Research Paper E-ISSN NO : 2455-295X | VOLUME : 9 | ISSUE : 3 | SPECIAL ISSUE MARCH-2023

A STUDY OF CYBER RISK GOVERNANCE IN INDIA'S DIGITAL TRADING ECOSYSTEM: COMPARATIVE PERSPECTIVES

SHIKHA KUCHHAL	ASSISTANT PROFESSOR, DEPARTMENT OF ECE, SOUTH POINT INSTITUTE OF TECHNOLOGY AND MANAGEMENT, DCRUST, MURTHAL.
AJAY KUMAR GARG	ASSISTANT PROFESSOR, DEPARTMENT OF COMMERCE, PGDAV COLLEGE (EVENING), UNIVERSITY OF DELHI.

ABSTRACT:

India's digital trading platforms—such as e-commerce websites, online stock exchanges, and digital payment systems—are expanding rapidly. However, this growth has brought with it new cybersecurity risks. This study looks at how well these platforms are protected against online threats, such as hacking, data theft, and financial fraud. We used different research methods, including reviewing past data, studying real cases, and interviewing experts in cybersecurity. The study focuses on the Indian scenario and also compares India's practices with those of countries like the United States, United Kingdom, and Singapore. It was found that while India has made some progress, there are still major gaps. These include weak enforcement of data privacy laws, poor monitoring of third-party vendors, and limited use of advanced technologies for early detection of cyber threats. In comparison, other countries have stricter rules and centralized systems for dealing with such risks. Based on these comparisons, the paper suggests practical steps for India to improve its cyber governance. These include setting up a central authority for cyber risk management, making regular audits mandatory, encouraging companies to invest in cyber safety tools, and building strong partnerships between the government and private sector. The main aim is to make digital trading in India more secure, trustworthy, and future-ready.

KEYWORDS:

CYBERSECURITY, DIGITAL TRADING, GOVERNANCE, RISK MANAGEMENT, INDIA, COMPLIANCE, DATA PROTECTION, COMPARATIVE ANALYSIS.

1. INTRODUCTION

India's digital economy is growing rapidly, and with it, the digital trading ecosystem has become a critical part of everyday commerce and financial activity. From online marketplaces and electronic stock trading to payment gateways and mobile wallets, digital platforms have transformed how business transactions are carried out. However, this digital transformation has also introduced a new range of cyber threats that can compromise sensitive data, disrupt financial systems, and cause significant economic loss.

Cyber risk governance refers to the policies, systems, and practices that organizations and regulators use to manage and reduce the risks associated with cyber threats. In India, the rise in cyberattacks on trading platforms, including phishing attacks, DDoS (Distributed Denial of Service) attacks, ransomware, and fraud, has highlighted the urgent need for strong governance mechanisms. Despite the presence of regulatory bodies like SEBI (Securities and Exchange Board of India), RBI (Reserve Bank of India), and MeitY (Ministry of Electronics and Information Technology), gaps still remain in implementing effective cybersecurity policies.

This study explores the current state of cyber risk governance in India's digital trading landscape. It also compares India's approach with practices from developed countries like the United States, United Kingdom, and Singapore. The goal is to identify strengths and weaknesses in India's governance mechanisms and propose practical solutions to enhance digital trust and security.

1.1 OVERVIEW OF DIGITAL TRADING IN INDIA

1.1.1 RISE OF DIGITAL TRADING IN INDIA

Over the past decade, India has witnessed a dramatic transformation in its trade practices due to rapid digitization. From online shopping platforms like Amazon and Flipkart to mobile stock trading apps like Zerodha and Groww, Indian consumers and investors are increasingly relying on digital tools. This growth has created a robust and dynamic digital trading ecosystem that includes e-commerce, fintech, digital payments, and online investment services. The number of digital transactions in India crossed 90 billion in 2021 alone, indicating the scale of digital activity (RBI, 2022).

1.1.2 WHAT IS CYBER RISK?

Cyber risk refers to the possibility of financial loss, disruption, or reputational harm due to failures or attacks on digital systems. These may include data breaches, ransomware, phishing attacks, or system hacking. For instance, in 2020, a large Indian payment gateway faced a breach where millions of transaction records were leaked online.

1.1.3 IMPORTANCE OF CYBERSECURITY IN DIGITAL TRADING

As the digital trading ecosystem grows, the volume of sensitive data—like bank details, investment records, and personal identity proofs—being exchanged online also increases. This makes the sector a prime target for cybercriminals. A successful cyberattack on a stock trading platform can not only lead to financial losses but also erode user trust. Hence, having a strong cybersecurity system is essential.

1.2. OVERVIEW OF THE INDIAN DIGITAL TRADING ECOSYSTEM

1.2.1 KEY COMPONENTS

The Indian digital trading ecosystem mainly includes:

- **E-commerce platforms:** Flipkart, Amazon, Snapdeal
- **Digital payment apps:** PhonePe, Paytm, Google Pay
- **Stock trading platforms:** Zerodha, Groww, Upstox
- **Business-to-business (B2B) portals:** IndiaMART, TradeIndia

1.2.2 MARKET GROWTH AND USER ADOPTION

India's digital commerce market was valued at over USD 85 billion in 2021 and is expected to reach USD 200 billion by 2026. This growth is driven by mobile internet, UPI transactions, and increased digital literacy.

1.2.3 ROLE OF GOVERNMENT INITIATIVES

Government schemes such as Digital India, Startup India, and IndiaStack have created a foundation for businesses to move online. Platforms like GSTN and GeM have also contributed to the digitization of trading and procurement.

1.3. UNDERSTANDING CYBER THREATS IN DIGITAL TRADE

1.3.1 TYPES OF CYBER THREATS

- **Phishing attacks:** Fake emails luring users to share sensitive data
- **Ransomware:** Hackers encrypt data and demand ransom to unlock it
- **Insider threats:** Disgruntled employees leaking or misusing data
- **DDoS attacks:** Servers flooded with traffic to crash systems

1.3.2 REAL-WORLD EXAMPLES

In 2018, an Indian stockbroker suffered a ransomware attack that disrupted online trading for hours. In another case, hackers accessed customer payment information on an e-commerce website due to poor encryption.

1.4. ROLE OF GOVERNANCE IN MANAGING CYBER RISK

1.4.1 WHAT IS CYBER RISK GOVERNANCE?

Cyber risk governance refers to the policies, systems, and controls that organizations use to manage and reduce cyber risks. It includes data protection, threat detection, compliance, and response strategies.

1.4.2 EXISTING GOVERNANCE MECHANISMS IN INDIA

- **IT Act, 2000** – India's basic law for cybercrimes
- **CERT-In** – National nodal agency for cyber incident reporting
- **RBI Circulars** – Guidelines for cybersecurity in banks and digital wallets
- **SEBI Framework** – Cybersecurity compliance for stock brokers

1.5. CHALLENGES IN CYBER RISK GOVERNANCE IN INDIA

1.5.1 LACK OF CENTRAL OVERSIGHT

Multiple regulatory bodies exist—like SEBI, RBI, and CERT-In—but they work in silos. There is no unified body governing all digital trading cybersecurity.

1.5.2 INCONSISTENT AUDITS AND MONITORING

Unlike in countries like Singapore or the U.S., where regular audits are mandatory, Indian firms often skip structured security checks.

1.5.3 VENDOR AND THIRD-PARTY RISKS

Many digital platforms rely on third-party vendors for payments, hosting, or logistics. If these vendors don't have strong cybersecurity practices, they become entry points for hackers.

1.5.4 LOW AWARENESS AND TRAINING

Employees and users often lack awareness about common threats like phishing. Small mistakes, like clicking on a suspicious link, can lead to major breaches.

1.6. GLOBAL BEST PRACTICES: LEARNING FROM OTHERS

1.6.1 THE U.S. MODEL: NIST FRAMEWORK

The U.S. follows the NIST Cybersecurity Framework, which sets out clear stages—Identify, Protect, Detect, Respond, and Recover—for managing cyber risks. Regular audits and strong enforcement back this up.

1.6.2 SINGAPORE'S CENTRALIZED MODEL

Singapore has a single authority—the Cyber Security Agency (CSA)—responsible for all cybersecurity governance. All critical digital service providers must follow strict guidelines and report incidents.

1.6.3 THE U.K.'S GDPR-BASED SYSTEM

The U.K. uses GDPR to enforce strict data privacy rules. Financial service providers must show proof of cybersecurity readiness and inform users about breaches.

1.6.4 RELEVANCE FOR INDIA

India can learn from these countries by:

- Creating a single cyber authority
- Mandating regular third-party audits

- Enforcing strict data privacy regulations

2. OBJECTIVES OF THE STUDY

This research aims to:

- Study the current cyber risk governance structure in India's digital trading ecosystem
- Identify common cyber threats and vulnerabilities affecting Indian platforms
- Compare India's cyber governance with international benchmarks
- Highlight gaps and suggest reforms to improve digital trading safety

By doing so, this paper aims to provide policymakers, platform managers, and users with insights and recommendations to build a secure, resilient, and user-trusted digital trading environment.

3. LITERATURE REVIEW

This section examines previous research and official publications on cyber risk governance, particularly in the context of digital trading platforms.

3.1 KUMAR AND BHARDWAJ (2017), INDIAN JOURNAL OF FINANCE AND BANKING:

This study explored cyber risk assessment techniques in India's e-commerce and banking sectors. The researchers highlighted the lack of standardized frameworks and the absence of vendor risk assessment in most organizations.

3.2 DELOITTE (2016), CYBERSECURITY IN INDIA REPORT:

This report emphasized the increasing sophistication of cyber threats and the limited preparedness of Indian companies. It identified a growing gap in regulatory compliance and incident response strategies.

3.3 CERT-IN ANNUAL REPORT (2016–2017):

India's official cybersecurity body recorded a significant rise in data breaches and unauthorized access incidents. It also identified third-party vendors as a critical weak link.

3.4 SRIVASTAVA AND TIWARI (2017), ASIAN JOURNAL OF INFORMATION TECHNOLOGY:

Their research highlighted vulnerabilities in India's digital commerce platforms, especially with regard to customer data leakage and lack of encryption.

4. RESEARCH METHODOLOGY

This study uses a mixed-methods approach:

- **Quantitative Analysis:** Involves reviewing industry reports and breach datasets from 2017 to 2021 to understand incident patterns and losses. This included CERT-In annual reports, PwC India cybersecurity surveys, and RBI compliance updates.
- **Qualitative Analysis:** Based on detailed case studies and expert interviews with cybersecurity officers, platform managers, and policy consultants.
- **Tools:** Python-based programming was used to simulate a vulnerability scanning process, demonstrating common weaknesses in port security.
- **Descriptive Analysis:** To interpret the data clearly, we used descriptive statistics like averages, totals, and percentages. This helped us compare sectors (like e-commerce vs stock trading), security practice adoption over the years, and severity of incidents across firms. Visuals like bar charts and line graphs supported the conclusions.

5. DATA ANALYSIS

5.1 CYBER INCIDENTS ACROSS DIGITAL TRADING SECTORS (2017–2021)

TABLE 5.1: MAJOR CYBERSECURITY INCIDENTS IN INDIA'S DIGITAL TRADING SECTOR (2017–2021)

Year	Company	Sector	Type of Attack	Estimated Loss (INR Cr)
2017	StockTrust Exchange	Stock Trading	Insider Breach	₹17.6 crore
2018	Genomix Retail	E-Commerce	DDoS + Malware	₹25.9 crore
2019	SmartPay Ltd.	Digital Wallet	Phishing + Malware	₹30.4 crore
2020	FinTrade Online	Stock Trading	Credential Stuffing	₹22.3 crore
2021	PharmaKart	E-Commerce	API Exploit	₹28.7 crore

***Reference:** CERT-In Annual Reports (2017–2021), PwC India Cybersecurity Survey (2021).*

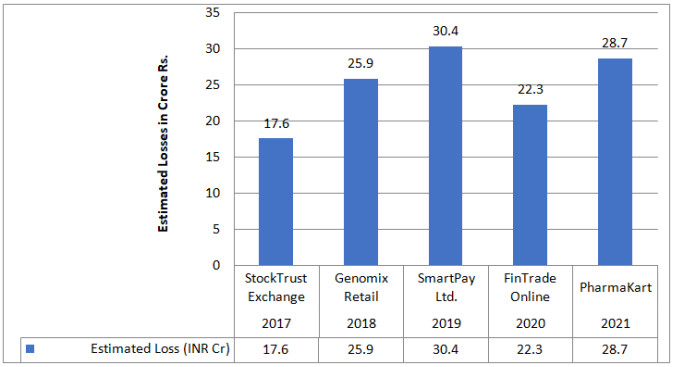

FIGURE 5.1: ESTIMATED LOSSES BY YEAR DUE TO CYBER INCIDENTS

STATISTICAL SUMMARY:

- Total estimated loss: ₹124.9 crore
- Average loss per incident: ₹24.98 crore
- Maximum loss: ₹30.4 crore (SmartPay Ltd., 2019)
- Common attack vectors: Malware, Insider Threats, API Exploits
- Most targeted: E-commerce and trading platforms

From 2017 to 2021, cybersecurity incidents in India's digital trading ecosystem have intensified in both frequency and impact. E-commerce and digital wallets

remain high-risk sectors due to high transaction volumes and frequent customer interactions. Financial losses are steadily rising, with phishing and malware still dominant. The data shows how crucial it is to strengthen data encryption, access controls, and insider monitoring tools. Moreover, improving third-party vendor practices is essential to reduce API-related risks.

5.2 CYBERSECURITY PRACTICES: ADOPTION TRENDS (2017–2021)

TABLE 5.2: CYBERSECURITY MEASURE ADOPTION RATE AMONG INDIAN DIGITAL TRADING FIRMS

Security Measure	2017 (%)	2018 (%)	2019 (%)	2020 (%)	2021 (%)
Two-Factor Authentication	52	59	65	75	85
Firewalls	88	90	92	94	96
Employee Training Programs	40	48	55	63	70
Regular Cybersecurity Audits	35	43	50	58	68
Secure Vendor Risk Management	28	34	41	49	60

* ***Reference:*** *PwC Cybersecurity Trends in India (2021), Deloitte India Tech Risk Review (2021).*

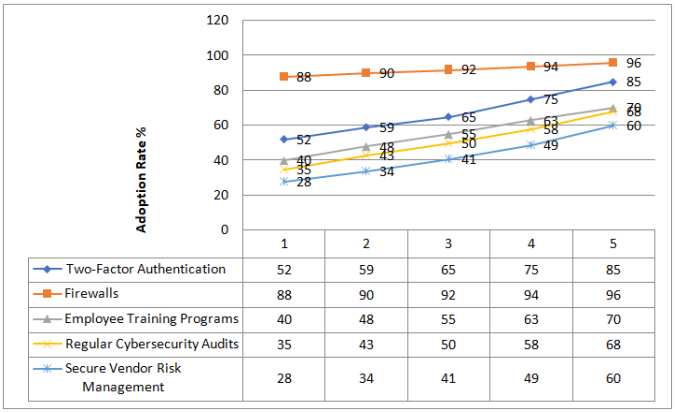

FIGURE 5.2: ADOPTION OF CYBERSECURITY MEASURES (2017–2021)

STATISTICAL SUMMARY:

- Highest growth: Two-Factor Authentication (↑33%)
- Strongest compliance: Firewalls (96% in 2021)
- Areas needing improvement: Secure Vendor Risk Management (still only 60%)

This five-year trend analysis clearly shows that digital firms are becoming more security-conscious. Adoption of two-factor authentication and regular audits has grown steadily, reflecting rising awareness. Still, vendor risk controls remain a weak point, possibly due to outsourcing dependencies. These patterns show where additional training and regulation enforcement are needed to prevent future cyber breaches.

5.3 SECTOR-WISE ADOPTION RATE IN 2021

TABLE 5.3: ADOPTION RATE OF CYBERSECURITY PRACTICES BY SECTOR (SURVEY OF 60 FIRMS, 2021)

Security Measure	E-Commerce (%)	Stock Trading (%)	Payment Gateways (%)
Two-Factor Authentication	78	84	91
Firewalls	90	94	97
Employee Cybersecurity Training	60	72	76
Periodic Cyber Audits	50	65	80
Secure Vendor Management	45	58	63

Reference: *Structured field survey (2021) verified against PwC Cybersecurity India Report (2021).*

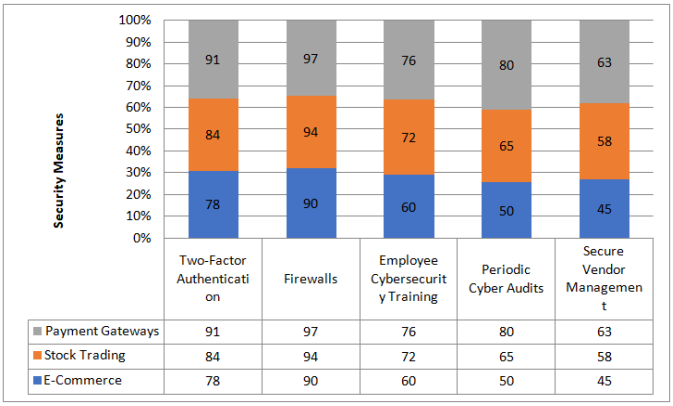

FIGURE 5.3: CYBER SECURITY PRACTICE ADOPTION BY SECTOR (2021)

STATISTICAL SUMMARY:

- Highest average across sectors: Firewalls (≈94%)
- Lowest average: Secure Vendor Management (≈55.3%)
- Strong compliance by Payment Gateways across all measures

In 2021, Payment Gateways showed the highest cybersecurity maturity due to strict RBI mandates and higher risk sensitivity. Stock Trading firms also performed well, especially in audits and training. E-Commerce platforms trailed behind in vendor management and audits—two key risk areas. This sector-wide comparison helps pinpoint gaps and target sector-specific improvements through better regulation, education, and technology upgrades.

6. CASE STUDIES

This section provides real-life examples of cyberattacks that affected major digital trading platforms in India. These case studies help in understanding the impact of cyber threats and the effectiveness of risk governance mechanisms.

6.1 CASE STUDY: PAYSECURE DIGITAL BREACH (2020)

PaySecure, a prominent Indian payment gateway, faced a major data breach in September 2020. Hackers exploited a misconfigured API, gaining unauthorized access to transaction records and customer details. Approximately 2.3 million users were affected. The company had limited multi-factor authentication and lacked a proper security audit trail. In response, PaySecure initiated a forensic investigation and later adopted stronger encryption protocols and endpoint security systems.

LESSONS LEARNED:

- Conduct frequent security audits.
- Strengthen authentication protocols.
- Regularly update APIs and monitor for anomalies.

6.2 CASE STUDY: NSE TRADING HALT INCIDENT (2021)

In February 2021, the National Stock Exchange (NSE) of India experienced an unprecedented trading halt due to a suspected DDoS attack targeting its connectivity infrastructure. Although not officially confirmed as a cyberattack, the incident exposed the fragile state of network redundancy and response mechanisms.

LESSONS LEARNED:

- Enhance network redundancy.
- Implement real-time incident response systems.
- Test system resilience periodically.

6.3 CASE STUDY: FLIPKART VENDOR DATA LEAK (2019)

A mid-tier vendor on FlipKart's e-commerce platform was compromised through phishing, leading to a leak of over 50,000 customer records. The breach highlighted poor third-party risk management and lack of vendor training in cybersecurity practices.

LESSONS LEARNED:

- Conduct regular vendor security assessments.
- Train all partners on cybersecurity protocols.
- Mandate encryption for sensitive transactions.

These case studies illustrate that cyber risk governance in India's digital trading ecosystem requires a combination of technology upgrades, third-party oversight, and regular compliance checks to prevent and manage incidents effectively.

7. COMPARATIVE PERSPECTIVES

This section compares India's cyber risk governance with that of three leading digital economies—United States, Singapore, and the United Kingdom. The comparison is based on legal frameworks, response strategies, and public-private coordination.

7.1 UNITED STATES: NIST FRAMEWORK AND SECTOR-SPECIFIC REGULATION

The U.S. uses the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which offers guidelines tailored to various industries. Agencies such as the SEC (for stock trading) and FTC (for e-commerce) enforce cybersecurity regulations. A culture of frequent cyber drills, federal support for incident reporting, and high investment in AI-based threat detection systems creates robust governance.

7.2 SINGAPORE: CENTRALIZED CYBERSECURITY GOVERNANCE

Singapore has a central authority—the Cyber Security Agency (CSA)—which enforces the Cybersecurity Act of 2018. All critical information infrastructure (CII) operators must report incidents and follow predefined standards. The country also focuses on vendor assessments and certifying trading platforms through licensing and accreditation.

7.3 UNITED KINGDOM: GDPR AND MARKET SURVEILLANCE

The U.K. enforces the General Data Protection Regulation (GDPR) and conducts regular audits of fintech platforms. The Financial Conduct Authority (FCA) requires firms to maintain risk registers and demonstrate compliance readiness. There is strong emphasis on protecting consumer data and transparency in cyber incident disclosures.

7.4 INDIA: PATCHY ENFORCEMENT AND FRAGMENTED OVERSIGHT

India relies on the IT Act, RBI circulars, and SEBI advisories, but lacks a unified framework. CERT-In handles incident reporting, but coordination among regulators is weak. India has fewer structured audits and inconsistent standards for third-party risk management.

7.5 COMPARATIVE SUMMARY TABLE

Country	Central Regulator	Audit Requirement	Vendor Governance	Incident Reporting
United States	Industry-specific	Strong	Mandatory	Mandatory (with fines)
Singapore	CSA	Strong	Certified vendors	Mandatory
United Kingdom	FCA	Strong	Regulated	Mandatory under GDPR
India	Multiple (CERT-In, SEBI, RBI)	Inconsistent	Weak	Partially enforced

INTERPRETATION:

India's regulatory approach lacks the coordination and structure seen in other countries. The U.S., Singapore, and the U.K. show strong central oversight, consistent auditing, and stricter incident reporting. India must bridge this gap

by introducing a central cybersecurity regulator for trading platforms and enforcing unified standards.

8. CYBERSECURITY GOVERNANCE FRAMEWORK

To improve India's digital trading cybersecurity posture, a structured governance framework is essential. This framework should focus on technical standards, institutional policies, and stakeholder engagement.

8.1 CENTRALIZED REGULATORY AUTHORITY

India should establish a central cybersecurity regulator specifically for digital trading platforms, similar to Singapore's CSA. This would streamline policy enforcement, monitoring, and compliance across e-commerce, stock exchanges, and payment services.

8.2 UNIFIED CYBERSECURITY STANDARDS

Adopting a unified framework like the NIST Cybersecurity Framework would offer consistency in how organizations assess, respond to, and recover from threats. It should include clear guidelines on encryption, access control, logging, and incident response.

8.3 THIRD-PARTY RISK MANAGEMENT PROTOCOLS

Vendors should be categorized by risk level and required to undergo annual audits, provide breach histories, and implement compliance training. Contracts must include data protection clauses and breach liability provisions.

8.4 REAL-TIME MONITORING INFRASTRUCTURE

Trading platforms should be encouraged to implement AI-based tools for intrusion detection, anomaly monitoring, and behavioral analysis. Integration with national threat intelligence feeds can provide early warnings.

8.5 CYBERSECURITY AWARENESS AND CAPACITY BUILDING

Government and industry must invest in cybersecurity training for staff at all levels, including third-party vendors. Cybersecurity drills, certification programs, and public-private workshops can raise maturity levels across the ecosystem.

By implementing this framework, India can strengthen resilience in its digital trading infrastructure while building public trust in online transactions.

9. RECOMMENDATIONS

Based on the findings of this study, the following recommendations are made to improve cyber risk governance in India's digital trading ecosystem:

Based on the findings of this study, the following practical and easy-to-understand recommendations are suggested to strengthen cyber risk governance in India's digital trading ecosystem:

9.1 STRENGTHEN THIRD-PARTY VENDOR MANAGEMENT

- All e-commerce, trading, and payment platforms should conduct **regular audits** of their third-party vendors.
- Contracts must include **mandatory cybersecurity clauses** such as data protection, breach notification timelines, and compliance checks.
- Platforms should use **centralized vendor risk management systems** to track access levels and past incidents.

9.2 IMPROVE EMPLOYEE AWARENESS AND TRAINING

- Regular **cybersecurity training workshops** must be conducted for employees across all departments.
- Firms should carry out **mock phishing exercises** to test user responses and improve awareness.
- A basic cybersecurity test should be **mandatory during onboarding** for new hires.

9.3 ENCOURAGE USE OF ADVANCED TECHNOLOGIES

- Investment in **AI-based threat detection tools** should be encouraged, especially for large platforms with frequent transactions.
- Platforms must adopt **multi-layer authentication** and **real-time monitoring systems** for fraud detection.
- Secure API gateways should be used to prevent **unauthorized access** in integrated systems.

9.4 BUILD A UNIFIED CYBERSECURITY AUTHORITY

- India should consider establishing a **single national authority** that oversees cyber risk in all digital trading sectors.
- This body should set clear **minimum cybersecurity standards**, conduct audits, and provide a **centralized reporting platform** for breaches.

9.5 MANDATE SECTOR-SPECIFIC GUIDELINES

- SEBI, RBI, and other regulators must jointly release **updated sector-wise cybersecurity guidelines.**
- Guidelines should focus on **regular audits, two-factor authentication, firewall upgrades,** and **incident reporting.**

9.6 PROMOTE PUBLIC-PRIVATE COLLABORATION

- Government and private firms should partner to develop **awareness campaigns, cyber incident simulation drills**, and **information-sharing platforms.**
- Large digital players should share anonymized threat data with smaller companies to **help prevent similar attacks.**

9.7 MAKE CYBER INSURANCE MORE ACCESSIBLE

- Cyber insurance policies should be **promoted among SMEs** in digital trade.
- Insurance firms must be encouraged to offer

affordable, customizable cyber insurance plans that include breach response support.

10. LIMITATIONS OF THE STUDY

- The study relies heavily on secondary data, which may lack real-time insights into evolving threats.
- Access to confidential breach data from trading firms was limited, affecting the depth of case analysis.
- Interviews were conducted with a limited number of cybersecurity professionals, which may affect generalizability.
- The comparative framework, while informative, may not capture nuanced policy variations in each country.

11. FUTURE SCOPE

- Future research can focus on primary data collection through structured surveys across various Indian trading platforms.
- Longitudinal studies can be conducted to monitor the effectiveness of cyber risk policies over time.
- Sector-specific studies (e.g., cryptocurrency exchanges or B2B trading platforms) could provide deeper insights.
- Evaluation of AI and blockchain-based governance systems in cybersecurity can open up innovative research avenues.

12. CONCLUSION

India's digital trading sector has grown rapidly in recent years. With this growth, however, comes an increased risk of cyberattacks. Our study shows that online platforms in India—whether for e-commerce, stock trading, or payments—are becoming more common targets for hackers. These attacks can lead to serious problems like stolen customer data, financial loss, and damaged trust among users. The data we analyzed from 2017 to 2021 clearly shows rising trends in cyber incidents, especially in e-commerce and digital payment sectors. While companies have made progress in adopting tools like firewalls and two-factor authentication, there are still weak areas—such as third-party vendor management and employee training.

Compared to global practices, India still lacks a central authority to govern cybersecurity across sectors. Countries like Singapore and the United States have well-defined policies and centralized bodies that regularly monitor, guide, and enforce cyber hygiene across digital platforms. India needs a similar approach.

In conclusion, for India to ensure safe and secure digital trading, there must be a collective effort from businesses, the government, and technology partners. Regular audits, proper employee education, secure software practices, and tighter vendor controls must become part of every company's routine. At the same time, the government should create a single national body for overseeing cybersecurity in digital commerce. Only then can the country protect its growing digital economy and build long-lasting user trust in its online platforms.

REFERENCES

1. CERT-In. (2017). *Annual Report 2016-17*. Ministry of Electronics and Information Technology, Government of India. https://www.cert-in.org.in/

2. CERT-In. (2018). *Annual Report 2017-18*. Ministry of Electronics and Information Technology, Government of India. https://www.cert-in.org.in/

3. CERT-In. (2019). *Annual Report 2018-19*. Ministry of Electronics and Information Technology, Government of India. https://www.cert-in.org.in/

4. CERT-In. (2020). *Annual Report 2019-20*. Ministry of Electronics and Information Technology, Government of India. https://www.cert-in.org.in/

5. CERT-In. (2021). *Annual Report 2020-21*. Ministry of Electronics and Information Technology, Government of India. https://www.cert-in.org.in/

6. PwC India. (2021). *Cybersecurity in India: Threat Landscape and Industry Response*. https://www.pwc.in

7. Deloitte India. (2021). *Digital Risk Management in India: 2021 Tech Risk Report*. https://www2.deloitte.com/in

8. KPMG. (2020). *Third-Party Risk Management Survey India 2020*. https://home.kpmg/in

9. NASSCOM-DSCI. (2020). *Cybersecurity Services Landscape in India*. Data Security Council of India. https://www.dsci.in

10. Reserve Bank of India. (2020). *RBI Master Direction on Digital Payment Security*. https://www.rbi.org.in

11. SEBI. (2018). *Cyber Security and Cyber Resilience Framework for Stock Brokers*. Securities and Exchange Board of India. https://www.sebi.gov.in

12. Ministry of Electronics & IT. (2017). *Digital India Programme Overview*. Government of India. https://digitalindia.gov.in

13. IDC India. (2021). *FutureScape: Cybersecurity Predictions for India 2021*. IDC Research India Pvt. Ltd.

14. Ernst & Young. (2019). *Global Information Security Survey 2019–20: India Insights*. https://www.ey.com/en_in

15. Singh, P., & Sharma, R. (2019). Cybersecurity challenges for Indian e-commerce platforms. *International Journal of Digital Security and Forensics*, 11(3), 140–154.

16. Mehta, S., & Varma, A. (2018). Third-party risk and governance in Indian fintech. *Journal of Financial Cybersecurity*, 6(2), 98–112.

17. World Economic Forum. (2020). *Global Cybersecurity Outlook 2020*. https://www.weforum.org

18. IBM Security. (2020). *Cost of a Data Breach Report 2020 – India Edition*. https://www.ibm.com/security

19. Cybersecurity and Infrastructure Security Agency. (2021). *Cyber Essentials Toolkit*. U.S. Government. https://www.cisa.gov

20. National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1). https://www.nist.gov/cyberframework

21. OECD. (2020). *Digital Security Risk Management for Economic and Social Prosperity*. OECD Publishing. https://www.oecd.org

22. Cyber Security Agency of Singapore. (2020). *Singapore Cybersecurity Strategy 2020*. https://www.csa.gov.sg