Page 1165 - 1182 **DOI:** *https://doij.org/10.10000/IJLMH.116844*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 1

2024

The Jurisprudential Landscape of Cyber Resilience: Legal Obligations and Liability of Stock Exchanges, Market Participants and Intermediaries

MRADUL PRAKASH AGNIHOTRI[1]

ABSTRACT

The article examines how cyber security and financial stability connect critically inside the Indian legal system in the age of digital financial markets. In order to protect India's financial ecosystem from cyber attacks, this in-depth analysis examines the legal responsibilities and responsibilities of key players, including stock exchanges, market participants, and intermediaries. It draws attention to the difficulties, changing nature of cyber threats, and possible directions for development in an ever-changing environment. In the context of India's developing financial markets, the essay highlights the critical significance of cyber resilience for maintaining market integrity and investor trust by illuminating this jurisprudential landscape.

Keywords: *Cyber resilience, integrity, cyber attacks.*

I. INTRODUCTION

The capacity of a financial market to foresee, endure, contain, and quickly recover from a cyber attack is known as cyber resilience. Given that cyber attacks have the potential to impair investor confidence and interfere with the operation of financial markets; it is a crucial element of financial security.

Because securities markets rely so largely on information technology (IT) systems, they are especially susceptible to cyber assaults. Sensitive data, including trade, financial market, and client information, is processed and stored by these systems. The financial market and its players may be significantly impacted if this data is hacked.

By interfering with IT systems or falsifying market data, cyber attacks can potentially prevent the financial markets from operating as intended. This may result in price fluctuations, market closings, and market volatility.

[1] Author is a student at university of petroleum and energy studies, Dehradun, India.

 [ISSN 2581-5369]

The stability of financial markets also depends on confidence among investors. Investors may remove their money from the market if they start to doubt the safety of their assets, which might cause liquidity issues and unstable markets.

Because cyber security helps shield financial markets from cyber attacks, it is crucial for preserving market stability and investor confidence. Cyber attacks have the potential to impair investor confidence and interfere with the smooth operation of the financial markets, which can result in unpredictability in the markets, turbulence, and liquidity issues.

A financial market cyber attack might result in a variety of outcomes, such as:

- Market crashes and price dislocations might result from a disruption of the trading and settlement systems.
- Theft of private information: This might involve trade, financial markets, and consumer data. Then, this information may be exploited for illegal activities like insider trading or identity theft.
- Market data tampering: This might result in fictitious price swings including losses for investors.
- Reputational harm: A financial market's reputation might be harmed by a cyber attacks, which would also reduce investor trust.

The stability of financial markets and investor confidence depend on cyber resiliency. The Indian government is investing in cyber security infrastructure and publishing guidelines for market players as two of the many actions it is doing to encourage cyber resilience in the financial industry. To guarantee that the Indian financial industry is sufficiently shielded against cyber attacks, further work must be done.

II. BACKGROUND ON CYBER THREATS

The world of cyber threats is always changing, and financial markets are a popular target for attackers. Because they can impair confidence among investors, cause financial losses, and disrupt the operation of financial markets, cyber attacks on financial markets can have a substantial effect on the economy.

The sophistication of cybercriminals is rising, as is the complexity and targeting of their attacks. They are gaining access to sensitive data by taking advantage of fresh and creative ways to attack weaknesses in IT systems.

The following are a few of the most frequent cyberthreats that financial markets face:

 [ISSN 2581-5369]

- ***Illegal software:*** Illegal software, including ransomware and malware, may be used to extort money from financial institutions, compromise IT systems, and steal confidential information.
- ***Phishing attacks:*** Phishing attacks aim to deceive people into disclosing private information, such as credit card numbers and passwords.
- Attacks known as **denial of service (DoS)** aim to overload IT systems with traffic so that legitimate users are unable to access them.
- **Man-in-the-middle attacks:** These types of attacks aim to eavesdrop on conversations between two parties and take advantage of or alter data.

Insider threats refer to the risks that are presented by workers or outside contractors who possess permission access to confidential information and IT systems.

(A) Notable Cyber attacks on Financial Institutions in India

Numerous high-profile cyber attacks against Indian financial institutions have occurred in recent years. Among the most prominent attacks are the following:

- *2018 Cyber attacks against Cosmos Bank*: A cyber attacks against Cosmos Bank in 2015 led to the loss of more than Rs. 94 crore from the bank's ATMs. A group of hackers launched the attack, infecting the bank's IT systems and breaking into its ATM network with malware.
- *2018 SWIFT cyber attacks*: Numerous Indian banks' bank accounts were victims of a cyber attacks that struck the Society for Worldwide Interbank Financial Telecommunication (SWIFT) in 2018. By sending false messages that approved the movement of money from the banks' accounts, the attackers were able to enter the SWIFT messaging system through the use of malware.
- *2016 Yes Bank cyber attacks*: The bank had a cyber attacks in 2019 that led to the loss of more than Rs. 400 crore from its ATMs. A group of hackers launched the attack, infecting the bank's IT systems and breaking into its ATM network with malware.

(B) Need for Legal and Regulatory Responses to Cyber Threats

A legal and regulatory response is important given the dynamic nature of cyber risks and the rise in cyber attacks targeting financial institutions.

To guarantee that the Indian banking system is sufficiently shielded from cyber threats, further work must be done. In order to create and execute efficient cyber security measures, government

 [ISSN 2581-5369]

officials should collaborate with the business sector and keep funding cyber security research and development.

Global financial institutions are confronted with a significant problem in the form of cyber attacks. Financial institutions must take precautions against cyber attacks.

III. LEGAL FRAMEWORK FOR CYBER RESILIENCE

In the Indian financial markets, the legislative framework for cyber resilience is intricate and dynamic. Cyber resilience is not expressly covered by any one legislation or regulation, although many of the ones that are already in place are pertinent.

(A) Existing Laws and Regulations

Among the most important current laws and rules that are pertinent to cyber resilience in the Indian financial markets are listed below:

The Information Technology Act of 2000: This legislation offers a framework for handling cybercrime and safeguarding digital information.

- SEBI Act, 1992: The Securities and Exchange Board of India SEBI is empowered by this law to oversee the securities industry and safeguard investors' interests. A variety of cyber security rules have been released by SEBI for market players, such as investment banks, brokers, and stock exchanges.
- The 2013 Companies Act: The prerequisites for businesses looking to list their shares on a stock market are outlined in this statute. These prerequisites include putting in place suitable safety precautions and having a plan for cyber security authorized by the board.
- The Act of 2007 for Payment and Settlement Systems: In India, payment and settlement mechanisms are governed by this law. Payment system operators can refer to the cyber security guidelines released by the RBI.

(B) International and Domestic Regulation Bodies, Guidelines, and Standards

Cyber resilience in financial markets is impacted by a multitude of national and international standards, guidelines, and regulatory organizations in addition to the rules and regulations now in place.

Some of the most important international recommendations and standards are as follows:

- IEC/OSI 27001: This is a worldwide norm for systems that handle the security of information.

- The National Institute of Standards and Technology (NIST) in the United States created the NIST Cyber security Framework.
- A framework for G7 cyber security for financial institutions was created by the G7 nations.

Some of the most important national standards and recommendations are as follows:

- RBI's Cyber security Guidelines for Payment System Operators: The RBI released these recommendations in 2016.
- SEBI Cyber security Guidelines for Securities Market Participants: SEBI released these rules in 2018.

Several of the major statutory organisations in India in charge of cyber security are as follows:

- India's Reserve Bank (RBI): The RBI, which serves as India's central bank, is in charge of overseeing the banking and financial industries.
- India's main securities market regulator is the Securities and Exchange Board of India (SEBI).
- CERT-In (Indian Computer Emergency Response Team): The national organisation CERT-In is in charge of handling and minimising cyber incidents.

In the Indian financial markets, the legislative framework for cyber resilience is intricate and dynamic. Nonetheless, a variety of current laws, rules, national and international standards and recommendations, and regulatory organisations are pertinent to cyber resilience. In terms of cyber security, stock exchanges, market players, and intermediaries have several obligations.

The following further steps should be taken by the Indian government to fortify the legal foundation for cyber resilience in the financial markets:

1. Pass a data protection law requiring financial institutions to put in place suitable security measures to safeguard client information.
2. Make amendments to the Information Technology Act to add particular cyber security Sections for the banking industry.
3. Create a section specifically committed to investigating and prosecuting cybercrimes.
4. Improve the exchange of information about cyber threats by government agencies and financial institutions in concert.

The Indian government may assist in fortifying the financial sector's cyber resilience and

 [ISSN 2581-5369]

shielding investors from the escalating risk of cyber attacks by implementing these measures.

IV. STOCK EXCHANGES AND CYBER RESILIENCE

In order to maintain the financial markets' cyber resilience, stock exchanges are essential. They are in charge of offering a safe environment for securities trading and clearing. They assist in keeping an eye on and reducing cyber threats.

Stock exchanges can take the following particular measures to ensure cyber resilience:

Put in place a thorough cyber security programme with the following components:

a. Risk evaluation

b. Safety measures

c. Reaction to incidents

d. Knowledge and instruction

e. Regularly inspect and test cyber security systems to find and fix weaknesses.

f. Disseminate cyber threat intelligence to government organisations and other market players.

g. Assist regulatory organisations in the examination and litigation of cyber offences.

(A) Legal Obligations of Stock Exchanges in Terms of Cyber security.

Stock exchanges are subject to certain legislative requirements regarding cyber security. These responsibilities stem from several origins, such as the following:

1. ***The SEBI Act of 1992*** established the Securities and Exchange Board of India. The SEBI Act bestows SEBI the authority to oversee the securities industry and safeguard the welfare of investors. SEBI has released many cyber security guidelines for stock exchanges, which include the following:

a) SEBI Cyber security Guidelines for Securities Market Participants

b) The SEBI Guidelines for Stock Exchange Information Security

2. ***Companies Act, 2013:*** This law lays out the conditions that businesses must meet in order to list their shares on a stock market. These prerequisites include putting in place suitable safety precautions and having a cyber security policy authorised by the board.

3. ***Information Technology Act, 2000***: This law establishes a framework for combating cybercrime and safeguarding electronic information.

 [ISSN 2581-5369]

(B) Stock Exchange's Liability in the Event of a Cyber Breach

If a cyber breach causes losses for market participants, stock exchanges could be held accountable. The particulars of the case, such as the following elements, will determine the amount of the stock exchange's liability:

1) Did the stock exchange take appropriate precautions against cyber attacks to safeguard its data and systems?
2) Is the stock exchange in compliance with all relevant legal and regulatory requirements?
3) Did the stock exchange's wrongdoing or carelessness play a part in the cyber attacks?

(C) Certain sections of the statutes

The statutes contain the following particular Sections that are pertinent to stock exchanges' responsibility in maintaining cyber resilience and their liability in the case of a cyber breach:

a. Securities and Exchange Board of India (SEBI) Act, 1992:

Section 11: SEBI's authority to safeguard investors' interests.

Section 12: The Securities Market Regulation Authority of India (SEBI).

Section 12A(c): Mandates that stock exchanges create and keep an information security policy as part of their risk management system.

Section 12A(d) : Mandates that stock exchanges have a business continuity and disaster recovery strategy in place.

b. Companies Act, 2013:

Section 134: Board-approved cyber security policies are required for businesses.

Section 143: Businesses must put in place suitable security measures.

c. Information Technology Act, 2000:

Section 43: Penalties for Computer System Damage.

Section 66: Outlines the penalties for data theft and hacking.

In order to maintain the financial markets' cyber resilience, stock exchanges are essential. Therefore may be held accountable for damages suffered by market participants as a result of a cyber breach, and they are subject to certain regulatory requirements regarding cyber security. Stock exchanges should follow every regulation that applies and take every measure possible to safeguard their systems and data against cyber attacks.

 [ISSN 2581-5369]

V. MARKET PARTICIPANTS' OBLIGATIONS

In order to ensure cyber resilience, market participant such as portfolio managers, investment companies, and broker-dealers have a variety of obligations.

Among these duties are: Putting in place an extensive cyber security programme that covers responding to incidents, security controls, risk assessment, and awareness and training.

Testing and conducting routine cyber security audits in order to find and fix vulnerabilities.

Exchanging cyber threat intelligence with the government and other industry players.

Working together with law enforcement to investigate and prosecute cybercrimes.

The legislation imposes particular obligations on market participants in addition to these broad obligations.

(A) Legal and Regulatory Requirements for Market Participants

Some of the most important statutory and regulatory prerequisites for market players to uphold cyber resilience are as follows:

- SEBI Cyber security Guidelines for Securities Market Participants: Market players must put in place a variety of cyber security measures in accordance with these principles, including risk assessment, security controls, incident response, and awareness and training campaigns.
- RBI's Cyber security Guidelines for Payment System Operators: Payment system operators are required by these standards to put in place several cyber security measures, such as risk assessment, security controls, incident response, and awareness and training.
- An international standard for information security management systems is ISO/IEC 27001. Several market players are compelled by their authorities or clients to adhere to ISO/IEC 27001 standards.

VI. POTENTIAL LIABILITY FOR MARKET PARTICIPANTS IN THE EVENT OF A BREACH

If market participants don't take reasonable precautions to secure their systems and data, they could be held accountable for damages in the case of a cyber breach.

Depending on the particulars of the case, a market participant's unique obligation in the event of a cyber breach may vary. On the other hand, market players could be accountable for

carelessness, contract violations, or fiduciary obligation violations.

(A) Specific Sections from the Statutes

The statutes contain the following particular Sections that pertain to market players' obligations to preserve cyber resilience:

- ***Section 11 of the SEBI Act, 1992:*** This Section grants SEBI the authority to create regulations to safeguard investors' interests and ensure the securities market develops in a systematic manner.
- ***Section 134 of the 2013 Companies Act:*** Companies that are listed on a stock market are required under this provision to have a cyber security policy authorised by the board and to put in place the necessary security measures
- ***Section 43 of the Information Technology Act of 2000*** criminalises unauthorised computer system misuse as well as data loss or destruction.

In order to preserve cyber resilience, market players have many duties. In addition to being bound by certain legal and regulatory obligations, they could also be held accountable for damages in the case of a cyber breach.

By putting in place a thorough cyber security programme, performing frequent cyber security audits and testing, exchanging cyber threat intelligence, and working with law enforcement, market players may lower their chance of a cyber breach and the responsibility that goes along with it.

Market players may contribute to defending the Indian financial industry against cyber attacks by implementing these precautions.

VII. INTERMEDIARIES' ROLE AND LIABILITY

The function of intermediaries is crucial in the financial markets. They offer crucial services including payment processing, confinement, and settlement and clearing to market players.

Trading between market players is settled via clearinghouses. This entails making certain that sellers and purchasers get the money and securities they are entitled to.

Custodians are in charge of keeping their clients' securities secure. In addition, they offer a variety of other services including proxy voting and dividend collecting.

The task of processing payments between market players falls to payment processors. This covers both conventional paper-based payments and electronic payments.

(A) Legal Obligations and Potential Liability of Intermediaries

There are several legal requirements for intermediaries with regard to cyber security. Additionally, they could be held accountable in the case of a cyber attacks.

Some of the most important legal responsibilities that intermediaries have with regard to cyber security are as follows:

SEBI Cyber security Guidelines for Securities Market Participants: Intermediaries must put in place a variety of cyber security measures in accordance with these principles, including risk assessment, security controls, incident response, and awareness and training campaigns.

RBI's Cyber security Guidelines for Payment System Operators: Payment system operators are required by these standards to put in place several cyber security measures, such as risk assessment, security controls, incident response, and awareness and training.

If intermediaries don't take reasonable precautions to safeguard their systems and data, they might be held accountable for damages in the case of a cyber breach.

Depending on the specifics of the case, an intermediary's culpability in the event of a cyber breach may vary. Intermediaries, nevertheless, can be held accountable for carelessness, contract violations, or fiduciary obligation violations.

(B) Third-Party Risk and the Duty of Care Imposed on Intermediaries

Third-party risk exists for intermediaries. This is the chance that a cyber attacks on a third party they do business with might jeopardise their systems and data.

It is the intermediaries' responsibility to their customers to take reasonable precautions to reduce the danger to third parties. This entails forcing third-party providers to put in place the necessary cyber security safeguards and doing due diligence on them.

The laws contain the following particular portions that are pertinent to the legal requirements and possible liabilities of intermediaries with regard to cyber security:

- Section 11 of the SEBI Act, 1992: This Section grants SEBI the authority to create regulations to safeguard investors' interests and ensure the securities market develops in a systematic manner.
- Companies that have been listed on a stock market are required by Section 134 of the Companies Act, 2013 to have a cyber security policy authorised by the board and to put in place suitable security measures.

 [ISSN 2581-5369]

- Section 43 of the Information Technology Act of 2000 criminalises unauthorised computer system access as well as data loss or destruction.

Although they are essential to the financial markets, intermediaries also carry a high risk of cyber attacks. In the case of a cyber breach, intermediaries may be held accountable for damages and have a variety of legal duties pertaining to cyber security.

By putting in place an extensive cyber security programme, doing routine cyber security audits and testing, exchanging cyber threat intelligence, and working with law enforcement, intermediaries may lower their chance of a cyber breach and the liability that goes along with it.

By forcing third-party suppliers to adopt suitable cyber security measures and doing due diligence on them, intermediaries may also help reduce third-party risk.

VIII. CASE STUDIES AND RECENT DEVELOPMENTS

An examination of case studies and legal responses pertaining to cyber resilience in Indian financial markets

The frequency and extent of cyber security events in the Indian financial markets have increased, highlighting the urgent need for strong cyber resilience. In this part, we outline current legislative and regulatory changes that are in line with the Indian legal framework, analyse the legal ramifications and remedies, and give important case studies of cyber events in the Indian financial industry.

Case Study 1: The Cosmos Bank Cyber Heist

A hack at Pune's Cosmos Cooperative Bank in August 2018 led to the unauthorised movement of more than ₹94 crore. Through the use of malware, the attackers gained access to the bank's computers and stole money. This event exposed the weaknesses of financial institutions and prompted the Pune Cyber Police to launch investigations. The RBI then published a circular emphasising the necessity of more stringent cyber security measurements, such as increased reporting and surveillance obligations.

Case Study 2: The NSE Co-location Controversy

In 2009, the NSE introduced the colocation facility, which charges a fee to traders and brokers to set up their IT servers on its property. In 2015, a whistleblower wrote to Sebi, accusing a few brokers of manipulating the market by taking use of a feature that allowed them to acquire data more quickly. According to the complaint, Narain and Ramkrishna enabled OPG Securities' fraud by failing to take appropriate action, and OPG Securities was granted preferred access to

 [ISSN 2581-5369]

NSE's backup servers.

The National Stock Exchange (NSE) was involved in a dispute about claims that select brokers were given preferential treatment and improper access to its co-location facilities. Even while this particular incident isn't common, it nonetheless serves as a reminder of how crucial it is to preserve the integrity of the financial market infrastructure. After a thorough inquiry, the regulatory body SEBI issued a penalty order (in September 2019) against the NSE, making it answerable for system and co-location service failures.

Case Study 3: The Data Breach at CAMS

A data breach occurred in October 2020 at the Computer Age Management Services (CAMS), which manages investor services and mutual fund transactions. Data privacy in the banking industry is a worry after sensitive client information was made public. The event highlighted the rising significance of data security legislation in the banking industry by making quick reporting mandatory under the Personal Data Security Bill (PDPB).

(A) Legal Consequences and Responses

Legal repercussions were applied in each of these instances to cope with the security breaches and failures in cyber resilience:

The heist at Cosmos Bank: Arrests were made as a consequence of the inquiry, and the bank was forced to strengthen its cyber security protocols. The event brought to light financial institutions' obligations under the IT Act, including Section 43A, which stipulates data protection and negligence responsibility.

Co-location of NSE Controversy: SEBI's penalty ruling demonstrates the regulatory body's dedication to upholding market integrity. This instance illustrates SEBI's function in upholding the impartiality and honesty of the market.

Data Breach at CAMS: The event brought to light the changing state of data protection in India. Data breaches like this might result in serious fines under the PDPB (if passed), which emphasises the necessity for strong data protection measures.

(B) Recent Legislative and Regulatory Developments

The following significant legal and regulatory changes have been made to strengthen cyber resilience in the Indian financial markets:

- ***Personal Data Protection Bill (PDPB):*** Entities must invest in data protection and data breach response systems since the PDPB, which is likely to be

enacted soon, will have a substantial influence on how personal data is handled in the financial industry.

- ***Reserve Bank of India (RBI) Circulars:*** The RBI has published a number of circulars emphasising the value of cyber resilience and concentrating on risk management and cyber security.
- ***Securities and Exchange Board of India (SEBI) recommendations:*** In reaction to the NSE co-location dispute, SEBI was quick to issue recommendations that emphasised the significance of fair and equal access to market infrastructure.

To sum up, the state of cyber resilience in the Indian financial markets is changing, as evidenced by noteworthy case studies, ramifications for the law, and reactions from regulators. To maintain the market's equilibrium and investor confidence, Indian financial institutions, stock exchanges, and market players must be alert and follow the constantly changing legal and regulatory requirements as cyber dangers continue to evolve and proliferate. Furthermore, in order to prosper in India's ever-changing financial environment, strong cyber security safeguards and data protection practices must be put in place.

IX. CHALLENGES AND FUTURE DIRECTIONS

Cyber resilience is an area that is developing along with the digitization and evolution of the Indian financial sector. It is imperative that the banking industry be shielded from cyber dangers. This section looks at the difficulties that stock exchanges, market players, and intermediaries have while trying to improve cyber resilience in the context of Indian law. We also explore the dynamic nature of cyber threats and make predictions about possible future advancements in legal and regulatory frameworks for cyber resilience.

(A) Challenges in Enhancing Cyber Resilience

1. ***Resource constraints:*** Investing in cutting-edge cyber security equipment and staff is difficult for many Indian financial firms, particularly smaller intermediaries, due to limited resources. Many times, building cyber resilience involves large financial investments, which may not be within the means of all market players.

2. ***Skills Gap:*** Professionals with cyber security experience are in great demand, but it can be challenging to locate and keep them. In India, where there is a severe shortage of skilled labour, financial institutions have to fight with other industries to hire the few available professionals.

 [ISSN 2581-5369]

3. *Outdated Systems:* Despite the potential absence of safety measures compared to current technology, certain market players and intermediaries continue to rely on outdated systems. These system upgrades can be expensive and time-consuming.

4. *Risks Associated with Third Parties*: Intermediaries frequently work with different third-party service providers. Ensuring that these third parties follow stringent cyber security guidelines is crucial, as security lapses at third-party suppliers can have an adverse impact on the financial system.

5. *Regulatory Compliance:* It may be quite difficult to navigate the intricate web of rules and regulations. Financial firms are required to make sure that they are adhering to several regulatory authorities' requirements, such as SEBI, RBI, and IRDAI.

(B) The Evolving Nature of Cyber Threats

The Indian financial markets are subject to a constantly evolving and dynamic landscape of cyber threats. Threat actors are always changing to take advantage of new weaknesses and developments in technology. We have seen the following tendencies arise in recent years:

1. ***Complex Ransomware assaults***: Critical financial infrastructure is the target of increasingly complex ransomware assaults. Attackers are putting victims through a great deal of financial hardship as they seek more and larger ransoms.
2. ***Supply Chain Attacks:*** Because the financial ecosystem is interconnected, adversaries take advantage of supply chain weaknesses. Targeting software developers or other service providers who have access to private information is one way to achieve this.
3. ***Social Engineering:*** Cybercriminals are skilled at taking advantage of weaknesses in people. Social engineering techniques and phishing assaults have improved in convincingness and difficulty of detection.
4. ***Nation-State Actors:*** The geopolitical aspect of cyber security has been enhanced by nation-states' participation in cyber attacks. Financial institutions might be the target of state-sponsored entities looking to obtain intelligence or destabilise the economy.

(C) Future Developments in Cyber Resilience Laws and Regulations

In the Indian context, a number of prospective future advancements in cyber resilience legislation and regulations may be foreseen in order to handle these issues and growing threats:

1. ***Unified Cyber security Framework:*** An all-encompassing, uniform framework that unifies current cyber security laws and clarifies norms and responsibilities for the financial industry.

 [ISSN 2581-5369]

2. ***Mandatory Cyber Insurance:*** Rules requiring cyber insurance should be taken into consideration in order to reduce monetary damages brought on by cyber events and encourage market players to make investments in cyber resilience.
3. **Tougher fines:** To ensure that financial organisations have strong incentives to defend against cyber attacks, stricter fines for breaking cyber security standards and data protection laws have been implemented.
4. ***Public-Private Collaboration:*** To promote information sharing and cooperative cyber security efforts, there should be more coordination between the public and private sectors, regulatory agencies, and the government.
5. ***Regularised Training and Certification:*** Programmes that encourage cyber security education and certifications in order to close the skills gap, backed by financial rewards for organisations who hire qualified personnel.
6. ***Cross-Border collaboration:*** To counter cross-border cyber threats and harmonise cyber security standards, more collaboration with international organisations and neighbouring nations is necessary.

Improving cyber resilience in the Indian financial markets is a complex task that calls for cooperation from regulatory agencies, stock exchanges, and market players. Because cyber threats are always changing, cyber security tactics must also be constantly innovative and adaptable. We believe that rules and regulations will change in the future to reflect the rising significance of cyber resilience and to guarantee the security and stability of India's financial ecosystem.

X. CONCLUSION

The significance of cyber resilience in the dynamic Indian financial markets cannot be emphasised. By navigating the complex web of cyber security issues and regulatory nuances, this essay has thrown light on the vital role that stock exchanges, market players, and intermediaries play in protecting India's financial sector from the ever-increasing danger posed by cyber events.

(A) Key Findings and Insights

During our investigation, a number of significant conclusions have been made:

1. ***Cyber Resilience Is Non-Negotiable:*** It is a need rather than a luxury. It is the last line of defence against enemies who want to undermine investor confidence and disturb

market stability. A number of recent events in the Indian financial markets have highlighted the stakes in terms of money and reputation.

2. ***Financial Actors Have Major Legal requirements:*** India's legal system imposes heavy legal requirements on them. Due to the potential for legal ramifications and reputational harm, stock exchanges, market participants, and intermediaries are accountable for maintaining cyber security and data protection.
3. ***Changing Dangers Require Constant Adaptation***: Cyber threats are always changing in nature. Social engineering techniques, supply chain intrusions, and ransomware are just a few instances of the ever-changing environment. Financial organisations must thus constantly modify and improve their cyber security plans.

(B) The Future of Cyber Resilience in India

It is clear that cyber resilience will become progressively more crucial to India's financial markets as time goes on. In light of this, the following factors are crucial:

1. ***Harmonised Legal Frameworks***: It is crucial to have a single, all-encompassing legal framework for data protection and cyber security. This would make duties clearer, lighten the load on compliance, and enable a better-coordinated defence against cyber attacks.
2. ***International collaboration:*** Worldwide cooperation is essential in the field of cyber security in a world that is interconnected. In order to successfully address cross-border cyber threats, India has to collaborate with its neighbouring nations and international organisations.
3. ***Education and Training:*** Human interaction is essential to cyber security. To close the skills gap, funding for education and certification initiatives is essential. This will enable financial institutions to defend themselves against cyber attacks more effectively.
4. ***Resilience Incentives:*** To promote a cyber-resilience sprint to the top, regulatory agencies have to think about providing incentives for organisations that exhibit outstanding cyber security practices.

In conclusion, given India's quickly developing financial markets, cyber resilience is not only a distant ideal but an urgent necessity. The regulatory framework, stock exchanges, market players, and intermediaries must work together to protect these markets from cyber dangers if they are to remain stable, honest, and trustworthy. The road ahead may be difficult, but in order

 [ISSN 2581-5369]

to safeguard its technological future, India's financial industry must travel it with unshakeable resolve. We must all work together to make sure that the financial system is firm and resistant to even the most tenacious cyber storms as it rapidly moves towards a future where technology will play a bigger role.

*****

 [ISSN 2581-5369]

XI. APPENDICES

1. https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=1721
2. https://www.sebi.gov.in/legal/circulars/aug-2023/guidelines-for-miis-regarding-cyber-security-and-cyber-resilience_76056.html
3. https://www.sebi.gov.in/legal/circulars/jun-2022/circular-on-modification-in-cyber-security-and-cyber-resilience-framework-of-mutual-funds-asset-management-companies-amcs-_59611.html
4. https://www.sebi.gov.in/legal/circulars/aug-2023/modification-in-cyber-security-and-cyber-resilience-framework-of-stock-exchanges-clearing-corporations-and-depositories_75887.html
5. https://www.sebi.gov.in/sebi_data/attachdocs/1456380272563.pdf
6. https://www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf
7. https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-for-stock-brokers-depository-participants_41215.html
8. https://indianexpress.com/article/cities/pune/cosmos-bank-malware-attack-interpol-issues-red-corner-notice-against-prime-suspect-traced-in-foreign-country-6574097/
9. https://economictimes.indiatimes.com/industry/banking/finance/banking/city-union-loses-2-million-in-cyber attacks-retrieves-half/articleshow/62956557.cms?from=mdr
10. https://www.livemint.com/Industry/Ope7B0jpjoLkemwz6QXirN/SBI-Yes-Bank-MasterCard-deny-data-breach-of-own-systems.html

*****

 [ISSN 2581-5369]