Pak. j. life soc. Sci. (2024), 22(1): 2184-2191 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences
www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2024-22.1.00161

RESEARCH ARTICLE

Challenges of Insuring Cyber Risks

Jaafar Kadhim Jebur [1], Amany Tammouz Abdul Rahman [2*]

1,2College of Law, University of Misan

ARTICLE INFO

Received: May 27, 2024

Accepted: Jul 1, 2024

Keywords

Challenges
Cyber
Insurance
Risk
Business companies
Legislation

***Corresponding Author:**

amanyprivate624@gmail.com

ABSTRACT

Although cyber risk insurance is a distinctive means for some businesses to cover losses and expenses resulting from those risks, this type of insurance still faces many challenges and constraints that hinder its growth and development compared to traditional risk insurance. These challenges can generally be classified into two main categories: Technical challenges related to the pricing of cyber risk insurance premiums and companies' fear of covering this type of risk, and legal challenges of the lack of legal rules on cyber risk insurance adding the ambiguity of the language of the contract.

INTRODUCTION

Business companies are now facing a major challenge to preserve privacy and protect their personal and customer data in front of the huge amount of cyber hazards that threaten the integrity of the business environment. However compliant they are with cybersecurity and safety procedures, this does not mean that these cybersecurity risks can be avoided altogether. Many of these risks are still uncontrollable because they are characterized by continuous development and cannot be avoided. However, the effects can be mitigated, in order to seek to mitigate the effects of cyber hazards. Recognizing these challenges and their negative impact on the future of businesses in general, A number of insurance companies have emerged offering non-traditional services such as cyber risk insurance, However, insurance of this new type of risk has faced many technical and legal challenges in terms of estimating the likelihood of cyber hazards and the extent of damage resulting therefrom is not defined by the extent that it is located in a cyberspace in which insurance companies share with the insured party, e-service employees, customers and stakeholders in general. This demonstrates the magnitude of the damages to be covered and the consequent difficulty in estimating insurance premiums and companies' fear of concluding insurance contracts against cyber risk, as well as the ambiguity of contract terms and the lack of legal rules specializing in cyber risk insurance.

2. Technical Challenges of Cyber Risk Insurance.

In this requirement, we will address the most significant technical challenges faced by this type of insurance, which has been discussed by many researchers in the field, namely: the difficulty of pricing insurance coverage from cyber risk, fear of insurance from cyber risk, which we will address by researching successively.

2.1. Difficulty of Pricing Insurance Coverage for Cyber Risks.

The lack of disclosure by businesses that have already been exposed to cyberrisket data about these risks and the physical and moral damage they have caused. To the scarcity of records necessary to fix insurance prices from cyber risks, despite the obligation of some countries to commercial companies that have already been exposed to a cyber risk of disclosure, as in the United Kingdom, companies are obliged to report this type of risk once they have achieved national security (Yueshan He). But we have two main problems: the first is that some laws may exclude from this obligation the cyber hazard that affects a few individuals. The other problem was described by some as biased laws, i.e. the relevant laws obliged business companies to disclose certain cyber risks without others. As in the United States, most states have adopted laws requiring companies to report cyber risks related to data breaches without those related to privacy violations or other cybersecurity incidents. For States that do not require businesses to report exposure to a cybercrime, the possibility of obtaining loss data for the purpose of reaching a conclusion of the cost of insurance prices is minimal (Sasha Romanosky). The insurance company will be a cyber risk company with two possibilities: the first is to set very high prices as a result of its uncertainty about potential losses in the future. The second risk is that the insurance company will set low prices and become unable to pay the obligations owed to policyholders that lead it to bankruptcy (Bob de Waard).

This is similar to (Penn Treaty Network America Insurance). Which was one of the largest insurers in the United States of America (Zain Mohey-Deen & Richard J. Rosen)? The question is, can it be priced according to the same mechanism as in traditional insurance contracts, or do cyber risk insurance contracts need to be unique to their own pricing mechanism?

By reference to the (CYBER RISK INSIGHTS) Conference 2019, we find that the use of technical bases based on proper actuarial analysis and probability models that were used in pricing and applying traditional insurance products to this type of insurance is only an exception to the public asset, The pricing of cyber risk insurance products depends heavily on market prices, which are based on competition, not analysis (Julie Bernard). In addition, insurance premiums are individually commensurate with the company's security vulnerability. Whenever the company is weak and exposed to cyber risks, the less the insurance premium can be done, and vice versa. Addressing the problem of high insurance prices lies in addressing this vulnerability through the investment of commercial companies in a security system (Yueshan He). Some companies seek to rely on a number of indirect factors for the purpose of pricing insurance contracts, by referring to market estimates of the cost of cyberattacks, or making special questionnaires to determine the risks from which it is possible to insure, or to rely on the pricing prevailing in the market that other insurers put at similar cyber risk (Andrew Granato). But these companies often fail to take into account when determining the insurance pricing equation their likelihood of being affected by advanced types of long-term cyber risks such as viruses, ransomware and hacking programs that lead to data violation, privacy and social engineering (Julie Bernard).

Regardless of the challenge of pricing cyber risk insurance premiums, insurers can rely on one of these factors for pricing premiums (Sasha Romanosky):

1. Reliance on external sources of pricing such as specialized organizations.
2. Estimate or guess the instalment payable.
3. Relying on competitors' pricing, although this practice may seem strange, it has become popular with many insurance companie.
4. Take advantage of their past experiences, and insurance companies tend to do this when trusted with their expertise sufficiently.
5. Rely on the instalments mentioned in other traditional insurance products.

Most recently, organizations have come up with the task of compiling data on losses due to cyber risk and the cost arising therefrom and selling it to insurance companies to assess the cost of insurance coverage and determine the appropriate premium prices United States-based industry leader (Sasha Romanosky). In order to accurately determine the premium, insurance companies may need to comply with the company's risk disclosure and the methods they have adopted to maintain a secure electronic system at work, as well as to determine the amount of technical and human support that can be provided if the risk is achieved (Sasha Romanosky). It may also be the best solution to evaluate these cyber risks by resorting to expert judgements in the field of cyber insurance or cyber security (Sasha Romanosky). Although this solution may be the most appropriate of the previous solutions, it is not without disadvantages as the risk factor of error still exists. As a result of experts disagreeing between them about opinions and backgrounds because of the different degree of knowledge of each of them, there is no moderate assessment of these risks either overestimating the risk or undervaluing it, which adversely affects the validity of projecting the amount of the premium (Michael Krisper, Jürgen Dobaj & Georg Macher).

2.2. Fear of Cyber Risk Insurance.

Business owners have considered this type of insurance to be a kind of luxury and not an urgent necessity. This has led companies to resort to other alternative solutions that are suitable for them, such as resorting to traditional general insurance contracts that perform the same purpose of insurance and low premiums, as opposed to not insuring specialized contracts against cyber risks, such as insurance for physical damages, crime insurance and general liability insurance (Julie Bernard). In fact, the general concerns about the high cost of insurance from cyber risks, what are only exaggerated concerns as the specialists in this field have found that these concerns are contrary to the reality of the Insurance Market, the coverage prices are almost equal to the annual budget allocated to IT security of the company that does not have insurance coverage. In light of this, the National Institute of Standards and Technology has directed NIST is a voluntary, non-binding framework for business companies to choose the best company in terms of cybersecurity practices, in order to incentivize companies to improve their security practices and reduce attack risk (Sasha Romanosky). Companies are increasingly fearful of entering into cyber risk insurance contracts because of their belief that these contracts do not adequately cover all damage caused by cyber risk (Biener, C., Eling M. & Wirfs, J). The terms of the contract may also be strict, i.e. they contain very restrictive clauses, restricting and narrowing the freedom of commercial companies, such as the contract stipulates that the insured business must contract with a cybersecurity company, which in turn represents an additional cost that burdens the company. The reason for the slowdown in insurance growth may be low coverage limits, while businesses prefer that cyber risk insurance contracts cover higher limits in how they cover all the costs they can incur if they are exposed to a cyber risk (Julie Bernard). It also poses a lack of knowledge and awareness of these risks. Or to disregard the damage that might be caused to the business if this risk is significantly challenged, Although this risk rating was raised from 15th in the 2013 year to 5th in the 2022 year, a large number of companies remain unaware of what cyber risk insurance is, as some surveys have found that 21 percent of businesses in Europe know what cyber insurance is for 79 percent of companies are not fully aware of what cyber risk means (Daniel Woods).

In our belief that the fear factor is a double-edged weapon, it may prompt companies to enter into cyber risk insurance contracts to protect against serious damage to these risks, and on the other hand, it may be a reason why companies are reluctant to do this type of insurance for its modernity, lack of knowledge of what it is and high cost. We believe in the need to activate the role of insurance brokers and multiply the time and effort to educate businesses and familiarize them with what this type of insurance is. The experience factor also plays a key role in this regard. Companies that have already experienced a cyber risk often speed up cyber risk insurance because of their fear of repeating exposure to those cyber risks. Unlike newly established companies that have never been

subjected to cyber threat, The greater the insured's experience, the greater the likelihood that he or she will be insured from cyber risk as a form of reaction to the risks to which he or she was previously exposed(Julie Bernard). Despite the insurers' feet to cover cyber risk, which is somewhat profitable for them, At the same time, however, this advantage may adversely affect customers' increased fear of the activity of insurance companies dealing with insurance contracts against cyber risk, as insurance companies are exposed to the same risks that customers think of insurance against, and the insurance company also engages in its activity in cyberspace (Bob de Waard).

3. Legal Challenges of Cyber Risk Insurance.

The cyber risk insurance market, in addition to technical challenges, has faced challenges of another kind, namely legal challenges, there are insufficient legal texts regulating cyber risk insurance contracts, and insurance contracts from this risk are somewhat complex, unmodified and ambiguous. We will divide this section into two parts, dealing first with the lack of cyber risk insurance laws, and second with the difficulty of drafting cyber risk insurance contracts.

3.1. Lack of Laws for Insurance against Cyber Risks.

The lack of legislative regulation of cyber risk insurance is one of the factors that businesses fear, as these companies often seek clear legal protection, as the general provisions of the insurance contract are almost insufficient to fill this legislative vacuum. It only outlines the insurance contract and is unable to regulate accurate and influential details in the field of cyber risk insurance. It would remove the ambiguity of this contract, and in this context it would be possible to use the case law and professional customs and the opinion of experts and specialists in the field of cybersecurity. In addition to using the experiences of some countries in the field of data protection and privacy, the legislation of this law in Iraq is imposed by practical necessity due to increased cyber risk and its ease of dissemination and increased awareness of the effects of these risks, generally speaking, cyberinsurance legislation and privacy are key to protecting electronic privacy, especially since this insurance requires more disclosure of customers' personal data than it actually needs (Bahaa Eltahawy; Jam et al., 2012).

Implementation of the GDPR could lead to an increase in the turnout of cyber risk insurance contracts, but so far the impact is somewhat modest for medium and small businesses (Even Langfeldt Friberg). In the absence of a cyber risk insurance law in Iraq, the question arises as to the scope of application of the General Data Protection Regulation (GDPR) to the cyber risk insurance contract? Can it be applied in Iraq or in other countries outside the European Union or is its application limited to EU countries?

Article 2 of the Regulation refers to the inapplicability of the provisions of the Regulation to any activity outside the scope of the European Union as a general rule and affirms that Article 99 decides to compel these Regulations and their direct applicability to all Member States as of May 25, 2018. But we find that, Article (3) has defined the territorial scope of the Regulation where it refers to the obligation to apply its provisions when processing or controlling personal data by any institution operating in the European Union regardless of whether the processing took place within the Union or in another country outside the Union, It also applies to institutions dealing with data whose subject matter relates to the European Union even if the institution is outside the Union. The provisions of the Regulation also apply to the processing of personal data by institutions not provided for in the European Union, but the processing process took place in a place where the law of a Member State applies under the rules of general international law. The regulation applies to all European citizens regardless of their whereabouts. It applies to any entity or institution that deals or controls the data of European citizens, or any entity located outside the European Union but handles personal data within the European Union.

We conclude from the foregoing that the scope of application of the regulation according to the above texts is broad and flexible, It is possible to apply its provisions to any company if it is the centre of its activity in the European Union or deals in personal data related to the European Union _ bearing in mind that there is no standard determining the relevance of personal data processed by insurance companies to the European Union _ or that its customers are in the European Union or that the data processing process takes place in the European Union.

However, the effect of the regulation on market growth may not meet expectations that fines and penalties are uninsurable (Mark Camillo). In addition, governments can contribute to the growth of the insurance market through legislation requiring government institutions to insure from cyber risks or by obliging companies to insure for preference in government contracts (Daniel Woods). We agree with the need to legislate a law regulating cyber risk insurance while not making it compulsory because high insurance prices may be a major obstacle to medium or small businesses. Large companies are also affected by compulsory insurance as the company's large size makes it complicated in terms of providing the data required for contracting and complying with the pre-contracting procedures. The closest solution to realism is to oblige specific people to insure against cyber risks such as government institutions, mixed companies or banks. These parties are the most needed to insure from cyber risks for their size and to be in touch with national security because the state is a party to it and is able to afford this type of insurance.

3.2. Difficulty in Drafting Cyber Risk Insurance Contracts.

The hallmark of cyber risk insurance contracts is complexity (Tsohou A). When drafting insurance contracts, insurance companies were affected by cyber risks, resulting in legal uncertainty affecting the writing of insurance contracts in multiple respects: The first aspect is the existence of legal uncertainty among customers as to whether the insurance company will cover some of the damages caused by the cyber risk to the insured business or not, such as the depreciation of the brand or stock, increased scrutiny of those wishing to invest in the company concerned, lower revenues or loss of customer confidence. The second aspect is the existence of legal uncertainty by insurance companies themselves, where cyber risk insurance lacks the existence of case law that contributes to raising their awareness about market policies, and resolving questions that may help these companies when writing their contracts (Andrew Granato & Andy Polacek). Uncertainty about insurance companies may result from their work in accordance with the provisions of the market that are not legally approved. Insurance companies must comply with the applicable practice with the approved or legally accepted markets. They must submit their contracts to government insurance committees and abide by all laws and regulations to obtain a work permit. However, the insurance company may ignore these liabilities and the legal restrictions imposed by the insurance commissioners and resort to selling insurance in an unapproved market by the State called "excess or surplus insurance lines" and estimated (NAIC), $1.8 million in annual premiums paid to insurers took place in these legally unrecognized markets (Sasha Romanosky).

The lack of legal expertise in writing cyber risk insurance contracts may result in the loss of the insurance company, Due to the haste in writing the terms of the contract, the insurance company may not stipulate that certain security care should be taken after the conclusion of the contract between it and the commercial company, resulting in the latter practice of fraudulent mint of less care in the field of its cybersecurity (Mohammed Said Ismail). The lack of standardized language for cyber risk insurance contracts, the ambiguity of contract terms and the lack of agreement of insurance companies often constitute a contributing factor in the slow development of the cyber risk insurance market (Sasha Romanosky). In addition to the foregoing, insurance companies remain generally unstable about what should be excluded from losses, which in turn leads to a lack of consistency between insurance companies' contracts and the occurrence of numerous litigation disputes.

The ambiguity of the language of the cyber risk insurance contracts also leads the insurer to renounce its obligations to the client (Julie Bernard). We believe that this ambiguity may be deliberate. Often, business companies requesting insurance are exploited and inspired by the method of drafting contract terms with the possibility of covering a certain number of cyber risks. The contract is based on the fact that the client believed it to fall within the coverage as a result of the client's inexperience in this area, to the surprise that the cyber risk could not be recovered because the realized cyber risk was not explicitly provided for in the terms of the contract. In addition to the above, the strict terms of the contract constitute an obstacle to companies' willingness to procure insurance coverage from cyber hazards, which raises their argument as to the usefulness of such insurance and whether it would be sufficient to remedy the consequences of cyber hazard or not, and would lead to numerous litigation between insurers and their clients. We believe that saying the need to standardize contract forms to all customers and pay them with the same premium regardless of the size of the client company or its employees or the amount of data it deals with is not fair. Although these contracts are easy to operate for insurance companies because of the time and effort needed to obtain the data of each customer individually. However, it slows the growth of the cyber insurance market, due to the reluctance of many SMEs to buy insurance products from cyber risk due to their inability to provide premium value. At the same time, concluding contracts for each client is difficult and complex. So we think that the combination of these two types of contracts is a good solution to get the advantages of the two methods and get rid of their defects at the same time. Where the insurance company can establish fixed contract forms for each specific category of companies, For example, the insurance company classifies its customers in such a way as to cover each category of them with a fixed-term contract form similar to companies that are of the same classification. Classification may be based on the size of the employees, the nature of the activity, the size of the capital, the extent of total or partial reliance on working in cyberspace, etc.

The cyber coverage available in the insurance market is still far from typical, and contracting procedures are still time-consuming.

CONCLUSION

First: Results:

1. The growth of the cyber risk insurance market is hampered by a number of technical challenges, the most important of which is the determination of insurance prices in the absence of records and data on the relatively modern cyber risk, which is difficult to count.
2. Commercial companies' fear of cyber risk insurance is a major impediment to the growth of this market, which has led some to introduce a number of mechanisms to determine insurance premiums accurately.
3. The lack of legal provisions on the regulation of cybercrime insurance is one of the most important legal challenges faced by this type of insurance.
4. Although the European General Data Protection Regulation (GDPR) for the year 2010 is specific to EU countries, its provisions can be applied to the cyber risk insurance contract outside the EU in cases specified in the Regulation.
5. The legislation of several laws on cybersecurity, privacy protection and data protection, as well as the formation of bodies and the development of specialized cybersecurity strategies, such as in Iraq, where the cybersecurity strategy of 2022 prepared the ground for the need to legislate all laws on cybersecurity and data protection, constitutes the cornerstone of the enactment of the Cybersecurity Insurance Act.
6. The difficulty of understanding and elaborating cyber risk insurance contracts plays a significant role in the lack of demand for this type of contract. Most business companies are difficult to know precisely what these contracts can cover and what they exclude from

covering them. Apart from the fact that the majority of court disputes were due to the ambiguous language of the cyber risk insurance contracts.

Second: Recommendations:

1. The need to create a uniform mechanism for pricing cybercrime insurance to avoid overstating its prices, and thus reluctance of commercial companies to insure against these risks. We propose to activate the role of experts and specialists taking into account the prevailing prices in the market and the need to standardize the models of cybercrime risk insurance contracts for each particular category of risk. Taking into account the move away from complexity and the tendency to simplify and clear language of the contract clauses.
2. Strengthen the culture of cybercrime insurance and begin to raise awareness of the importance and necessity of such insurance from State departments, breaking the fear barrier of most businesses.
3. Legislation on cyberinsurance, with the need to legislate Iraq's personal data protection law and taking into account the provisions of the European Data Protection Regulation (GDPR).

REFERENCES

1. Biener, C., Eling, M., & Wirfs, J. H. (2015). *"Insurability of cyber risk: An empirical analysis*". The Geneva Papers on Risk and Insurance-Issues and Practice, 40, 131-158.
2. Bob de Waard, Bernold Nieuwesteeg & Louis Visscher. (2018). "*The Law and Economics of Cyber Insurance Contracts: A Case Study*", European Review of Private Law, Volume 26, Issue 3.
3. Camillo, M. (2017). Cyber risk and the changing role of insurance. Journal of Cyber Policy, 2(1), 53-63.
4. Eltahawy, B., & Dang, D. (2022). Understanding Cyberprivacy: Context, Concept, and Issues.
5. Even Langfeldt Friberg, (2018). "*The Cyber-Insurance Market in Norway*": An Empirical Study of the Supply-side and a Small Sample of the Maritime Demand-side Master's thesis, TALLINN UNIVERSITY OF TECHNOLOGY School of Information Technologies.
6. Franke Ulrik, Meland per Hakon. (2019). "*Demand side expectations of cyber insurance"*, International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA).
7. Jam, F. A., Haq, I. U., & Fatima, T. (2012). Phychological contract and job outcomes: Mediating role of affective commitment. *Journal of Educational and Social Research*, *2*(4), 79-79.
8. Julie Bernard, (2011). "*Over coming challenges to cyber insurance growth expanding stand alone policy adoption among middle market businesses*", a report from the Deloitte center for financial services.
9. Kanval, N., Ihsan, H., Irum, S., & Ambreen, I. (2024). Human Capital Formation, Foreign Direct Investment Inflows, and Economic Growth: A Way Forward to Achieve Sustainable Development. *Journal of Management Practices, Humanities and Social Sciences*, *8*(3), 48-61.
10. Krisper, M., Dobaj, J., & Macher, G. (2020, August). Assessing risk estimations for cyber-security using expert judgment. In European Conference on Software Process Improvement (pp. 120-134). Cham: Springer International Publishing.
11. Mohammed Said Ismail,(2021). Cybersecurity: "*Legal Problems and Proposed Solutions - A Study in Country and Comparative Law*", International Law Journal, Volume X, Issue III, (Law Conference Issue in Response to Global Crises - Means and Challenges), Law Faculty, University of Qatar.

12. Rashid, A., Jehan, Z., & Kanval, N. (2023). External Shocks, Stock Market Volatility, and Macroeconomic Performance: An Empirical Evidence from Pakistan. *Journal of Economic Cooperation & Development*, *44*(2), 1-26.
13. Sasha Romanosky, (2016)."*Examining the costs and causes of cyber incidents*", Journal of Cybersecurity, Volume 2, Issue 2, December.
14. Sasha Romanosky. (2019). "*Content analysis of cyber insurance policies: how do carriers price cyber risk?*" Journal of Cyber security, Volume 5, Issue 1.
15. 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.
16. Woods, D., & Simpson, A. (2017). Policy measures and cyber insurance: a framework. Journal of Cyber Policy, 2(2), 209-226.
17. Yueshan He, (2016). "*Cyber Risk Insurance Pricing Based on Optimized Insured Strategy"*. A research paper presented to the University of Waterloo in partial fulfillment of the requirement for the degree of Master of Mathematics in Computational Mathematics".
18. Zain Mohey-Deen, Richard J. Rosen. (2018). "*The risks of pricing new insurance products: The case of long-term care*", THE FEDERAL RESERVE BANK ESSAYS ON ISSUES OF CHICAGO, NUMBER 397.