Article

Not peer-reviewed version

assessCICA: Assessing and Mitigating Financial Losses from Cyber-Attacks with Role of Cyber Insurance in Post-Pandemic Era

Asura Akter Sunna , Tanzina Sultana , Naresh Kshetri * , Mohammed Majbah Uddin

Posted Date: 17 March 2025

doi: 10.20944/preprints202503.1130.v1

Keywords: cyber insurance; cyber-attacks; cybersecurity; financial loss; insurance effectiveness; risk management

Article

assessCICA: Assessing and Mitigating Financial Losses from Cyber-Attacks with Role of Cyber Insurance in Post-Pandemic Era

Asura Akter Sunna [1,*], Tanzina Sultana [2], Naresh Kshetri [3] and Mohammed Majbah Uddin [4]

[1] School of Business & Technology, Emporia State University, asunna@g.emporia.edu

[2] Sch of Comp & Infn Science, University of the Cumberlands, tsultana30981@ucumberlands.edu

[3] Department of Cybersecurity, Rochester Institute of Technology, naresh.kshetri@rit.edu

[4] Clinical & Translational Science Institute, University of Florida, m.uddin1@ufl.edu

* Correspondence: isultana@g.emporia.edu; This manuscript is accepted at 13th (IEEE) ISDFS 2025, Boston, MA, USA.

Abstract: The number of cybercrimes are increasing in this post-pandemic era, due to which organizations around the world are concerned about the recovery of the financial losses that arise from these cyber-attacks. As a result, cyber insurance has become an essential tool for risk management, providing financial safety and enhanced cybersecurity to the businesses. The study explores the context of cyberattacks, difficulties associated with coverage plans, risk assessments for cyber threats, and the dynamic nature of cyberattacks. It explains the importance of artificial intelligence (AI) in cyber risk assessment and securing digital assets. In addition to describing the different coverage options, such as third-party policies, first-party coverage for direct expenses, and "silent cyber" coverage within traditional policies, the paper investigates the evolution of cyber insurance. A thorough analysis of the previous literature focuses on how AI might improve cybersecurity, the difficulties faced by insurers and insured parties, and the rise in sophisticated cyberthreats in the years following the epidemic. The study uses a qualitative technique and analyses secondary data from various case studies, academic papers, and industry reports. In addition to examining essential cybersecurity and data protection laws, such as, the CCPA and GDPR, it compares coverage types and insurability standards across several geographic locations (the USA, Europe, and Australia). Comprehensive cyber insurance coverage is crucial, as demonstrated by two case studies involving Sinclair Broadcast Group and Change Healthcare cyber incident. These case studies present the effects of cyberattacks and the levels of financial recovery from real world scenarios. Finally, the paper outlines future research paths, highlighting the necessity of standardized insurance policies, customized coverage for businesses. Although cyber insurance is essential for preventing monetary losses, it may be made much more effective by standardizing procedures, integrating it with cybersecurity best practices, and improving risk assessment techniques.

Keywords: cyber insurance; cyber-attacks; cybersecurity; financial loss; insurance effectiveness; risk management

I. Introduction

Cyberattacks are attempts to exploit weakness in networks, systems, or devices in order to obtain data without authorization. Since technology has become a necessary component of everyday life, especially since COVID-19, the effect of these attacks has increased, posing significant risks to governments, corporations, and individuals. The area under attack for cybercriminals has expanded due to the quick development of digital technologies [1], and the widespread usage of cloud computing, IoT, and artificial intelligence. Cyber catastrophes, ranging from ransomware and data breaches to sophisticated phishing tactics, can do significant harm to one's finances, operations, and reputation. Organizations use cybersecurity tools like firewalls, encryption, and staff training to

 doi:10.20944/preprints202503.1130.v1

counter these risks. However, because cyber risks are always changing, standard security measures might not be sufficient to handle the financial and legal implications from an attack.

This is where cyber insurance becomes crucial. Cyber insurance protects companies financially by assisting them in recovering from liability claims, network outages, and data breaches [2]. However, cyber insurance has obstacles including inconsistent policy coverage, difficulties evaluating cyber risks, and the continually evolving threat landscape, despite the growing demand for it. Furthermore, artificial intelligence (AI) can assist with proactive cyber risk assessment by analyzing massive databases. This study examines the advantages, disadvantages, and future directions of cyber insurance. It also evaluates how cybersecurity frameworks and artificial intelligence (AI) enhance cyber risk assessments, empowering companies to make informed choices about protecting their digital assets.

According to Granato and Polacek, cyber insurance originated when American International Group (AIG) initially wrote the internet security liability policy in 1997, which was designed for IT companies managing networks for other consumers. Today, the market has broadened significantly, offering mainly three types of coverage: traditional third-party policies, first-party policies, and silent cyber coverage that exists within other policies. Third-party liability insurance generally covers the costs that the business incurred when their clients are affected by cyberattacks for which the said business was responsible. Later, the first-party coverages emerged which reimburses the companies for their own direct cyber insurance related expenses, such as data recovery, ransom payments, credit monitoring, restoring brand reputation, etc. Beyond these two types of explicit cyber insurance coverage policy, there is an implicit coverage which is known as silent cyber coverage. Sometimes, potential cyber related losses are covered by traditional property and casualty policies, which are not designed for cyber risks [3].

This study explores how cyber insurance might be used as a risk management tool to reduce the operational and financial risks resulting from cyberattacks. The first section of this study provides an overview and background of cyber insurance and the objectives of this study. The second section contains a literature review of relevant works that were done in cyber insurance by other experts in this field in the post-pandemic era. The third section covers the methodologies followed in writing this paper. The fourth section explains the role of cyber insurance in this time, including the types of coverages, insurability criteria and a comparison of cyber insurance act of different geographic locations in the world. The fifth section presents two case studies analysing previous real life cyber incidents and the role of cyber insurance in recovering from the losses. The sixth section discusses the findings and the limitations of existing cyber insurance coverages. The seventh section concludes the paper and highlights the future research scopes in this area.

II. Literature Review

As Artificial Intelligence (AI) provides cybersecurity awareness, cyber threat assessments, AI can aid cybersecurity resilience via cybersecurity insurance life cycle [4]. Using algorithms like machine learning (ML) and deep learning (DL) algorithms, AI can analyze giant datasets ahead of possible cyberattacks. In terms of reducing cybersecurity threats, NIST Risk Management Framework (RMF) has released several publications to address business risks. The coverage of cyber insurance policy as it is possible to review claims, reactions, data on previous occurrences as the preparedness to manage security and privacy. The deep analysis of cybersecurity risk factors and customized insurance coverage is needed for financial losses and damages.

An emerging tool to protect business firms is cyber insurance [5], as the number of cyberattacks is growing every year. The necessity of protection for information systems and minimizing the financial losses is extremely crucial due to malicious cyber threats, critical severity attacks, and ransomware attacks. Insurance markets and insurance practices with respect to cyber insurance are growing and will certainly expand further in future. Although cyber insurance covers a variety of cyber incidents including network damage financial losses, and many more, some financial losses in terms of an organization's reputation can never be recovered. Besides several challenges to business

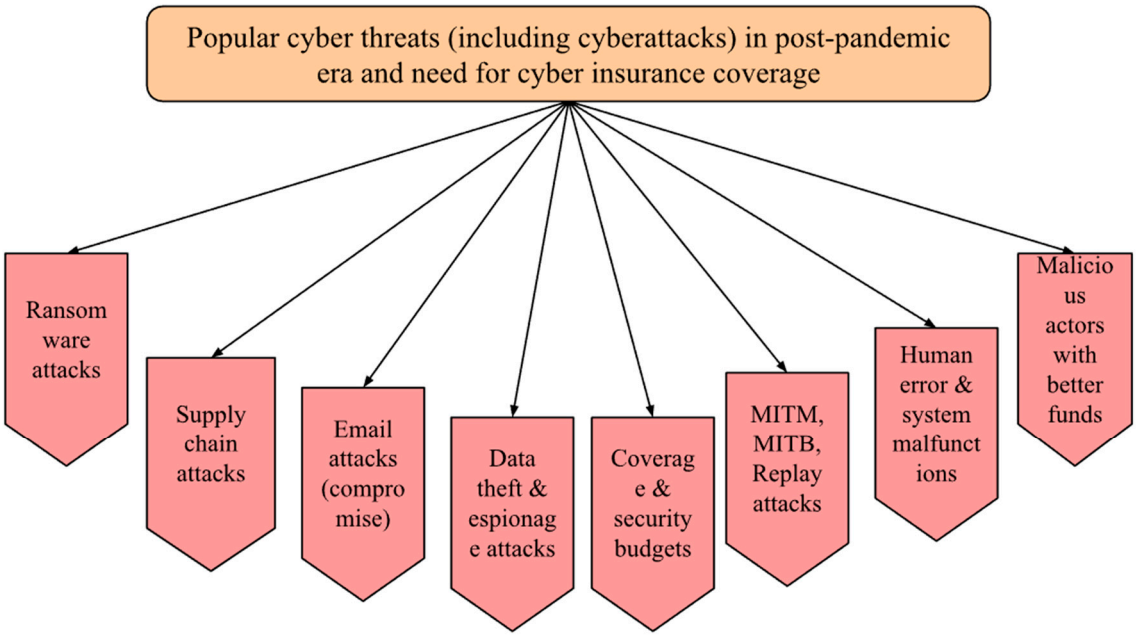
 doi:10.20944/preprints202503.1130.v1

organizations some of the popular cybersecurity threats are supply-chain attacks, file transfer fraud / attacks, business email compromise / email attacks, and / or ransomware attacks.

A review has been done for cyber insurance challenges [6] with respect to contractual agreement status in three different categories. The potential losses from cyberattacks are becoming more significant and increasing every year. Articles collected from search results in the study are used to review cyber insurance challenges and their solutions on four digital libraries (Science Direct, ACM, IEEE, and Springer). General challenges that appear on cyber insurers on top of no contractual agreement are cost-benefits aspects of investment (low security investment, budget distribution of cybersecurity, uninsured business firms), and cyber insurance awareness (framework of cyber insurance, management of cyber risk apart from coverage, premium rates determination, cyber losses modeling due to many kinds of cyber incidents).

New challenges in effective cybersecurity measures by authors [7] as financial institutions are primary targets after the pandemic. Changing policy on data protection and privacy rules (including cyber insurance companies) with top security investment priority as increase in the security bouquet by several organizations and business firms. Malicious actors are always one step ahead with better talents and better funds compared to cybersecurity defense and counter measures. As the annual number of ransomware attacks worldwide increased dramatically, some frontier cybersecurity challenges included crypto / (buy now pay later) BNPL, state-sponsored attacks, AI origination attacks, third party service providers, web application attacks, and regulatory challenges in financial services with drastic revolution.

An unexpected scenario for all cyber power nations was Covid-19 pandemic with emerging cybersecurity challenges [8]. People were asked to leave their offices, homes, and institutions as the world came to halt with viruses spreading around the globe. New modus operandi were used by cyber criminals (from cyber insurance frauds to covid vaccines scams) to monetize system changes and successful execution of ransomware attacks. Major cyber affected areas were hospitals, healthcare, industry, education, smart governments, telecommunication sectors, smart grids, banking institutions, and many more. Man-In-The-Middle (MITM) attacks (including MITB and Replay attacks) were on rise as relief works were being carried out and thousands of people were waiting for their treatment and vaccines. There is no doubt that cybercrimes (and COVID-19 themed attacks) have ravaged the society and lifestyle of people not only during pandemic but now still after pandemic.



 doi:10.20944/preprints202503.1130.v1

Figure 1. Summary of cyber threats (including increasing cyberattacks) in post-pandemic era and need of cyber insurance in mitigating financial losses from our literature review [4–8].

III. Methodology

The research methodology we use in this study is qualitative, and it analyzes the secondary data sources including industry reports, academic papers, news items, regulatory guidelines, and case studies relating to cyber insurance. It attempts to comprehend the changing nature of cyberthreats and how insurance helps reduce financial risks. It reviews and compliments the findings of the previous literature that was done in this area. The secondary data was collected from cyber security industry reports. In this paper we focus on previous research work conducted for cyber-crime and its protection attempt from damage. For comparative analysis of cyber insurance plan, its scope, deliverables, and penalties we took Cyber Security Framework followed by European Union (GDPR), USA California Consumer Privacy Act (CCPA) and Australian Privacy Act 1988. Additionally, we included an analysis of two case studies, one involving cyber insurance coverage and one without comparing and contrasting the significant role cyber insurance plays in financial recovery following cyber incidents. The limitations of this study include the reliability of publicly available data only, and due to the evolving nature of cyber insurance policies, some findings might be subject to change based on emerging industry trends.

IV. The Role of Cyber Insurance

Insurance assures business for operations, while insurance policymakers and companies follow guidelines on their own or sometimes follow industry trends. Cyber insurance is categorized based on the types of cyber coverage available. Some institutions follow the loss events approach, and some companies follow the precautionary approach. Here, one thing comes into consideration: while cyber-attacks do not follow any specific pattern, find any scope of vulnerability. Traditional policies face challenges with cyber risks, such as **information asymmetry**, **correlated losses**, and **rapidly evolving technology**. In response, insurers take one of three approaches: excluding cyber risks from standard policies, adding cyber agreements to existing coverage, or creating discrete cyber products.

Financial mitigation of losses, Coverage of direct costs (e.g., data recovery, legal fees), Coverage of indirect costs (e.g., reputational damage, business interruption), Risk management and compliance benefits, Encouragement of best practices in cybersecurity, Regulatory compliance facilitation, Limitations and challenges, Policy exclusions and limitations, Difficulty in determining policy adequacy

Organization accepts cyber security policies to secure their business operations from the market practices, cyber insurance comprising both cybersecurity and identity theft insurance. Cyber security insurance protects business against data breaches and business interruption, whereas Identity theft issuance covers individuals against unauthorized transactions. Identity theft coverage reflects a small segment of the total insurance market. According to NIAC guidelines there are 4 types of Cyber insurance sectioned both standalone and packaged cybersecurity and identity theft [9] .

Market Analysis from 2015-2017 shows [10]

* Total participants increased from 453 to 615 mainly in packaged coverage
* Cyber insurance necessity increases substantially reaching .034% of P&C industry premiums by 2017
* Premium volume grew 31% in 2016 and 55% in 2017
* Market shifted from standalone to packaged coverage dominance by 2017
* Professional surplus insurers write 20% of coverage, but firms with surplus affiliations write 60%

A. Insurance Type

Cyber insurance covers a variety of incidents that mostly lead to financial losses, business interruption, network damage etc. Additionally, some policies cover Systems Malfunctions, data breaches, loss of integrity or availability , malicious activities, and human errors [5] and [9] . The

 doi:10.20944/preprints202503.1130.v1

following table will demonstrate comparisons of insurance coverage between the USA and Europe market.

Table 1. Cyber Insurance Coverage comparison between USA and Europe [5]. And [9].

Region	**USA**	**Europe**
First Party Coverage		
1. Loss or Damage of digital Assets	It covers the cost of repair or restore of lost data and software cyber insurance company mostly covers this portion of loss approximately 70%	Strong coverage by Household Insurance and Cyber Insurance covers 39% of it
2. Business Interruption	Covers lost income and cost due to network failure this rate depends on the organizational structure and types of industry mostly it goes around 4%	If it comes to the Account blockage, then cyber Insurance provide a handsome amount otherwise business interruption does not include in policy category with high importance
3. Cyber Extortion	Forensics investigation and ransom payments this segment covers the highest section around 59% (Wells-Dietel & Erkan-Barlow, 2023) of the payment covers this section.	Cyber Extortion also includes a higher rate from the cyber insurance policy almost 68% payment are covered through this.
4. Forensics investigation and Restoration costs	Software restoration along with the system restoration covers in this section.	Data recovery cost covered Household Insurance 54.90%, and 39.22% by Standalone insurance whereas Liability and Legal Protection provide a very short amount of coverage for forensic investigation.
Third Party Coverage		
1. Coverage types	Outlines third-party coverage areas including Credit Monitoring/Cell Center, Multimedia Liability, and Public Relations.	Encompass broad categories of third- party protection including Malware Transmission, Copyright Violations and Cyberbullying compensation. GDPR provides specific coverage percentage or particular scenario
2. Granularity	The coverage study emphasizes a qualitative methodology, provides broad explanations of insurance types and their uses for personal and organizational aspect instead of in-depth statistical analyses in category wise	GDPR provides detailed quantitative breakdowns of coverage proportions for various scenarios, specifically focusing on Data Protection Violations and Antivirus Software implementations. Different insurance types specialize in specific coverage areas, with SAI (Security Assurance

 doi:10.20944/preprints202503.1130.v1

		Insurance) primarily covering Malware Transmission cases, while LYI (Liability Yield Insurance) focuses on Damage Claims Protection.
3. Use Cases and Context	California Act focuses on purpose and scope of coverage types with practical examples of each.	The analysis provides valuable insights into insurance coverage comparisons, where they followed GDPR framework to design insurance policies and finding out most comprehensive support for specific third-party liabilities and allowing for effective evaluation of coverage options across predefined categories.
4. Applications	Insurance comparison based on coverage proportions.	GDPR framework is particularly valuable for insurance policy selection, allowing individuals to compare coverage proportions across different policy types (SAI, LYI, LPI, HOI) and identify potential coverage gaps in critical areas like IT assistance and cyberbullying protection.

Stand-alone cyber insurance (SAI) offers broad coverage for financial losses from online fraud, identity theft, and reputational damage, while traditional policies provide minimal protection. SAI includes valuable IT security services like antivirus software and secure storage. Traditional policies often explicitly exclude cyber coverage or use unclear language about cyber protection, limiting their effectiveness against cybercrime.

B. Insurability Criteria

Insurability criteria, as outlined by Mehr and Cammack [11] and [12] , emphasize that insured incidents must be fortuitous, calculable, and involve large but manageable losses that occur independently. A large number of similar exposure units is required to estimate probabilities, and premiums must be affordable. For insurance to make sense, losses need to be three things: big enough to matter, clearly defined, and easy to verify (including when, where, and how they happened). Insurance companies also need to: keep the biggest possible losses under control, make sure average losses aren't too high, set reasonable coverage limits, follow all laws and regulations, and have enough information about the risks they're covering [5].

According to the insurability criteria insurance service providers mostly derive incidents on their reason and impact. Therefore, most of the insurance company cover Non Malicious events covered: (Mistakes, omissions) where Power outages which caused operation discrepancy are not covered

** External Collaborations events that become the threat for the company, but this situation stands in very exclusive vendors specially the renown/ reputable vendors.

C. Compare different Cyber security and Management Act according to geographical area:

Most insurance companies pay attention while designing their policy to Ransomware amounts and the type of data processed by the applicant organization; less importance is paid to the information, such as the business structure, IT security budget, and IT security Management Practice. Insurers pay attention to whether they provide updated information. The insurer examines the interested organization's cyber risks to help determine whether to accept coverage and an appropriate premium. The risk assessment looks at the organization's risk exposure and the state of security measures currently in place. Cyber insurance trend follows the commercial loss and mostly covers the loss of data and monetary recovery from Ransomware attacks. These policies have yet to implement a more nuanced approach that considers the actual value and importance of individuals'

 doi:10.20944/preprints202503.1130.v1

emotional loss or other psychological impact. The insurer considers risk accumulation scenarios or occurrences that can lead to claims across a sizable portion of the insurance policy portfolio, as part of the underwriting process (e.g., an electrical outage in a big geographical area). The following table compares each continent's cyber security risk assessment and mitigation practice.

Table 2. Comparison of Cyber security and Management Act (USA, Europe, and Australia).

	USA	Europe	Australia
Scope	California Consumer Privacy Act [14] focuses on the consumers' collection of data where only residents were the initial service receiver of this act.	This comprehensive regulation focuses on the data and information systems infrastructure, where data protection, Network Security Directive, and cybersecurity strategies are some main content. GDPR highlights global impact, EU's harmonization effort and strategies to take actions against cyber threats.	Australia follows their Privacy Act 1988 [13], Privacy Amendment Act and Consumer Data Right and they targets data protection and cyber resilience across various sectors liner banking energy and telecommunication
Principle	CCPA - spotlights transparency and control allowing consumers to request their data access, data monetization and protects consumers from discrimination upon their privacy choices	Golden Rule of Information Security Policy harbored in privacy by design, explicit consent, and data minimization. Initiate strict data sharing rule, breach notification severe penalties for noncompliance.	Emphasis on mandatory breach notification also prioritizes consumer protection over fundamental rights, focusing on practical measures like credit reporting, secure data sharing, and incident reporting.
Data Breach notification Requirements	CCPA encourages businesses to notify users however there is not a certain timeline.	GDPR [15] follows the 72 hours timeframe for notify data protection authority and individuals must also notify if the breach constitutes a significant threat to their rights.	Following GDPR Australian Framework follows informing Australian Information Commissioner and affected individuals within 72 hours if any breach cases serious harm [16]
Enforcement and Penalties	CCPA Attorney General fines up to $7500 per intentional violation and $2500 per unintentional violation	National Data protection authorities impose up to €20M or 4% of the global revenue for serious violations while affected individuals can ask for compensation.	The Office Australian Information Commissioner Office administers these penalties amounting up to $2.1 M AUD for serious or repeated breaches.
Features	Focuses on clients restricting Data Monetization and protecting consumers rights.	Establishes two fundamental rights: data portability (moving personal data between services) and the right to erasure (having personal data deleted upon request). Sets regulations for international data transfers and mandates that large organizations employ Data Protection Officers to supervise data handling practices.	Australian Framework enforces banking standards governing data security and financial privacy. Requires security incident reporting and national frameworks.

 doi:10.20944/preprints202503.1130.v1

Conclusion	Focuses on individual consumers rights	They set a global standard of privacy, emphasizing fundamental rights, strict compliance, and risk management.	Australian Framework protects industry specific regulations and practical implementation strategies.

Regional data protection priorities vary: US emphasizes consumer protection, EU focuses on privacy rights, and Australia adopts a pragmatic data security approach.

V. Case Studies

A. Case Study I - Sinclair Broadcast Group, Inc. Ransomware Attack 2021

In October 2021 Sinclair Broadcast Group, Inc. detected a security breach and confirmed that ransomware has encrypted certain servers and workstations, disrupting office and operational networks, as well as stole data from the company's system. Sinclair Broadcast Group, Inc. is a diversified media company focused on local sports and news. It operates 21 regional sports networks, oversees 185 television stations across 86 markets, and owns national networks such as Tennis Channel and Stadium, along with affiliations to major broadcast networks [17]. The company lost millions of dollars in advertising revenue as a result of this attack, which also damaged the company's system and disrupted the broadcasting operations. Even though the company restored the network from the backup and did not pay ransom, it still went through a great number of financial losses, which was partially recovered through cyber insurance policy taken prior to the incident. Following is the analysis of this incident and lesson learned from this case:

Table 3. Comparison of actions, impact, recovery, and lessons learned (Case Study I) from Sinclair Broadcast Group, Inc. Ransomware Attack 2021 [17–19].

Action taken upon detection of the incident	Impacts of the incident:	Recovery:	Lessons learned:
• Initiated Incident response plan • Took measures to contain the incident • Initiated an investigation • Deployed legal counsel, a cybersecurity forensic firm, and other incident response professionals • Notified law enforcement and other governmental agencies	• Disruption in internal operations for several weeks • Disruption in broadcasting • Paid no ransom • $63 million losses from advertising revenue (Brumfield, 2022)	• Restored the network from the backup (Brumfield, 2022) • $50 million insurance coverage through a series of layered insurance policies. First three layers of insurers already paid the claim, and a lawsuit is ongoing for unpaid insurance claims. (ProgramBusiness, 2024)	• Incident response plan is crucial to manage such cyber threats • Secure backups for protection of data and network systems • Regulatory compliance will help in meeting any legal obligations • Cyber insurance to minimize devastating financial losses.

B. Case Study II - Change Healthcare Security Incident 2024

Change Healthcare is a leading service provider for healthcare industry, health insurances and other companies. They accounted for nearly 40 percent of health insurance claims. On February 21, 2024, CHC experienced a ransomware attack that led to unauthorized access to sensitive data, including personal, health, and financial information. CHC worked with cybersecurity specialists to

 doi:10.20944/preprints202503.1130.v1

look into and improve security procedures, engaged law enforcement, and made an immediate effort to control the intrusion. Impacted individuals were notified in different stages and were offered two years of complimentary credit monitoring and identity protection services. CHC continued to reinforce its policies and safeguard systems to prevent future incidents [20]. The incident disrupted the payment system of the healthcare industry, lost sensitive data, paid $22 million for ransom among significant financial loss from service disruption, etc. No information regarding cyber insurance was found as part of the financial recovery plan. Following are the analysis and lesson learned from the incident:

Table 4. Comparison of actions, impacts, recovery, and lessons learned (Case Study II) from Change Healthcare Security Incident 2024 [20,21].

Action taken upon detection of the incident	Impacts of the incident:	Recovery:	Lessons learned:
• Disconnected system to prevent further impact • Initiated investigation of the breach • Involved law enforcement (Change Healthcare, 2024)	• Disrupted payment system in healthcare industry • Lost sensitive data • Paid $22 million in ransom to contain the risk of stolen data (Young, 2024) • Financial losses from service disruption • Costs regarding incident response, and legal actions • Reputational impact	• Restored its electronic payments platfor in around four weeks • Paid ransom to contain the risk of stolen data • Monitoring online platforms, such as dark web, for misuse of stolen data • Created a public notice and a substitute website to share updates and resources • No information regarding cyber insurance were found	• Need to enhance data security • Proactive incident response plan to manage incident • Periodic backup of data • Cyber insurance to minimize financial losses

VI. Discussion and Limitation

Identifying potential financial impacts due to increasing cyber-attacks is challenging in the post pandemic era as compared to pre pandemic era. Although the cyber threat assessment for financial impact can be done, it is not as much as enough for insurance providers (as first insurance products appeared in the USA) [22]. In terms of regulation from the European Council as an issue of cyber threat insurance, impact of cyber threats via three factors - time, scope, and degree of interaction. The cost of data breach is increasing globally as the expected harm by cyberattacks is always more and continuous. The USA is considered as the most powerful cyber nation and on the other hand, the USA is the most attacked nation, hence, the cyber-insurance market is more advanced in the United States than in the rest of the world [23]. Insurance coverage regarding the data breach whether by employee or intruders is directly relational to organizational reputation and publicity which everyone wants to avoid. There is a lack of knowledge, clear understanding, including the standardization of cyber insurance products offered by insurance companies.

Although the means of protecting business and customers has been done in various ways, cyber insurance is one way for unexpected cyber incidents. Several industries (including almost all) have suffered from cyber-attacks (such as data theft, hacking, espionage, extortion) in the past, one of the most critical ones is the healthcare industry [6]. The challenges not only arise for cyber insured and cyber insurer before a contractual agreement exists, after the contractual agreement exists, and no

 doi:10.20944/preprints202503.1130.v1

contractual agreement between the two parties (for cyber insurance services). As an important global business risk, cyber risks are now at the forefront for small, medium, and large business organizations. Information retraction, security breaches at business firms, specific attack methods (like replay attacks, IP spoofing, denial of service attacks, ransomware attacks, man-in-the-middle attacks, poisoning of protocols and many more etc.) are common as there is no standard definition of cyber risks [24]. Companies (including the US banking sector) have complex corporate structures that they do not want to disclose before the cyberattacks and after the cyberattacks.

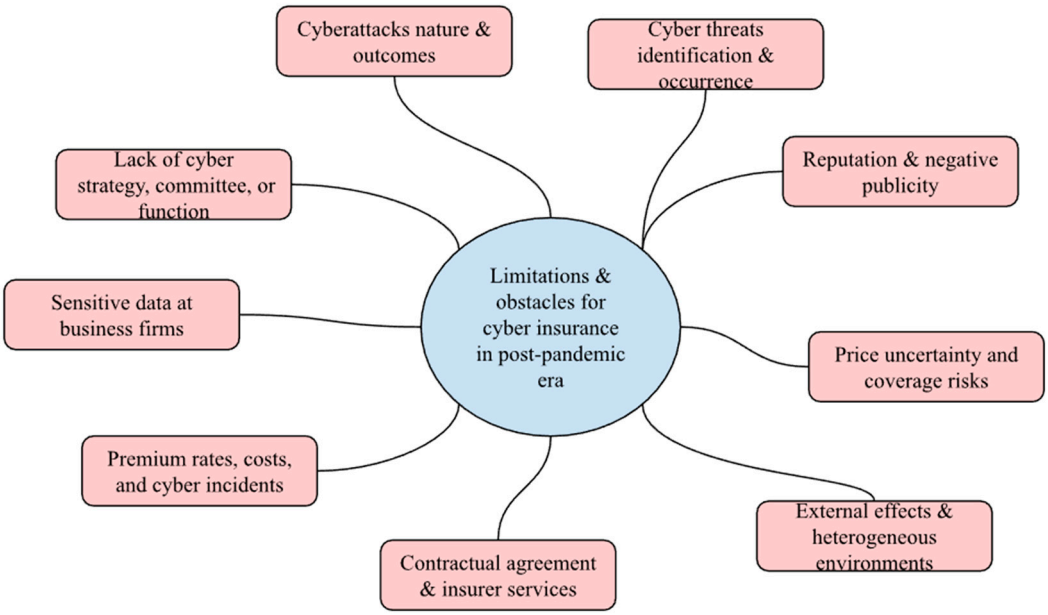


Figure 2. Limitation and obstacles for cyber-insurance (for both insurance providers & insured business firms) in post-pandemic era [6,22–27].

VII. Conclusion and Future Scope

Cyber insurance offers essential financial security, helping businesses recover from expensive data breaches and possible claims. There are still many obstacles to overcome, including inconsistent policy coverage, the limitations of accurately evaluating complex cyber risks, and a constantly evolving cyber risk landscape. Because AI can analyze large datasets and detect potential vulnerabilities before they happen, it provides exciting possibilities for more proactive and comprehensive risk assessment. This study has examined the benefits and drawbacks of cyber insurance, the impact of well-established cybersecurity frameworks, and the potential for artificial intelligence to greatly improve risk assessments. A comprehensive and effective cyber insurance coverage is crucial, as demonstrated by the case studies of Sinclair Broadcast Group and Change Healthcare, which clearly show the practical consequences of cyberattacks and various degrees of financial recovery. Despite being a dynamic and rapidly changing industry, cyber insurance is becoming more and more essential for businesses looking to protect their invaluable digital assets and maintain operations in the face of growing and sophisticated cyberthreats.

The review of other literary works in this area reveals that the cyber insurance policy in the market lacks standardization in policy coverage. The ambiguity in policy terms might lead to dispute in the face of actual incident [28]. Future research, collaboration of market leaders, and intervention from policy makers is necessary in this area to analyze and prepare more clear and uniform terms and conditions regarding cyber insurance coverage. Wang demonstrated how private sector cybersecurity investment reduces overall cyber loss and proposed tailored, threat-specific insurance policies, particularly beneficial for SMEs, that combine coverage with risk knowledge and

 doi:10.20944/preprints202503.1130.v1

mitigation support. Further research in this area can explore if availability of cyber insurance causes increase or decrease of investments in cyber security and how much impact it has in strengthening cyber security measures [29]. Additionally, this study compared cyber security and management act for USA, Europe and Australia, further investigation on other geographic areas such as Asia, Africa and South America might reveal more in depth findings to enrich existing cyber security and management act worldwide.

References

1. Zakharevych, M., & Hryhorenko, V. (2024). Digital Competence and Digital Literacy of Higher Education Acquires. Collection of Scientific Papers of Uman State Pedagogical University, 1, 119–129. https://doi.org/10.31499/2307-4906.1.2024.302215
2. Panda, S. *et al.* (2021) 'Cyber-Insurance: Past, present and future', *Encyclopedia of Cryptography, Security and Privacy*, pp. 1–4. doi:10.1007/978-3-642-27739-9_1624-1. [Sec1-Ref2]
3. Granato, A. and Polacek, A. (2019) *The growth and challenges of Cyber Insurance*, *Federal Reserve Bank of Chicago*. Available at: https://www.chicagofed.org/publications/chicago-fed-letter/2019/426 (Accessed: 18 February 2025).
4. Jawhar, S., Kimble, C. E., Miller, J. R., & Bitar, Z. (2024, January). Enhancing Cyber Resilience with AI-Powered Cyber Insurance Risk Assessment. In *2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0435-0438). IEEE.
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*(3), 737-748. https://doi.org/10.1007/s10207-023-00660-8
6. Aziz, B. (2020, October). A systematic literature review of cyber insurance challenges. In *2020 International Conference on Information Technology Systems and Innovation (ICITSI)* (pp. 357-363). Houston, USA. IEEE.
7. Bajracharya, A., Harvey, B., & Rawat, D. B. (2023, March). Recent advances in cybersecurity and fraud detection in financial services: a survey. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0368-0374). IEEE.
8. Choudhary, A., Choudhary, G., Pareek, K., Kunndra, C., Luthra, J., & Dragoni, N. (2022). Emerging cyber security challenges after COVID pandemic: a survey. *Journal of Internet Services and Information Security*, *12*(2), 21-50.
9. Schütz, F., Rampold, F., Kalisch, A., & Masuch, K. (2023). Consumer Cyber Insurance as Risk Transfer: A Coverage Analysis. Procedia Computer Science, 219, 521–528. ScienceDirect. https://doi.org/10.1016/j.procs.2023.01.320
10. Xie, X., Lee, C., & Eling, M. (2020). Cyber insurance offering and performance: an analysis of the U.S. cyber insurance market. The Geneva Papers on Risk and Insurance - Issues and Practice, 45, 690–736. https://doi.org/10.1057/s41288-020-00176-5
11. Pfeffer, I., Mehr, R. I., & Cammack, E. (1973). Principles of Insurance. The Journal of Risk and Insurance, 40(2), 274. https://doi.org/10.2307/252122
12. Berliner, B. (1985). Large Risks and Limits of Insurability. *The Geneva Papers on Risk and Insurance*, *10*(37), 313–329. http://www.jstor.org/stable/41950168
13. OAIC. (2024). The Privacy Act. OAIC; Australian Government. https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act
14. State of California Department of Justice. (2024, March 13). California Consumer Privacy Act (CCPA). State of California - Department of Justice - Office of the Attorney General. https://oag.ca.gov/privacy/ccpa
15. GDPR. (2018). General Data Protection Regulation (GDPR). General Data Protection Regulation (GDPR). https://gdpr-info.eu/
16. Thilla Rajaretnam. (2020). A Review of Data Governance Regulation, Practices and Cyber Security Strategies for Businesses: An Australian Perspective. International Journal of Technology Management and Information System, 2(1), 1–17. https://myjms.mohe.gov.my/index.php/ijtmis/article/view/8359

 doi:10.20944/preprints202503.1130.v1

17. Sinclair Press Releases (2021) Sinclair Broadcast Group provides information on Cybersecurity incident, Sinclair, Inc. Available at: https://sbgi.net/sinclair-broadcast-group-provides-information-on-cybersecurity-incident/ (Accessed: 13 January 2025).
18. Brumfield, C. (2022) SEC filings show hidden ransomware costs and losses, CSO Online. Available at: https://www.csoonline.com/article/572321/sec-filings-show-hidden-ransomware-costs-and-losses.html (Accessed: 13 January 2025).
19. ProgramBusiness, P. (2024) Sinclair files lawsuit against Cyber Insurers - programbusiness: Where insurance industry clicks, ProgramBusiness. Available at: https://programbusiness.com/news/sinclair-files-lawsuit-against-cyber-insurers-over-unpaid-ransomware-claims/ (Accessed: 13 January 2025).
20. Change Healthcare (2024) DATA BREACH NOTICE (June 20, 2024; updated July 31, 2024, and August 8, 2024), Change Healthcare. Available at: https://www.changehealthcare.com/hipaa-substitute-notice-spanish.html (Accessed: 13 January 2025).
21. Young, K. (2024) Cyber case study: Change healthcare cyberattack, CoverLink Insurance - Ohio Insurance Agency. Available at: https://coverlink.com/cyber-liability-insurance/cyber-case-study-change-healthcare-cyberattack/ (Accessed: 14 January 2025).
22. Pavlík, L., Ficek, M., & Rak, J. (2022). Dynamic assessment of cyber threats in the field of insurance. *Risks*, *10*(12), 222.
23. Kshetri, N. (2019). The economics of cyber-insurance. *IT Professional*, *20*(6), 9-14.
24. Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance*, *89*(3), 725-763.
25. Hutson, J., Coble, K., Kshetri, N., & Smith, A. (2023). Exploring the intersection of digital marketing and retail: Challenges and opportunities in AI, privacy, and customer experience. *Confronting Security and Privacy Challenges in Digital Marketing*, 50-72. https://doi.org/10.4018/978-1-6684-8958-1.ch003
26. Osama, O. F., Kshetri, N., Rahman, M. M., & Pokharel, B. P. (2025). healthMLsec: Machine Learning based Vulnerability Assessment in Health Systems: A Framework for Enhancing Cybersecurity and Patient Data. https://www.preprints.org/manuscript/202502.2165/v1
27. Kshetri, N., Rahman, M. M., Sayeed, S. A., & Sultana, I. (2024, May). cryptoRAN: A review on cryptojacking and ransomware attacks wrt banking industry-threats, challenges, & problems. In *2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT)* (pp. 523-528). IEEE. https://doi.org/10.1109/InCACCT61598.2024.10550970
28. Cremer, F. (2024) 'On the efficacy of modern cyber (re)insurance: an analysis of policy coverage, capacity constraints, cyber warfare, and data availability', available: https://doi.org/10.34961/researchrepository-ul.27369810.v1.
29. Wang, S.S (2019), 'Integrated framework for information security investment and cyber insurance', Pacific-Basin Finance Journal, Volume 57, 101173, ISSN 0927-538X, https://doi.org/10.1016/j.pacfin.2019.101173.