Library Progress International *Print version ISSN 0970 1052*
Vol.44 No. 3, Jul-Dec 2024: P.12748-12754 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Cyber Insurance Need of the Hour: To Combat Growing Cyber-Attacks within Cyber Space

Sipra Routaray[1], Meenakshi Arya[2] and Dr. Rashmi Agnihotri[3]
[1]Mulund College of Commerce (Autonomous)
[2]Narsee Monjee College of Commerce & Economics (Autonomous)
[3]K.G Joshi & N.G Bedekar College of Arts & Commerce (Autonomous)

How to cite this article: Sipra Routaray, Meenakshi Arya, Rashmi Agnihotri (2024). Cyber Insurance Need of the Hour: To Combat Growing Cyber-Attacks within Cyber Space *Library Progress International,* 44(3), 12748-12754.

ABSTRACT
There are still alarming gaps among organisations and individuals regarding' cyber-attacks in cyber space and measures to create awareness about cyber insurance. In the realm of cyber space, cyber-attacks can occur, impacting both individuals and businesses. For individuals, this often involves crimes such as identity theft and personal data breaches. For businesses, cyber-attacks can include the theft of intellectual property and other sensitive information. The threat posed by cyber-attacks has grown considerably in recent years. Globally, the survey revealed diverse reasons for not obtaining cyber insurance. It was found that people lacked a clear understanding of cyber insurance products or perceived it as too expensive.

Keywords: Cyber Threats, Cyber Attacks, Cyber Space, Cyber Insurance

INTRODUCTION

Over the past few decades, cyberspace has significantly enhanced social connectivity and productivity, greatly improving information sharing and communication between individuals and communities. cyber technologies have also led to greater personal digital dependency on digital systems, creating ways for adverse events such as data breaches and cyberattacks. These technologies also bring an insidious threat of constant cyber risk, introducing danger into everyday digital activities and undermining user confidence and productivity.

There has been a significant increase in the number, scale, sophistication, and effectiveness of malicious cyber incidents in recent years, particularly since the advent of the pandemic and the widespread adoption of "work-from-home" practices. The extent of privacy breaches, the proliferation of cybercriminal activity, and the severity of financial consequences have been punishing. Cyber incidents are persistent and costly cause of business interruption. Furthermore, as entire industries undergo digital transformation, vulnerabilities localized within online connection points multiply due to escalating interdependencies. Individuals and businesses alike are adversely impacted by cyber incidents, prompting efforts to investigate strategies and tactics to mitigate cyber risk, including cyber insurance. However, cyber insurers face substantial challenges. The lack of historical cyber threat data makes it difficult for insurers to accurately predict future customer cyber risk. Absolutely, the dynamic and interconnected nature of cyberspace significantly increases the risk and potential impact of cascading loss events. These interconnected systems can amplify the effects of cyber incidents, leading to widespread disruptions and substantial losses. Mitigating such risks requires comprehensive strategies, including robust cybersecurity measures, continuous monitoring, and rapid response protocols to address and contain threats quickly.

The intrinsic nature of cyberspace presents unique challenges to cyber insurers, which are often inconsistent with the risk attributes commonly associated with traditional personal line insurance products. These challenges include, among others, a lack of historical claim/loss data for underwriting and pricing, the interdependencies of cyber architecture increasing cyber risk, difficulties in assessing cyber risk, the intangibility of risk assets (such as data and reputation), a lack of industry standardization, high and indeterminate tail risks, and moral hazards. While these challenges are present in both commercial and personal cyber insurance (PCI) domains, each market segment has its own unique characteristics.

Objectives:

1. To study about the concept of cyber insurance, cyber threat, cyber-attacks & cyber space.
2. To study about current cyber security attacks & trends.

Significance of the research: This research will benefit researchers, students, and policyholders (of cyber insurance). This research article will serve as a valuable guide for future academic studies on cyber insurance.

Limitation: Due to paucity of time and resources, this article is only based on secondary data.

LITERATURE REVIEW

Praditya et al., (2024) highlighted in the era of globalization and digitalization, cyber-attacks and digital disruption pose serious threats to information security. This qualitative research analyses various cyber-attack types (including malware, phishing, and DDoS) and their impact. The study focuses on the pivotal role of Human Intelligence (HUMINT) in addressing these threats. HUMINT involves understanding attacker motivations through social and psychological analysis, digital foot printing, and detailed information development.

Jain, S., & Sinha, S. (2024) The authors emphasize the importance of robust cybersecurity measures, including encryption, multi-factor authentication, and regular software updates, to safeguard sensitive customer data. They also stress the need for customer education on cybersecurity and the implementation of RBI's guidelines for cyber fraud.

Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023) examined the current landscape and trends in cyber insurance, highlighting the importance of cyber insurance as a complement to organizational safeguards. They discuss the drivers, obstacles, practices, and processes involved in the cyber insurance domain, emphasizing the need for harmonization in language and underwriting processes to facilitate market growth and policy comparison.

Juaningsih, I. N., & Hidayat, R. N. (2022) discusses the issue of regulatory obesity in Indonesia's cyberspace laws, highlighting the existence of 30 regulations at the statutory level that are general in nature and not well-integrated. This lack of integration leads to legal uncertainty and loopholes that can be exploited for cybercrimes. The authors propose an omnibus method to draft comprehensive laws that effectively integrate legal norms to protect the community in cyberspace. They emphasize the need for reform in the realm of law to address the rise of cybercrimes, which threaten public security and state resilience.

Li, Y., & Liu, Q. (2021) examined the advancements in the field of cyber security. The authors discuss the challenges, weaknesses, and strengths of various methods proposed to prevent or mitigate cyber-attacks. They delve into different types of new descendant attacks, standard security frameworks, history, sources and early-generation cyber-security methods. Additionally, the paper highlights emerging trends and recent developments in cyber security, as well as security threats and challenges.

Ratna, R. (2020) discussed the concept, benefits, various service providers, cost of cyber insurance. The article is written using secondary sources of data. Cyber-crimes can have disastrous effects on the companies especially financial institutions, hospitals, social media company, defence sector companies because they have huge volume of personal data. Data security is one of the primary responsibilities of companies as they have access to their customer's/user's private and confidential information. Having cyber insurance in India is must for such companies.

Johnson JA (2019) mentioned malicious individuals continuously seek ways to exploit computers for nefarious purposes. The process of procuring cyber insurance policies mirrors that of obtaining any other type of insurance. Choosing between companies involves understanding the differences in coverage, limits, deductibles, exclusions, and the specific terms and conditions of each policy. Attorneys should possess a basic understanding of cyber risks to effectively advise clients on protecting their businesses. Working with insurance professionals can significantly enhance this understanding and streamline the process.

Gajapathy, V., & Patil, R. M. (2018) analysed the market for cyber insurance in India and the awareness of it among the digital marketers. It also studies the current policies available and its adequacy to the current market situation and its scope. It has been evident that, India has a huge market for Cyber Insurance and it will have a huge growth in days to come. Author concluded that Cyber Insurance has a major role to protect the interest of the companies and individuals. 85% of the respondents who have encountered cyber-crime have felt the need for Cyber Insurance.

Raghavan, R. (2018) examined whether the risk of cyber-crime can be managed reasonably, with the insurance as an effective Risk Transfer Medium, inter alia, with various Public-Private Partnership measures to combat the threat. Author suggests that the economic losses from cyber-attack events have the potential to be as large as those caused by furious hurricanes. Insurers could benefit from considering the cover for cyber-attacks in these terms and make explicit allowance for aggregating cyber-related catastrophes.

Source: Author

INTERRELATEDNESS OF CYBER SPACE, CYBER ATTACKS & CYBER INSURANCE

Cyber Space*:* is generally considered to include all networks that connect IT systems. This encompasses network environments such as LAN and WAN, where information is stored and communication takes place. It is a global domain within the information environment, comprising interconnected networks of information technology infrastructures and resident data. This includes the internet, telecommunications networks, computer systems, embedded processors, and controllers. While cyberspace is commonly viewed primarily as a technological domain in current literature, its definition and significance have expanded across various disciplines in recent years. These include fields such as information and national security, international law and cybercrime, social and political domains, Internet governance, and even cyber-geography, among others.

Cyber Attacks: A cyber-attack is an intentional unauthorized action by an individual or group in cyberspace aimed at compromising the integrity, confidentiality, or availability of information, data, or information processing systems. Typical cyber-attacks include the deployment of computer viruses, worms, or ransomware. Ransomware, specifically, is malicious software used to block access to data or entire computer systems, often by encrypting data. Attackers typically demand a ransom payment in cryptocurrency for decryption. Other forms of cyber-attacks include phishing (attempts to obtain passwords or personal information), CEO fraud (fake urgent payment requests purportedly from the CEO), and data theft.

The financial impact of such attacks are substantial. Costs may include losses for crisis management, expenses for notifying affected parties of data privacy breaches, fines for breaching data privacy regulations, losses from business interruptions, fees for IT service providers, and payments for extortion demands. Liability risks may also arise, such as third-party claims for damages resulting from data theft or breaches of data protection laws.

Types of Cyber Attacks:

- ***Phishing*****:** One of the most common cybercrimes is phishing, where hackers send targets emails that appear to be from a trusted source or well-known individual. These emails often contain attachments designed to deceive the recipient into clicking on them.
- ***Malware*****:** Malicious software, or malware, is used to damage computer systems. Types of malwares include ransomware, viruses, worms, and spyware. When you open an attachment or click a suspicious link, the malware is downloaded and installed on your computer, causing significant disruption.
- ***Denial-of-Service (DoS)*****:** A DoS attack overwhelms a website or application with artificial traffic, exceeding its capacity. Once the attack is underway, legitimate users are unable to access the site or application. Such attacks may be motivated by a desire to extort payment from the victims.
- ***SQL Injection Attack*****:** This type of attack is particularly harmful to businesses. Cybercriminals use SQL injection to target databases, leading to data deletion, corruption, modification, theft, and authentication bypassing, among other crimes.
- ***Drive-by Attack*****:** In this attack, hackers embed malicious code in the PHP or HTTP code of a website or web application page. When someone visits the infected page, the virus is automatically downloaded and installed on their computer. Insecure websites or applications are the primary targets of drive-by attacks.
- ***Password Attack*****:** This is a common method for gaining unauthorized access to systems on a network. Hackers may sniff the connection between a system and a network or steal passwords from a person's desk. They also use brute force techniques to guess passwords randomly, often leveraging personal information such as the target's name, occupation, or job title.

- ***Man-in-the-Middle (MITM) Attack*:** In this type of attack, the hacker positions themselves between the user and the application. The goal is to steal information such as login credentials, credit card details, and account information from users of financial apps, websites, and eCommerce portals.
- ***Eavesdropping Attack*:** This attack involves intercepting information being transmitted over a network or to any connected device. It is particularly challenging to detect because the network appears to function normally. Hackers install a sniffer on a server or system, which intercepts the data being transferred.
- ***Cross-Site Scripting (XSS) Attack*:** In an XSS attack, attackers embed malicious resources into targeted applications or websites, corrupting the database with harmful JavaScript. When users visit the compromised site, the malicious JavaScript is sent to their browser as part of the HTML body and gets executed. This allows the attacker to steal cookies, session tokens, and other sensitive information.

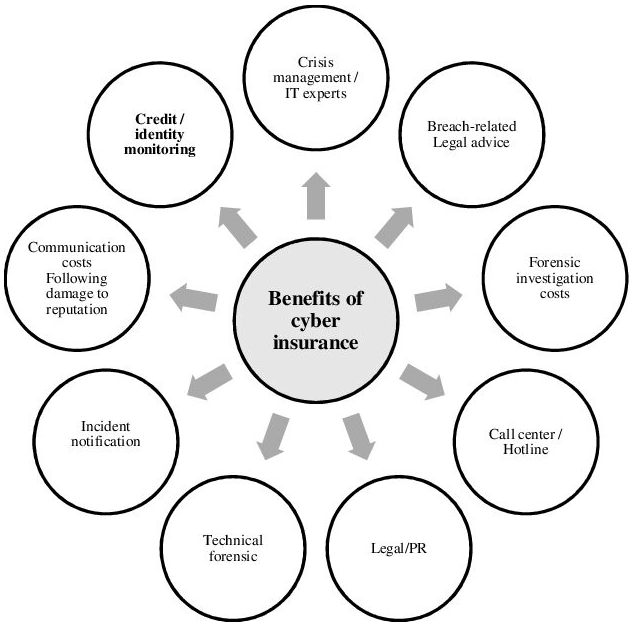
Causes of Cyber Attacks

- The increase in online transactions and digital data means that product launch outcomes, client and transaction figures, and other market information are readily accessible.
- People are using their mobile devices to access business networks for daily tasks. While smarter technology products enhance connectivity, they can also introduce new security threats. Hackers may exploit these vulnerabilities, gaining instant access to networks.
- Professional hacking groups and organizations are advancing technologically. Modern malware is challenging to detect and is designed to steal data for financial gain. Some individuals believe that hacking offers a more lucrative career path than working in cybersecurity.

Practices for Prevention of Cyber Attacks to be followed by Individuals

- Never share or send your personal data, such as bank account numbers, passwords, or ATM PINs, over an unencrypted network, including unencrypted email.
- Never sign up for any social networking platform or website unless it is legitimate and authentic. Always refresh and update your operating system regularly.
- Install and frequently update security software such as firewalls, anti-virus, and anti-spyware programs on your computer. Avoid visiting, following, or responding to spam and untrusted websites or links.
- Never click on pop-ups that offer site surveys or studies on eCommerce websites or any other site, as they may contain malicious software. When you interact with these pop-ups, a background download may occur, and the file can contain malware and malicious code. This is known as a drive-by download.
- Avoid visiting, following, or responding to spam and untrusted websites or links.

Cyber Insurance: encompasses agreements aimed at mitigating liabilities, property losses, and theft resulting from data breaches. These policies also provide coverage for financial losses due to data damage, income loss from network security failures, cyber extortion, cyber terrorism, post-incident public relations expenses, and reimbursements for criminal reward funds. Cyber insurance products offer various types of coverage like: (a) coverage for losses and liabilities resulting from data theft, (b) coverage for costs associated with forensic identification and remediation to respond to breaches, and (c) coverage for legal and regulatory fines and penalties and (d) Privacy issues.



Source: EIOPA (2018)

Major challenges of cyber insurance market:

- Less awareness about cyber insurance amongst buyers.
- Enterprises finding purchasing and claim processes of cyber insurance to be wearisome.
- Damages due to cyber extortion, reputational loss, and rapidly evolving data and privacy policies makes it hard to quantify breadth and adequacy of cyber insurance cover.
- Cut throat competition on premium amounts by insurance companies

CONCLUSION

Technological shifts have greatly improved our daily lives and led to incredible discoveries, but they have also opened a new set of risks and challenges for consumers and businesses. The internet, once a destination we "visited" (Internet parlours/ cyber cafes) has now become an omnipresent reality in which we "live." Algorithms are embedded in every aspect of our life be it our homes, cars, and the ways we shop, and interact with others. This trend has been further accelerated by the pandemic, creating a dual-screen existence where part of our lives occurs in the physical world and the other in the virtual realm. While this technological advancement has brought many improvements to our daily lives and led to incredible discoveries, it has also exposed us to a new set of risks, challenges and threats. Considering that cybersecurity is still in its early stages, we anticipate that insurance will play a pivotal role in shaping a new cyber culture. This will not only enhance our resilience against cybercrime and threats but also strengthen the cyber space.

The cyber insurance market is emerging and expanding as cyberattacks increase in frequency and severity, prompting individuals and institutions to seek protection against these risks. However, the industry confronts substantial challenges. These include a scarcity of historical data for accurate risk assessment, difficulties in forecasting future cyber risks, the potential for major cascading loss events, uncertainties among market participants regarding policy coverage details, and ongoing legal disputes over core issues. The future growth of the market hinges on successfully addressing these challenges.

REFERENCES

1. *Manzano, L. A. F., & Belmar, I. (2024/01//). Cyber insurance: Challenges and opportunities of an emerging market. Computer and Internet Lawyer, 41(1), 12-13.*
2. *Praditya, E., Maarif, S., Ali, Y., Saragih, H. J. R., & Duarte, R. (2024). The Role of Human Intelligence (HUMINT) in Deterring Cyber Attacks and Digital Disruption. Journal of Cybersecurity Research, 12(3), 127-142.*
3. *Jain, S., & Sinha, S. (2024). Cyber Security Threat in the Digital Banking Sector. International Journal of Advanced Legal Research, 4(3). ISSN: 2582-7340.*

4. *McGregor, R., Reaiche, C., Boyle, S., & Corral de Zubielqui, G. (2023). Cyberspace and Personal Cyber Insurance: A Systematic Review. Journal of Computer Information Systems, 64(1), 157–171.*
5. *Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023).* Cyber insurance: State of the art, trends and future directions. *International Journal of Information Security, 22(5), 737-748.*
6. *Gareth Mott, Sarah Turner, Jason R.C. Nurse, Jamie MacColl, James Sullivan, Anna Cartwright, Edward Cartwright, Between a rock and a hard(ening) place: Cyber insurance in the ransomware era, Computers & Security, Volume 128, 2023, 103162, ISSN 0167-4048.*
7. *Khyati Tejpal, Jayashree Vivek Patole (2023) "CYBERSECURITY: PRESSING PRIORITY IN INDIA", The Online Journal of Distance Education and e-Learning, April, Volume 11, Issue 2*
8. *Karishma Ruparelia (2023) "Growing Importance of Cyber Insurance in Indian Banking Sector", OxfordConference.https://www.researchgate.net/publication/374915054_Growing_Importance_of_Cyber_Insurance_in_Indian_Banking_Sector*
9. *Juaningsih, I. N., & Hidayat, R. N. (2022). Legal Protection For The Community In Cyber Space Through Regulation Forming With The Omnibus Method Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal, 2(2), 143-156.*
10. *Mirza, M. N., & Akram, M. S. (2022). 3-Cs of Cyberspace and Pakistan: Cyber Crime, Cyber Terrorism and Cyber Warfare* **Strategic Studies, 42***(1), 62-80*
11. *Increased cyber threats call for measures: Is cyber insurance the answer? (2022/12/01/). International Financial Law Review.*
12. *Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. Energy Reports, 7, 8176-8186. DOI: 10.1016/j.egyr.2021.08.126*
13. *Dobie GEA. 2021 Allianz Risk Barometer. Germany: ALLIANZ Global Corporate and Specialty SE; 2021.*
14. *Li Y, Liu Q. A comprehensive review study of Cyber Attacks and cyber security; emerging trends and recent developments. Energy Rep. 2021;7:8176–86.*
15. *Lallie HS, Shepherd LA, Nurse JRC, Erola A, Epiphaniou G, Maple C, Bellekens X. Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput Secur. 2021;105:102248.*
16. *Carter DM. Cyberspace and Cyberculture. In: Kobayashi A, editor. International encyclopedia of human geography. 2nd ed. Elsevier: Oxford; 2020. p. 143–47.*
17. *Süzen AA. A risk assessment of cyber-attacks and defence strategies in industry 4.0 ecosystem. Int J Comput Netw Inf Secur. 2020;1(1):1–12.*
18. *Ratna, R. (2020) Cyber Insurance – The Need of Hour.The Institute of Company Secretaries of India.https://www.icsi.edu/media/webmodules/Cyber_Insurance_TheNeedofHour.pdf*
19. *Khaliligarekani (2020) M. Incentive Mechanisms for Managing and Controlling Cyber Risks: The Role of Cyber Insurance and Resource Pooling. USA: University of Michigan;*
20. *Dambra S, Bilge L, Balzarotti D. SoK: cyber insurance - technical challenges and a system security roadmap. In: IEEE Symposium on Security and Privacy (SP) San Francisco, CA, USA; 2020. p. 1367–83.*
21. *Mareši NC. Information in cyberspace - actuality and challenges. Strategic Impact. 2020;76:76*
22. *Willi F, Bundt M. Personal cyber insurance: protecting our digital lives. Zurich, Switzerland: Swiss Reinsurance Company Ltd; 2019*
23. *Granato A, Polacek A. The growth and challenges of cyber insurance. In: Essays on issues. Chicago, USA: The Federal Reserve Bank of Chicago; 2019. p. 1–6.*
24. *Bandyopadhyay, T., & Mookerjee, V. (2019/04//). A model to analyze the challenge of using cyber insurance. Information Systems Frontiers, 21(2), 301-325.*
25. *Johnson, J. A. (2019/08//). 21st century insurance: CYBER INSURANCE. Computer and Internet Lawyer, 36(8), 15-20.*
26. *Gao C, Guo Q, Jiang D, Wang Z, Fang C, Hao M. Theoretical basis and technical methods of cyberspace geography. J Geogr Sci. 2019;29(12):1949–64.*

27. *Gajapathy, V., & Patil, R. M. (2018). Cyber Insurance–A Rising Market in India. Global Journal of Enterprise Information System, 10(3), 13-18.*

28. *Raghavan, R. (2018). Cyber Insurance – A Risk Mitigation Tool for Cyber Risk in India. Bimaquest, 18(1).*

29. *Agrafiotis I, Nurse JRC, Goldsmith M, Creese S, Upton D. A taxonomy of cyber-harms: defining the impacts of cyber attacks and understanding how they propogate. J Cybersecur (Oxford). 2018;4(1):4.*

30. *EIOPA (2018). Understanding Cyber Insurance – A Structured Dialogue with Insurance Com-panies. Luxembourg: Publications Office of the European Union.*

31. *Shanker AK, Usha G. Cyber threat landscape in cyber space. 2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA); 2017; Coimbatore, India. Institute of Electrical and Electronics Engineers Inc.*

32. *Kalinich K, Foord-Kelcey L. Global Cyber Market Overview (AON): Uncovering the Hidden Opportunities. Chicargo, USA: AON Inpoint; 2017.*

33. *(ENISA), E.N.a.I.S.A., R. N, and R. Europe. Incentives and barriers of the cyber insurance market in Europe. Resilience and CIIP Program. Greece: European Network and Information Security Agency (ENISA); 2016.*

34. *Tøndel I, Seehusen F, Gjære EA, Moe ME. Differentiating cyber risk of insurance customers: the insurance company perspective. International Conference on Availability, Reliability, and Security; 2016; Salzburg, Austria. p. 175–90.*

35. *Eling M, Hendrick Wirfs J. Cyber risk: too big to insure? Risk transfer options for a mercurial risk class. Switzerland: University of St. Gallen; 2016. p. 1–174. 978-3-7297-2006-*