collaboration between countries to advance technological innovation, protect digital rights, and strengthen cybersecurity resilience, is a fundamental component of the plan. The United States is dedicated to upholding democratic, human rights, and legal norms while combating the abuse of digital tools by hostile actors and authoritarian governments. The Department of State has established three guiding principles to accomplish these goals: implementing a comprehensive diplomatic approach across all sectors of the digital ecosystem, integrating cybersecurity into sustainable development initiatives, and advancing a technology-driven vision based on international law. Promoting an open and inclusive digital infrastructure, harmonizing global digital governance regulations, fortifying alliances against cyberthreats, and bolstering partner countries' cybersecurity capacities are the strategy's four main areas of activity. In order to prevent enemies from dictating the direction of digital governance in the future, the United States also seeks to strengthen its position as a leader in multilateral organizations that establish international cybersecurity standards.

To achieve these objectives, the Department of State has set three guiding principles: advancing a technology-driven vision grounded in international law; integrating cybersecurity into sustainable development initiatives; and putting in place a

[15] U.S. Department of State, *United States International Cyberspace & Digital Policy Strategy* (May, 2024), https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/.

comprehensive diplomatic approach across all sectors of the digital ecosystem. The strategy's four primary areas of action include strengthening partnerships against cyberthreats, promoting an open and inclusive digital infrastructure, standardizing global digital governance norms, and enhancing partner nations' cybersecurity capabilities. The United States also aims to bolster its role as a leader in multilateral organizations that set global cybersecurity standards to keep adversaries from controlling the future course of digital governance.



Source: World Economic Forum, Global Risks Perception Survey 2022-2023

The U.S. General Services administrations articled on [16]May 12, 2021, It proposes actions to improve software supply chain integrity and cybersecurity. It requires agencies to implement encryption, multifactor authentication, zero-trust architecture, and secure cloud usage. Data on cyber threats must be shared by service providers, and software developers must increase transparency. Significant cyber incidents will be looked into by a Cybersecurity Safety Review Board, which will also suggest improvements.

Standardized cyber incident response playbooks and endpoint detection systems will be implemented by federal agencies. Contractor's risk losing government contracts if they don't follow the most recent Federal Acquisition Regulation (FAR) guidelines. Companies should hold public comment periods, train staff, and update compliance programs. By encouraging cooperation between the federal government and the commercial sector, these changes address the growing challenges posed by cyberspace and ensure national security.

The U.S. National Science Foundation (NSF) has [17]announced Seven new National Artificial Intelligence Research Institutes will be established with a $140 million investment. This program is a component of a larger federal endeavor to maximize AI's potential while reducing related hazards. These institutes will strengthen the U.S. AI workforce by advancing ethical AI, cybersecurity, climate change solutions, neuroscience, education, and societal decision-making.

Leading research institutions oversee these institutes, which combine interdisciplinary knowledge and are supported by a number of federal agencies as well as business partners.

[16] U.S. General Services Administration, *Actions to improve software supply chain integrity and cybersecurity* (May 12, 2021), https://www.gsa.gov/technology/government-it-initiatives/cybersecurity/executive-order-14028.
[17] PRESS RELEASE, *National Cyber Security Index* (May 4, 2023), https://www.nsf.gov/news/nsf-announces-7-new-national-artificial.

Their areas of interest include climate-smart agriculture, AI-enhanced decision-making, neuroscience-driven AI, AI trustworthiness, intelligent cybersecurity systems, and inclusive AI technologies for education. This significant investment underscores the government's dedication to leading AI, encouraging responsible innovation, and making sure the advantages of AI are shared fairly throughout society.

On March 28, 2024, the United States was ranked 11th with a score of 84.17 in the National Cyber Security Index, which is also validated by the World Health Organization. It is ranked first in the Network Readiness Index, thirteenth in the Global Cybersecurity Index, and nineteenth in the E-Government Development Index. The nation is home to 323.9 million people, covers 9.6 million km2, and has a $61.7K GDP per person.

3. CHALLENGES

3.1 INDIA

Times of India as voice of India posted that [18]the cybersecurity environment of 2023 is characterized by a growing dependence on digital infrastructure, which exposes businesses to changing risks. Increased security measures are necessary to safeguard sensitive data due to the surge in sophisticated cyberattacks. India recorded 13.91 lakh cybersecurity incidents in 2022, according to CERT-In data, indicating a continuing problem even if the number of cases decreased slightly from 14.02 lakh in 2021. Proactive measures are required to counter these risks.

By the end of 2023, there will be 14.4 billion IoT devices in India, a significant growth that increases the attack surface for cybercriminals. Risks are increased by security flaws including inadequate authentication and out-of-date software. Furthermore, the problem is made worse by an estimated 3 million cybersecurity professionals are needed. To lessen these difficulties, industry cooperation and cybersecurity education must be strengthened.

The Cybersecurity Centre of Excellence [19]posted on Strong government initiatives are now required to tackle cyber dangers in India as a result of the growing digitization of industries. Programs like Cyber Surakshit Bharat, Cyber Swachhta Kendra, and CERT-In are essential for malware detection, awareness-raising, and incident response. India's cyber resilience is further reinforced by the National Cybersecurity Policy, which guarantees data security and adherence to regulations in a constantly changing threat environment.

To improve cybersecurity, innovation and skill development must be encouraged. The Hyderabad-based Telangana government's Center of Excellence fosters workforce

[18] Shubham Mishra, *Challenges faced by cyber security in 2023*, THE TIMES OF INDIA, June 19, 2023, 11:27 AM IST.

[19] Cybersecurity Centre of Excellence, *The Role Of Government Initiatives In Tackling Cybersecurity Challenges In India*, https://ccoe.dsci.in/blog/the-role-of-government-initiatives-in-tackling-cybersecurity-challenges-in-india.

development, research, and startups. Cybersecurity capabilities are improved through partnerships with groups such as the Data Security Council of India. India can create a robust digital ecosystem to fend off new cyberthreats by providing companies with strong security frameworks and promoting public-private collaborations.

The financial express which has posted as [20]India's Cyber threats targeting vital industries like healthcare and finance have increased along with India's digital revolution. High-profile attacks reveal security flaws, such those carried out by the North Korean Lazarus gang. Proactive tactics, legislative frameworks, and investments in cutting-edge technologies are all necessary to strengthen cybersecurity and reduce risks while shielding digital assets from ever-more-sophisticated cybercriminal activity.

Cybersecurity is strengthened by government programs like CERT-In and the Digital Personal Data Protection Act yet risks still exist. The creation of the National Cybersecurity Authority (NCSA) can improve innovation, resource allocation, and readiness. India can secure its digital economy and establish itself as a leader in international cybersecurity initiatives by promoting cooperation, tightening laws, and giving cybersecurity education first priority.

The Business standard vocalic on [21]the India's information security spending is expected to expand by 16.4% by 2025, which highlights how urgent cybersecurity is in a world that is gradually becoming more digital. Businesses are prioritizing investments in security services, cloud security, and access management to strengthen their defenses against

[20] Guest, *Navigating cybersecurity challenges: Safeguarding India's digital transformation in a threatening landscape*, FINANCIAL EXPRESS, February 8, 2025.

[21] BS Reporter Mumbai, *Investment in information security likely to grow 16.4% in 2025: Gartner*, BUSINESS-STANDARD, Mar 11, 2025.

sophisticated cyber threats as they struggle with enduring security challenges, such as ransomware, data sprawl from GenAI, and changing regulations.

The lack of qualified cybersecurity specialists is reflected in the increasing reliance on managed security services, which forces businesses to look for specialized security management firms. Due to the requirement for improved cloud security and the incorporation of AI models into enterprise applications, security software spending is expected to reach $1.2 billion at the same time. India's dedication to bolstering its cybersecurity infrastructure is demonstrated by this increasing expenditure.

3.2 UNITED STATES OF AMERICA

The U.S Securities and Exchange Commissions on [22]Oct. 19, 2015, demonstrated that small and midsize businesses (SMBs) are at the forefront of cybersecurity risks and that, because of their low resources and weakened defenses, they are frequently the main targets of cybercriminals. Due to their increased dependence on digital platforms, cloud computing, and interconnected business ecosystems, SMBs are now more vulnerable to sophisticated cyberattacks that could endanger their survival, such as ransomware, phishing, and fraudulent financial transactions.

Cyberattacks have serious repercussions for SMBs, with many unable to recoup from the financial and reputational harm they have suffered. Research shows that targeted attacks are becoming more common, which emphasizes the necessity of preventative cybersecurity measures. Important efforts in risk mitigation include enhancing public-

[22] Luis A. Aguilar, *The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses* (Oct. 19, 2015), https://www.sec.gov/newsroom/speeches-statements/cybersecurity-challenges-small-midsize-businesses.

private collaborations, putting in place affordable cybersecurity frameworks, and growing educational initiatives. SMBs continue to be extremely susceptible in the absence of swift action, putting the stability of the economy at risk.

The OXFORD Academic on 2nd December 2021 articled with a [23]view The cyber threats to the United States' vital financial infrastructure have increased over the last 20 years, putting the Financial Services Sector (FSS) at danger on a systemic level. Cyberattacks pose a threat to data security and institutional stability as financial transactions become more digitalized. These risks are increased by the sector's interconnection, since major institution disruptions can lead to broader instability, which calls for stricter cybersecurity regulations and regulatory monitoring.

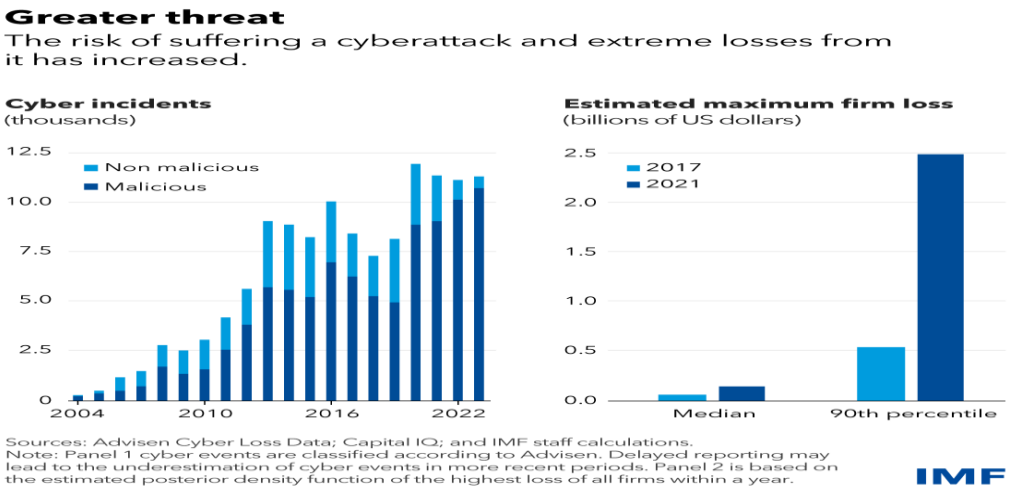
Government-industry cybersecurity cooperation is still lacking despite advancements. Businesses are compelled by regulations to implement security measures, yet disparities in investment still exist, particularly among smaller businesses. Information exchange is impeded by competitive obstacles, which erodes collective defense. Despite investing more than other sectors, financial institutions are vulnerable due to gaps in intelligence sharing. To mitigate evolving cyber dangers, it is imperative to strengthen collaboration, enforce strong standards, and cultivate trust among stakeholders.

The International monetary fund (IMF) has incurred financial instability by a post on April 9, 2024, where [24]Cyber As a result of increased digitalization and geopolitical tensions, dangers to the banking sector have increased. Because financial institutions handle

[23] Sean Atkins, Chappell Lawson, *Cooperation amidst competition: cybersecurity partnership in the US financial services sector* Volume 7, Journal of Cybersecurity, 2nd December, 2021.

[24] Fabio Natalucci, Mahvash S. Qureshi and Felix Suntheim, *Rising Cyber Threats Pose Serious Concerns for Financial Stability* (April 9, 2024), https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability.

enormous volumes of sensitive data and enable vital transactions, the growing scope of cyberattacks presents systemic concerns. Stronger regulatory frameworks are required since a serious attack on a big institution might lead to market volatility, payment network disruptions, and widespread economic misery.



Coordination between financial authorities, businesses, and international organizations is necessary to address these threats. It is essential to improve risk assessment, strengthen cybersecurity governance, and build resilience through effective incident response procedures. To reduce systemic risks, public action—including regulatory supervision and international collaboration—is crucial. By assisting countries in creating regulatory frameworks that protect financial stability, the IMF plays a critical role in directing cybersecurity policy.

The Centre for Internet Security (CIS) is a [25]nonprofit organization devoted to improving public and private enterprises' cybersecurity response and readiness. To protect IT systems

[25] HOME PAGE, *Center for Internet Security (2000),* https://www.cisecurity.org.

and data from changing cyberthreats, it creates internationally accepted best practices, such as the CIS Critical Security Controls and CIS Benchmarks. established during the past 25 years as well.

Resources from CIS, including the CIS Hardened Images, offer pre-configured virtual machine images that are made to adhere to strict security guidelines. Additionally, it runs communities like as the Multi-State Information Sharing and Analysis Centre (MS-ISAC), which aims to enhance state, local, tribal, and territorial government institutions' overall cybersecurity posture.

As data theft being the major threat, there are few judgments on the same lines where one of the judgment submits [26]a copyright infringement case in which the plaintiff claims that the defendants' compilation resulted in a pirated copy of his dictionary. After posing a number of questions, the lower court decided in favour of the plaintiff, granting him Rs. 5,000 in damages and upholding the injunction against the defendants.

Additionally, in the Lok Sabha Debates, the Standing Committee on Finance met for the third time on February 14, 2005, to review the Credit Information Companies (Regulation) Bill, 2004, with a focus on the regulatory framework governing credit information entities. This was part of the Credit Information Companies Regulation Act, 2005. The Committee carefully examined important clauses, emphasizing the need to restrict the number of these businesses while maintaining nationwide coverage of credit data.

The Securities Appellate Tribunal (SAT) should have initial appellate jurisdiction, according to the Committee's recommendation, with the authority to hire experts as

[26] V. Govindan v. E.M. Gopalakrishna Kone, 1954 S.C.C. Online Mad 368.

needed. It also indicated that a specific financial services appellate authority may be created if growing caseloads warranted it. These changes sought to guarantee an integrated approach to credit information governance, improve supervision, and simplify financial rules.

4. TRENDS

4.1 INDIAN TRENDS

The Sattrix as one of the prominent authorities have revealed the upcoming modernization in Indian cybersecurity area as [27]India's digital change come increased cybersecurity threats, such as ransomware-as-a-service (RaaS), AI-powered assaults, and weaknesses on the Internet of Things. As 5G and quantum computing transform the technical environment, cybercriminals take advantage of these developments to initiate complex attacks. Businesses must implement blockchain security, improve biometric authentication, and embrace Zero Trust Architecture in order to reduce risks and stay in compliance with strict data protection laws.

The swift spread of deepfake and social media exploitation technologies makes cybersecurity measures even more difficult, necessitating sophisticated detection systems and public awareness initiatives. Proactive security frameworks are necessary because autonomous technologies, such as self-driving cars, create new attack avenues. Cybersecurity maturity must be given top priority by businesses through ongoing

[27] Sattrix, *TOP 13 CYBERSECURITY TRENDS INDIA MUST EMBRACE BY 2025 TO STAY AHEAD* (Dec. 24, 2024), https://www.sattrix.com/blog/2025-cybersecurity-trends-india-to-watch/.

monitoring, adherence to regulations, and staff development. In an ever-changing threat landscape, maintaining digital resilience requires bolstering defenses.

Also, economic times enshrined on [28]"SECPOD PREVENT 2025: India's leadership in cybersecurity innovation and the launch of Saner Cloud", With SECPOD PREVENT 2025 leading the way in a prevention-first approach to security, the cybersecurity sector is seeing a revolutionary change. In order to address vulnerabilities before they become cyber incidents, the event brings together security executives, researchers, and businesses to facilitate essential conversations about the shift from reactive defenses to proactive threat prevention.

The introduction of Saner Cloud, a Cloud-Native Application Protection Platform (CNAPP) intended for automated remediation and early risk identification, was a significant highlight. Prominent speakers who offered insights into contemporary threat mitigation included Adam Pennington from MITRE ATT&CK and Nils Puhlmann of the Cloud Security Alliance. Chandrashekhar Basavanna, CEO of SECPOD, highlighted the need of proactive security, establishing prevention as a key tactic for businesses managing the constantly changing cyberthreats of today.

Subsequently, the Business-standard posted the trendy showdown on 29th Dec 2024 titled as [29]"97% of Indian organisations investing in AI & ML technology: DSCI report" With 84% of businesses investing in cloud security and 97% of firms implementing AI/ML, India's cybersecurity market is growing quickly. The market reached $6 billion in 2023,

[28] Chandrashekhar Basavanna, *SECPOD PREVENT 2025: India's leadership in cybersecurity innovation and the launch of Saner Cloud*, The Economic Times, Feb 27, 2025.

[29] Ashutosh Mishra, *97% of Indian organisations investing in AI & ML technology: DSCI report*, BUSINESS-STANDARD, Dec 29, 2023.

growing at a 30% CAGR. In the face of growing cyberthreats, government programs and business cooperation are solidifying India's standing as a global cybersecurity hub and fostering innovation and resilience in vital industries.

With 84% of firms seeing phishing as a major threat and 90% mentioning email as a major attack channel, cybersecurity issues still exist despite progress. 75% of businesses face a serious talent shortage, and in 2023, BFSI cybersecurity investment jumped to $1.7 billion. Cyberattacks result in financial losses (75%), as well as harm to one's reputation (87.5%), underscoring the necessity of more robust security protocols and personnel training.

Also, in another article by Business Standard articled as [30]"Investment in India's end-user spending on information security is expected to reach $3.3 billion in 2025, a 16.4% increase from 2024, according to a Gartner report on the subject. Due to issues like ransomware, data sprawl brought on by AI, and strict restrictions, security services will see the largest growth, increasing by 19%. To increase resilience, businesses are placing a higher priority on incident response, real-time threat identification, and improved security measures.

By 2028, security is expected to account for 40% of IT contracts, and a lack of qualified personnel is driving up demand for managed security services. Spending on security software will reach $1.2 billion, driven by vulnerabilities posed by AI and the need for cloud security. As India's digital economy grows, investments in infrastructure protection, data privacy, and application security will increase, strengthening the country's cybersecurity framework.

[30] BS Reporter Mumbai, *Investment in information security likely to grow 16.4% in 2025: Gartner*, BUSINESS-STANDARD, Mar 11, 2025.

4.2 AMERICAN TRENDS

United states of America do not amicable for security but formulation of the same canvased through past records as being a long-term victim of cybersecurity also, Industrial Cyber company have posted an article on MARCH 14, 2024, titled with [31]"US Federal Budget for FY 2025 boosts cybersecurity investments amid escalating threats", shows a large investment in cybersecurity to improve federal infrastructure, combat new threats, and increase resilience. In order to strengthen national security by guaranteeing strong defenses against cyberattacks, the government has allocated $13 billion for cybersecurity across civilian agencies. The Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ) receive a significant amount of funding to enhance their investigative, counterintelligence, and cyber intelligence capabilities.

Additionally, $103 million of the $3 billion allotted to the Cybersecurity and Infrastructure Security Agency (CISA) in the budget is devoted to enhancing security measures. This includes large expenditures for infrastructure security, network resilience, and endpoint detection. $800 million will be given to the Department of Health and Human Services (HHS) to help hospitals adopt cybersecurity best practices and safeguard vital patient data. Furthermore, $455 million will be used to further AI research, guaranteeing the safe and secure application of AI in the energy and national security domains.

[31] Industrial Cyber, *US Federal Budget for FY 2025 boosts cybersecurity investments amid escalating threats* (March 14, 2024), https://industrialcyber.co/critical-infrastructure/us-federal-budget-for-fy-2025-boosts-cybersecurity-investments-amid-escalating-threats/.

4.3 JUDGMENTS

On August 10, 2021, [32]instead of dismissing a case with exceptional costs, the Apex Court chose to grant it for a modest fee of one thousand rupees. The petition was brought by a novice attorney. The Court determined that the petitions' unsupported claims, which mostly relied on rumours and news reports, were inadequate to support the use of its writ jurisdiction. The Court voiced unhappiness with the Respondent-Union of India's brief affidavit, stating that a detailed investigation and report must be made by the Committee in order to proceed.

The case centers on claims that Pegasus malware was used to watch people without following the proper legal procedures, including political figures and journalists. According to the petitioners, the program permits total device control, making it possible to implant fictitious evidence and get unlawful access to personal information. The Court is debating whether these grave claims require an independent investigation, especially in view of the NSO Group's revelation that Pegasus was only offered to governments that had been thoroughly screened, which raised questions about unlawful monitoring methods.

In 2023, the High Court of Delhi have ordered on [33]the A writ case filed by Trusted Info Systems Private Limited aimed to overturn the Indian Computer Emergency Response Team's Online Practical Skill Test results, which gave out scores of 65% and 70% in 2020 and 2021, respectively. According to the court, the expert body's assessment should not be influenced unless there is proof of bias or criminality, hence the petition was denied. Since the cool-off period had passed and no hard proof of favouritism or irregularity had been shown, the court determined that the petition was now complete.

[32] Manohar Lal Sharma vs. Union of India, MANU-SC-0989-2021.
[33] Trusted Info Systems (P) Ltd. v. Indian Computer Emergency Response Team, 2023 S.C.C. OnLine Del 7433.

5. CONCLUSION

Growing digitization and the associated increase in cyberthreats are driving a rapid evolution of the cybersecurity landscape in both India and the US. A Cyber Security and Cyber Resilience Framework (CSCRF) was created by the Securities and Exchange Board of India (SEBI) in India to improve the security of regulated firms. It requires strict security controls and incident response procedures. By working with stakeholders to strike a balance between operational flexibility and cybersecurity requirements, SEBI is taking a proactive approach to protecting digital infrastructure with this effort. The framework highlights the value of board-level supervision and promotes the use of cutting-edge technology like blockchain and artificial intelligence to increase resilience. In order to address industry concerns, SEBI has also extended compliance deadlines and granted regulatory forbearance, allowing firms to successfully implement the required cybersecurity safeguards.

The Securities and Exchange Commission (SEC), which focuses on investor protection and market integrity, is a key regulator of the securities markets in the United States. The Cyber and Emerging Technologies Unit (CETU) was established by the SEC to combat misbehaviour linked to cyberspace and shield individual investors from deceptive practices. Through the examination of fraudulent schemes and the enforcement of cybersecurity regulations, this section seeks to counteract cyber dangers. In addition, a new cybersecurity risk management regulation has been proposed by the SEC for investment funds and advisers, mandating that they put in place thorough procedures to reduce cybersecurity risks and promptly disclose major occurrences.

Both nations understand how important it is to have strong cybersecurity policies in order to safeguard their digital industries and financial systems. With an emphasis on

strengthening organizations like CERT-In and encouraging public-private collaborations, India has greatly expanded its budgetary allotment for cybersecurity projects. By placing a strong emphasis on domestic research and development, capacity-building programs, and international collaboration, the National Cyber Security Policy seeks to establish a safe and resilient cyberspace. India is giving cybersecurity expenditures top priority in order to protect its digital infrastructure and promote innovation as cyber threats continue to change.

To reduce risks and improve digital governance, the United States' National Cybersecurity Strategy places a strong emphasis on cooperation between the public and commercial sectors. In addition to investing in a qualified cybersecurity staff, the strategy lays out important pillars such as protecting critical systems and breaking up cybercriminal networks. With large funding allotted to agencies to bolster their cyber capabilities and safeguard vital infrastructure, the federal budget for FY 2025 shows a strong commitment to cybersecurity. A lack of qualified personnel and the requirement for constant adaptation to new threats are two obstacles that both countries must overcome as they negotiate the complexity of cybersecurity. Because of the quick growth of IoT devices and the growing complexity of cyberattacks, proactive tactics and improved security measures are required in India. Public-private collaborations and affordable cybersecurity frameworks are crucial, as small and midsize firms in the United States are especially susceptible to cyber threats.

In conclusion, the changing cybersecurity environment in the US and India highlights the need for thorough legal frameworks, calculated financial outlays, and cooperative initiatives to counter the escalating cyberthreats. Realizing the importance of a safe digital environment for both national security and economic stability, both nations are making major efforts to strengthen their cybersecurity resilience. Building a strong cybersecurity infrastructure will require a focus on innovation, education, and international collaboration as they continue to adjust to the shifting threat landscape.