Cyber Security and The Role of Cyber Insurance in Financial Institutions

Alok Gupta

Assistant Professor, Department of Financial Studies,
V.B.S. Purvanchal University, Jaunpur, U.P.

Email Id: alokmfc76@gmail.com

ABSTRACT

Financial services, which play an essential role in the economy, are fast to embrace new technology that will benefit their customers and help them run their businesses more smoothly. The safety of their customers' private data and the honesty of their financial dealings are therefore essential concerns for banks. The widespread usage of these cutting-edge technology has, however, led to a significant increase in the number of cyber security vulnerabilities. To mitigate the impact of internet-related hazards, banks may decide to get cyber insurance, which covers both persons and companies. The main objective of this study is to investigate the current and potential cyber hazards to India's banking system, as well as the function of cyber insurance in reducing these risks. The essay goes even farther by analyzing the various cyber insurance policies provided by Indian businesses.

Keywords: Cyber Security, Cyber Insurance

INTRODUCTION

Since technology advancements have changed the way banks operate, the significance of cyber security has grown in the modern digital age. Payment processors, banks, investment firms, and insurance companies are the targets of cybercriminals. Financial institutions are particularly at risk because to their significance to the economy and their dependence on digital technology to deliver services. The proliferation of cyber risks and the volume of sensitive data transactions have made robust cyber security measures a must for financial institutions.

There is a never-ending stream of new forms of cybercrime that threaten internet security, from phishing and ransom ware to advance persistent threats (APTs) and more. According to the International Monetary Fund (IMF), cyber risks are on the rise in the global financial system, prompting regulatory bodies to emphasize the need for more cyber resilience among financial institutions. Beyond monetary losses, cyber-attacks have far-reaching implications. Damage to one's brand, penalties from regulators, and consumer distrust are all possible outcomes. Threat detection, constant monitoring, risk assessment, and incident response should all be part of a comprehensive cyber security architecture that financial institutions have in place to safeguard their assets and maintain stakeholder confidence.

As the complexity of cyber risks continues to rise, cyber insurance has become a crucial component of risk management strategies for financial institutions. Companies can protect themselves by purchasing cyber insurance, which allows them to shift part of the risk associated with cyber-attacks to an insurance company. As the expenses of cyber disasters keep rising through the roof, this kind of financial security is becoming more vital. According to Cyber security Ventures, the annual cost of cybercrime is expected to surpass $10.5 trillion by 2025, highlighting the urgent need for effective risk mitigation strategies. Cyber insurance may assist organizations strengthen their cyber defences by compensating them

monetarily in the event of a cyber-incident and by incentivizing them to take robust preventative actions.

Cyber insurance and cyber security must collaborate if banks are to keep up with the dynamic nature of cyber threats. Insurance firms are increasingly going the extra mile to ensure policyholders comply with cyber security regulations by requesting proof of compliance. By fostering a sense of accountability, this dynamic relationship encourages financial institutions to invest in measures that reduce their overall cyber risk. Companies are under increasing pressure from regulators to include cyber insurance into their risk management strategies so that they may meet industry standards and laws.

The Current Cyber Threat Landscape

Cybercriminals' methods of attack against the banking sector are evolving and becoming more sophisticated. Criminals employ a wide variety of tactics while trying to enter financial networks in order to steal sensitive data, conduct fraudulent transactions, or halt operations. A growing number of ransom ware assaults have the banking industry on edge. In these attacks, hackers encrypt firm data and demand money to recover it. Ransom ware attack on Colonial Pipeline is only one example of how high-profile events may cause significant financial and operational damage.

Parallel to ransom ware, phishing efforts are frequent and seek to gain sensitive data by deceiving victims into disclosing personal details. Cyber security and Infrastructure Security Agency's (2023) Cyber security Threat Trends Report details the prevalence of attacks on financial institutions employing advanced phishing methods masquerading as official mail. The goal of these deceitful tactics is to get victims to divulge personal information that might be used for fraud or identity theft.

In addition, the proliferation of internet-connected devices and the development of the Internet of Things (IoT) pose additional risks to financial systems. When businesses use smart technology to improve operational efficiency, they unintentionally make themselves more vulnerable to theft by increasing the number of potential entry points for criminals. Based on this, the banking industry needs to be on high alert all the time to spot threats and take action against them.

The Importance of Cyber Security in Financial Institutions

The importance of banks and other financial institutions to the economy makes robust cyber security measures paramount. Cyber security is an integral aspect of any company's overarching strategy and impacts every facet of the business. An organization's credibility, financial resources, and legal standing can all take a serious hit in the event of a cyber-security incident.

Using a combination of people, processes, and technology, financial institutions may better defend themselves against cyber-attacks. Part of this includes making sure that staff receive regular cybersecurity awareness training, putting in place advanced threat detection systems, and making strategies for when incidents occur. To ensure effective cyber security, it is vital to use best practices like encryption and multi-factor authentication to safeguard sensitive data. Additionally, frequent risk assessments should be carried out to identify any vulnerabilities.

Global regulatory bodies have responded to the financial industry's cyber security concerns by developing guidelines and recommendations. Companies are required to develop cyber security policies that follow certain requirements by the NYDFS to ensure that New York financial institutions are ready to handle cyber-attacks.

The Evolution of Cyber Insurance

The proliferation and complexity of cyber assaults have led to a rise in the popularity of cyber insurance. Cyber insurance, while considered an ancillary product, is now an essential tool for risk management for financial organizations. Standard insurance policies don't necessarily cover the unique risks presented by cyber incidents, which is why this transition is happening.

Insurance against cybercrime often pays for data restoration, legal bills, regulatory fines, and PR costs. Some insurers have responded to the skyrocketing cost of cyber insurance by creating specialized coverage for financial institutions like banks. This accounts for the expenses incurred by the company directly (first-party losses) as well as any indirect costs (third-party losses) that may result from claims filed by partners or consumers affected by a data breach.

Insurers are also ahead of the curve when it comes to offering policyholders with risk management solutions. A lot of insurance firms now want to see evidence of how secure a company is online before they'll insure it. Completing third-party audits, conducting security assessments, or providing evidence of implemented safeguards may all be necessary steps in this process. When these rules push institutions to invest in robust cyber defenses, it may promote a culture of accountability and less risk.

OBJECTIVE OF THE STUDY

1. To evaluate the effectiveness of the cyber security measures used by financial institutions.
2. To study the emerging cybersecurity threats faced by the banking sector in India.
3. To analyze the significance of cyber insurance for the banking sector in India and examine various cyber insurance models offered by Indian insurance companies.

REVIEW OF LITERATURE

Bhattacharya and Kumar (2019) Delve into the several aspects of cyber dangers impacting the Indian banking industry, drawing attention to how these threats undermine customer confidence and endanger the financial viability of organizations. The research highlights the dynamic character of cyberattacks, pointing out that they are becoming increasingly complex and focused, especially on financial institutions and service providers.

Agarwal and Jain (2018) Proceed by discussing the present state of cyber security in Indian banks. The rapid advancement of technology, inadequate infrastructure, and a shortage of skilled laborers are highlighted as major obstacles that result in vulnerabilities. Some organizations have invested much in cyber security, but their research shows that there are still gaps that need to be plugged before they can guarantee total protection.

Choudhary and Singh (2018) find out which methods employed by Indian banks were most effective. Their study found that banks with an incident response plan, educated staff, and a regular audit schedule had a lower likelihood of incident breaches. The authors suggest a standardized cyber security architecture for the whole industry to make it more resistant to cyber-attacks.

Bansal and Gupta (2017) Learn more about cyber insurance and how it may help mitigate the financial impact of cyber disasters. In light of the increasing number of cyber risks, their research suggests that financial institutions should seriously consider purchasing cyber insurance. Cyber insurance may be financially beneficial to firms and encourages them to enhance their security procedures, according to the report.

Desai and Nair (2016) address the specific challenges of cyber risk management in Indian banks. They highlight the complexities involved in integrating cybersecurity measures into existing risk management frameworks. The authors point out that regulatory compliance, combined with the need for ongoing risk assessments and updates to security protocols, poses significant hurdles for banks aiming to fortify their defences against cyber threats.

Manwaring, Kayleen & Hanrahan, Pamela. (2010) The Banking Executive Accountability Regime's implementation process commenced in February 2018. The new information security Prudential Standard CPS 234 was finally made public for review after APRA waited a month to disclose the preliminary version. This result was reached as a result of the offered comments and ideas. The first "key requirement" is that all organizations that are regulated by APRA must "clearly define the information-security related roles and responsibilities of the Board and of senior management, governing bodies, and individuals." The first "key requirement" in the draft is this particular quality of the demand. This article will analyze the circumstances surrounding each director of a financial institution that has had a cyber security breach that has affected customer data, systems, or infrastructure. The primary motivation for doing this research is to analyze the results of these modifications. According to the study's findings, these modifications lay the framework for how the public and authorities would see the responsibilities of directors in encouraging the implementation of adequate cyber security measures. In turn, this expectation affects the degree of care that is required of directors.

RESEARCH METHODOLOGY

The Increasing Relevance of Cyber Insurance in the Indian Banking Sector" is the title of the research that was carried out after collecting qualitative data. Rephrasing, it's when one makes use of other people's work to back up their own arguments and findings. This study mostly relies on books, journals, and publications published by the government. You may compare plans from several Indian firms that offer cyber insurance. This is in line with our research on cyber insurance markets throughout the world, including India.

So, What Precisely Does It Mean to Have Cyber Insurance?

Risks connected with the Internet, and more especially with IT infrastructure and related activities, can be mitigated by cyber-insurance, a kind of coverage that protects both individuals and companies. For this particular type of security, the word "cyber-insurance" is appropriate. Most standard insurance policies either don't mention or don't cover this specific kind of danger. This sort of danger is typically not covered by insurance. Insurance against cybercrime can assist pay for damages caused by things like hacking, theft, denial of service attacks, extortion, and data loss. Additional coverage options include first-party insurance and liability insurance, the latter of which compensates companies in the event of a loss. Remember that this policy covers two distinct kinds of losses; that is an essential consideration. One way to look at a loss is as a financial windfall for the violated company; so, the first party is often said to have suffered a direct loss. As a result of a cyber-breach, third parties, like customers or partners, may suffer losses, and the associated expenditures to compensate them are known as third-party losses. Such losses can be caused by a variety of things. To put it plainly, cyber-insurance is set up to mitigate the monetary fallout from phishing attempts or cyber-attacks that may illicitly acquire sensitive information (such as consumers' credit card numbers, bank account data, or social security numbers) and utilize it for illicit activities. Coverage is in place to protect such data against possible compromise, to rephrase.

Some of The Benefits of Cyber Insurance Include the Following:

There are a number of different ways in which businesses might benefit from purchasing cyber insurance.

Insurance against financial loss or additional expenses in the case of a cyber-attack while doing business is one of the several benefits of cyber insurance. In the event of a cyber-attack, this protection may be provided since it is readily available. This makes getting back up after a loss a lot easier ransom ware infections can occur when cybercriminals encrypt a company's data and then demand payment from the owners to decrypt it. One instance of extortion would be this. People may safeguard themselves against this type of damage by purchasing cyber insurance. Insurance against cyber-attacks can help pay for clean-up costs in the event that a business or individual's digital assets are compromised.

Claims of Privacy Infringement: It is the responsibility of every company to inform its customers when there has been a data breach due to a cyberattack. Companies should also be ready to deal with allegations of privacy infringement. Legal fees and other costs that a company may spend due to a data breach are also covered by the cyber insurance policy.

The provision of forensic assistance is an included benefit in several cyber insurance policies. Thanks to this clause, policyholders can get help from cyber experts if they are victims of a cyber-attack. For businesses and banks, these experts mean helping to assess the damage, retrieving lost data, and planning for recovery.

Liability to The Media and Damage to One's Reputation: The costs that are spent in the event that a claim of defamation or infringement of any intellectual property is brought against a commercial organization, bank, or financial corporation or individual can also be covered by cyber insurance. This allegation has the ability to have an effect on the reputation of the company as well as the brand that they have established.

Legal Responsibilities: In the event that a company is subjected to legal action, cyber insurance may also assist with covering the expenses that have been incurred by banks, financial institutions, or any other corporate organization or individual as a result of information breaches and the penalties that have followed. This is because cyber insurance protects against the possibility of a company being sued.

Most Pressing Challenges Confronting Cyber-Insurance: -

1. There is a lower level of consumers' awareness regarding cyber insurance.
2. The processes of acquiring cyber insurance and filing claims are becoming increasingly stressful for businesses.
3. It is difficult to estimate the scope and appropriateness of cyber insurance cover because of the damages that can be caused by cyber extortion, reputational harm, and regulations that are always shifting regarding data and privacy.
4. There is a cutthroat rivalry among insurance providers about the premium levels.
5. Aspects of data that are protected by cyber-insurance include:
6. (PHI) stands for "personal health information.
7. Details that can be used to identify an individual (PII)
8. Information from a third party or research that is confidential
9. PCI stands for payment card information.
10. Confidential information about research or information obtained from a third-party data hosting, computer processing that is outsourced, or data storage.

Attacks on The Internet in India

According to the Allianz Risk Barometer 2019, the most significant risk that businesses in India face is referred to as "Cyber Incidents/Attacks. Recently, India has been the target of a significant number of cyber-attacks. The following are some examples of them:

Theft that Occurred in July 2016 at the Union Bank of India

Hackers stole 171 million from the Union Bank of India after infiltrating their system with a phishing email that fooled an employee into giving them their login credentials. Thanks to swift action, the bank was able to retrieve almost all of the funds before they were lost.

May 2017 was the Month That the Wannacry Ransom Ware

Ransom ware spread rapidly around the world when hackers in India made hundreds of computer systems unavailable by demanding payment. Andhra Pradesh's state police and West Bengal's state utilities both had their systems compromised by the Wannacry ransom ware attack.

A Data Breach at Zomato in May 2017

An online meal delivery service called Zomato found out that a "moral" hacker had stolen the personal details of 17 million users, including names, email addresses, and hashed passwords. The hacker asked the business to list its security holes on the Dark Web and sell them.

Carried out by Petya Ransom Ware in June 2017

India was one of the countries hit hard by the Petya ransom ware outbreak. Attacks on the Danish business AP Moller-Maersk's Jawaharlal Nehru Port Trust in Mumbai suspended all activities pertaining to containers.

According to the 2018 CISCO Annual Cyber Security Report, a whopping 63% of cyber-attacks led to damages exceeding five hundred thousand dollars. These damages encompassed many forms of financial loss, such as income, clients, opportunities, and out-of-pocket costs.

Cyber Insurance is Essential for India's Banks for Several Reasons, Including:

Thanks to all the new technology that has come out, cybersecurity is now a huge part of the economy. Since establishing trust and credibility with customers is the foundation of banking, it becomes quite pertinent. Financial institutions should get cyber security insurance for the five reasons listed below.

Cashless transactions, which involve the use of virtual money like debit and credit cards, are becoming increasingly popular as consumers choose to forego using traditional currency. Data and privacy rights of stakeholders must be safeguarded by cyber security measures in these circumstances.

Customers' faith in financial institutions tends to decline after a data leak. Due to this, the organizations tasked with managing money issues face a formidable obstacle. If significant data breaches happen due to insufficient cyber security measures, clients may lose trust in financial firms. In order to keep their customers' trust, financial institutions must make cyber security a top priority.

Recovering from a data breach and compensating stakeholders requires substantial financial and time resources for a bank. This is making it difficult for the bank to maintain the trust of its constituents. It may take a long time and a lot of suffering to fix all the damage the hacker did. Aside from dealing with the

complexity of the issue, it would also need checking claims and deactivating cards. Concurrently, cyber insurance may provide expert guidance on how to stay safe online or, in the event of a loss, how to lessen its blow.

Consumers' private information, if misused, can cause serious problems. Even if the fraudulent activity is promptly stopped and your cards cancelled, your personal information might still be used in an unauthorized way. The reasoning behind this is because we will be keeping an eye on your data. Therefore, cyber insurance is really beneficial at the present time.

When it comes to protecting themselves, banks are more important than any other kind of financial organization. It gets this value in exchange for storing sensitive personal information that would be lost if erased. Customers' private data may still be vulnerable to hackers even if cyber insurance safeguards data that was previously believed to be protected from cybercrime.

Any one of these things may happen, and it would be devastating for banks' reputations. For this reason, cyber liability insurance is more important than ever before for banks to protect their customers and their customers' businesses from cybercriminals.

Before Purchasing Cyber Insurance, Financial Institutions Should Think About the Following Cyber Risks:

At this very moment, a cyber-insurance company is dealing with or is accountable for dealing with enormous volumes of data that belong to clients, candidates, and workers. This collection includes sensitive information such as bank account details, personal identification numbers, and payment card details.

There has Been A Significant Uptick in Discussions About Cyber Intelligence.

A disruption will occur in the organization if a device fails, a denial of service attack occurs, or another type of community intrusion happens.

Damage to a company's reputation makes customers distrust its logo, which lowers sales and loses money.

Since financial institutions are typically not covered for incident response or business enterprise interruption caused by a cyber-attack or the failure of technology under professional indemnity and other conventional insurance regulations, it is prudent to consider additional cyber insurance in the event that this incident happens.

Table: 1 Examining the Cyber Insurance Market in India In Comparison to Global Standards

Insurance Policies for Cyber Risks	Indian Industry	Worldwide Market
Industry Perspectives	Among the first to embrace the technology are the banking and financial sectors.	Services in healthcare, retail, manufacturing, banking and finance, IT, telecommunications, professional services, and retail
Market Insight	By 2018, 350 cyber insurance plans would have been sold, up 40% from 2017.	Cyber insurance was expected to climb 27% from 4.2bn in 2017 to 22.8bn in 20244, according to DSCI.

Premium	Due to market competition, premiums have dropped.	According to Allianz, cyber coverage currently means
	Market share. Banks, financial institutions, global IT and pharma, and Industrial IoT manufacturers pay $6,500–$8,000 for one million USD coverage.	Around $2 billion in premiums collected globally. Experts predict that by 2025, the premium for cyber insurance would have risen to $20 billion worldwide.
Cover	Risk coverage from $1M to $200M. Big public and commercial banks can only lend $50-100 million.	New restrictions need coverage changes.

Analysis: -

Despite data breaches and cloud computing promoting corporate growth, cyber security insurance is too expensive.

The KPMG analysis expects a 25.4% CAGR for cyber security insurance from $4.52 billion in 2017 to $17.55 billion in 2020.

Indian demand for cyber safety insurance coverage increased by over 50% between 2016 and 2017. In 2017, 250 financial institutions offered cyber insurance; in 2018, 350 did. Cyber safety insurance costs 200 crores INR and is expected to reach 400 crores.

Asia-Pacific region is a very favourable marketplace for cyber insurance providing organizations. The companies in this area are predisposed to cyber-attacks more as a result of negative safety against cyber-attacks. In India Cyber Insurance is supplied often by using private companies or joint venture companies. While in overseas cyber security Insurance is supplied by means of a few public sector businesses also.

A Comparison of The Cyber Insurance Models of Two Major Indian Companies:

Companies were selected at random for the purpose of comparison. Not to mention that these two cyber insurance companies are huge names in India.

	Cyber Insurance from HDFC ERGO	Allianz Cyber Insurance by BAJAJ
Eligibility	18+ years	18+ years
Premium	INR 1,410 - INR 14,273	INR 662 – INR 8,993
Sum Assured	Ranging in between INR 50,000 to INR 1,00,00,000	Ranging in between INR 1,00,000 to INR 1,00,00,000

Analysis: -

Bajaj Allianz and HDFC Ergo dominate cyber insurance. Electronic business, internet networks, and information assets are HDFC Ergo cyber insured. Most financial losses from phishing, email spoofing, illicit fund/asset transfers, and fraud are covered. Technical failure and company law infractions are not covered. In 2018, it created E@security cyber security protection for online losses. Different from Bajaj Allianz, HDFC Ergo cyber insurance covers professional negotiators and advisors.

Bajaj Allianz general cyber insurance covers extortion, theft, and more. The Bajaj Allianz cyber security insurance protects cybercrime victims. Online fraud, cyber stalking, extortion, identity theft, malware, and phishing attacks may be insured over-the-counter. Counselling, cyber extortion, third-party data breach, and court transportation are covered. India's first cybercrime insurer was Bajaj Allianz.

CONCLUSION

Since the digital industry is entering a period of rapid growth, financial institutions should consider purchasing cyber insurance to safeguard themselves from cyber-attacks and other dangers. After observing a more robust growth trajectory in cyber insurance demand in India, we may draw inferences on its significance for the banking sector. Cyber insurance is becoming a must for banks and other financial organizations due to the increasing frequency and severity of cyber-attacks and data breaches. With the recently proposed mergers of public sector banks creating much larger corporations, cyber insurance would become more necessary. Insurance companies can profit greatly from cyber insurance because there is a large unrealized market potential and no public sector competition, according to studies comparing the cyber insurance models of HDFC Ergo and Bajaj Allianz and cyber insurance markets worldwide. This is especially true in India and other countries. Given the anticipated increase in cyber-attacks and the advent of new cyber insurance kinds and marketplaces, this study's findings emphasize the vital necessity of cyber insurance for India's banking industry.

REFERENCES

1. Agarwal, R., & Jain, A. (2018). Cybersecurity in Indian banks: Current trends and challenges. *Journal of Banking and Finance in India*, 6(2), 112-130. https://doi.org/10.1016/j.jbfi.2018.06.004
2. Bansal, S., & Gupta, R. (2017). Cyber insurance: A growing necessity for financial institutions in India. *Indian Journal of Finance and Risk Management*, 5(1), 45-58. https://doi.org/10.1108/IJFRM-01-2017-0002
3. Bhattacharya, S., & Kumar, R. (2019). The impact of cyber threats on the Indian financial sector. *International Journal of Financial Studies*, 7(3), 40-58. https://doi.org/10.3390/ijfs7030040
4. Böhme, R., & Schwartz, G. (2010). Modeling Cyber-Insurance: Toward a Comprehensive Framework. The Economics of Information Security. Springer.
5. Choudhary, A., & Singh, M. (2018). Cybersecurity measures in Indian banking: A comparative study. *Journal of Financial Services and Management*, 8(2), 72-85. https://doi.org/10.1504/IJFSM.2018.094622
6. Cruz, A., & Sampaio, P. (2011). Cyber Insurance: A Tool for Risk Management. Journal of Business Continuity & Emergency Planning, 5(2), 115-125.
7. Desai, A., & Nair, S. (2016). Cyber risk management in Indian banks: Issues and challenges. *Indian Journal of Banking and Finance*, 10(3), 150-166.
8. Gupta, K., & Sharma, P. (2017). The role of cyber insurance in mitigating risks in the Indian financial sector. *Journal of Risk Management and Insurance*, 19(4), 230-245. https://doi.org/10.1108/JRMI-12-2017-0065
9. Joshi, V., & Kaur, R. (2019). Cybersecurity frameworks for Indian financial institutions. *Journal of Financial Compliance*, 5(1), 85-99. https://doi.org/10.1108/JFC-10-2018-0082
10. Kelley, J., & Lussier, M. (2013). The Role of Cyber Insurance in Protecting Against Cyber Threats. The International Journal of Digital Information and Wireless Communications, 3(1), 1-11.

11. Kshetri, N. (2013). Cybersecurity and Cyber Insurance: An Overview. International Journal of Information Systems for Crisis Response and Management, 5(4), 32-45.
12. Kumar, A., & Sharma, N. (2018). Cyber threats in the Indian banking sector: An analysis of recent incidents. *Indian Journal of Cyber Law*, 4(2), 100-115.
13. Manwaring, Kayleen & Hanrahan, Pamela. (2010). bearing responsibility for cyber security in financial institutions: the rising tide of directors' personal liability, Journal of Banking & Finance Law and Practice (forthcoming). 30.
14. Mehta, A., & Yadav, R. (2018). Cybersecurity and financial institutions: A study of Indian banks. *International Journal of Financial Services Management*, 9(2), 210-225. https://doi.org/10.1504/IJFSM.2018.092232.