ESIC2024, Vol 8.2, S2 Posted: 04/08/2024

Legal Concept of Cyber Risk Insurance Contract

Dr. Jaafar Kadhim Jebur, Amany Tammouz Abdul Rahman

College of Law, University of Misan
Email: jaafar.kadhim.Jebur@uomisan.edu.iq

Abstracts

Business companies are at an unconventional and non-material risk that threatens their business reputation or brand potential in the market. (Cyber Risk), so insurance companies have introduced specialized insurance contracts designed to mitigate the impact of this devastating risk. The need for commercial companies to purchase cyber risk insurance policies has recently increased due to persistent and increasing threats to their operating systems containing the company's database and customers. It has become necessary for businesses to take note of how the cyber risk policy can be covered. At the same time, it is difficult to identify common exceptions in cyber risk insurance contracts because it is relatively recent. In addition, there is a kind of confusion between the insurance contract of cyber risk and some contracts that you may suspect on the other hand.

Keywords: Legal Concept, Cybercrime Insurance, Cyber Risk Insurance, Business Companies.

Introduction

Cyber Risk Insurance Contracts have privacy that distinguishes them from the corresponding traditional types of insurance in terms of terms, nature of risks or damages covered. Cyber risk insurers have not agreed on the cyber risk excluded from their coverage yet, some insurers may exclude certain cyber risk coverage. While another insurance company includes a cyber hazard with coverage provisions, this is often due to the lack of a cyber risk insurance law that identifies the risks covered within the contract. Given that the cyber risk insurance contract is relatively recent, the confusion between (cyber risk insurance contract), between (electronic insurance contract) on the one hand, and between (cybersecurity contracts) on the other hand, so it is necessary initially to indicate what the insurance contract is from cybersecurity and to clarify its privacy compared to the other types of insurance. After that, a statement of the exceptions that may be made to this contract, then distinguish it from suspected decades, so we will divide this research into two requirements, we devote the first to the introduction of the cyber risk insurance contract and the exceptions contained therein. In the second requirement, we address the distinction of the insurance contract from cyber risk to suspect.

Definition and exceptions to the Cyber Risk Insurance Contract.

It is necessary to inform businesses about what cyber risk insurance contract is and what risks it can cover, but at the same time we find it difficult to identify the common exceptions in cyber risk insurance contracts due to its newness.

2.1. Definition of Cyber Risk Insurance Contract.

It may be difficult to insure against cyber risks due to the absence of historical data about this new type of risk, as insurance generally needs to provide a large number of data and statistics about losses and damages and how to price them. This led many insurance companies to overlook the introduction of cyber risk insurance contracts while some insurance companies introduced insurance contracts covering damages resulting from specific categories of cyber risk. However, covering cyber risks in insurance contracts may be either in the form of individual policies (stand- alone policies) where each risk is covered by a policy of its own, or the policy may cover many risks simultaneously (Salah Hadi and Zeid Ismail). What distinguishes cyber risk insurance contracts from other conventional contracts is the difficulty of standardizing the terms and terms of cyber risk insurance policies (Chadha Abdul Juma Musa). As a result, the underwriting of cyber risk insurance is often highly ad hoc as each business customer has its own coverage, making insurance for this risk independently or so-called risk more common, because the changing nature of cyber risk makes the scope of insurance coverage in a state of flux (Even Langfeldt Friberg).

Through the conclusion of the Cyber Risk Insurance Contract, commercial companies pursue two main objectives: The first is to mitigate the risks. The insurance contract guarantees compensation for financial losses and interrupts its operations due to the cyber risks covered by this contract. The contract also aims to compensate the company (the insured) for the legal exposures it requires and makes it more aware of these exposures by meeting higher standards in terms of data protection and cyber security (Sofronov, G., & Trück, S). The second is to fill the shortfall in traditional insurance policies by considering that the cyber risks are broad and multiple and in a continuous development that is not covered by the traditional insurance policies, where electronic losses are excluded. Therefore, it can be said that the cyber risk insurance contract came to complement the shortfall and fill the gaps in traditional insurance policies so that these risks are legally covered. The cyber risk insurance contract often covers the following losses (Majid Mohammed Suleiman):

1. Crisis management costs incurred in dealing with adverse cyber incidents, especially violation of personal data.

2. Non-physical interruptions caused by the cyber risks of commercial companies, different from the interruption of traditional businesses because the latter arises from physical hazards such as fire. The interruption of intangible works is caused by the interruption of intangible information technology such as the failure of the system. What distinguishes this coverage from the rest of the coverage in the field of cyberinsurance is that it applies a waiting period calculated by hours and once it ends, the losses are compensated retroactively, for example, 120 days after the outage starts or 90 days after the outage ends.

3. Costs of specialists in the field of electronic extortion and the costs of ransoms resulting from the extortion process.

4. Liability arising from breach of privacy, confidentiality and information technology security.

5. First Response Costs: Cyber risk insurers are obliged according to their contract with the commercial company to cover the costs of the first response to detect the presence of cyber hazard, such as the costs of a legal consultant or an IT specialist who can provide the support and coordination required to minimize the damage caused by realizing the cyber risk if it occurs.

6. Fees and costs necessary for data protection and recovery of costs and expenses incurred by the covered company to restore recreate or restore access to any software or electronic data from backups or originals. Collect and recreate such software or electronic data from other sources to the level or condition on which they were located immediately before they were changed, destroyed, deleted or damaged (Sofronov, G., & Trück, S.) .

7. The majority of insurance contracts provide coverage from the risk of social engineering route.

8. Compensation for damage to the company's operating systems and material components, such as computers.

9. Long-term reputational damage to the insured company, which is often difficult for the judge to assess.

10. Liability arising from infringement of intellectual property rights and publication.

11. Network Security Liability: Cyber Risk Insurance provides coverage for defense and settlement costs in the event of third parties suing the commercial company for breach of privacy, unintended dissemination of malware, incitement to denial of service attack, unauthorized access to the system, unauthorized use, and denial of service attack by third parties, transfer of malware to the business or its customers (Salah Hadi and Zeid Ismail).

12. Some insurance companies may cover death or bodily injury and regulatory penalties although the predominant position in cyber risk insurance contracts is that they cannot be covered.

The cyber risk insurance contract is based on the principle of multilateral security where we cannot assume that all parties to the contract trust each other. So the specificity of the contract is that security is not assessed by surveillance of cyber risks caused by external parties. It also requires the inclusion of potential internal attackers to the parties to the contract, i.e. everyone should be protected against anyone else. It is worth noting that the drafting of cyber risk insurance contracts is often in general terms so that all the risks under them are dealt with in accordance with a single coverage and the purpose is to minimize the obligations required of the insurance company in the future so that the total amount paid to commercial companies does not exceed the agreed limit of each commitment. This is known as b (Assembly language or clause) in the insurance contract, and the judiciary settled in the United Kingdom Supreme Court in the AIG Euorpe limited case) "(v. woodman) However, all actions arising out of an act or omission

and related to each other are genuinely interrelated and in some way tailored to each other, it ensures that they are regarded as a single action (Cartwright, A., Cartwright, E., & Edun, E. S Grzebiela, T) .

Based on the foregoing, we can define the cyber risk insurance contract as: "A contract covering damages arising from risks directly or indirectly associated with information technology targeting every natural or moral person operating through cyberspace."

2.2. Exceptions to the Cyber Risk Insurance Contract.

The lack of a general and consistent rule applicable to all cyber risk insurance contracts leads to discrepancies between insurers' contracts in terms of exceptions in their contract terms. Through a number of contracts and studies on cyber risk insurance, the most common exceptions are those that are not directly related to cyber risk per se but to the circumstances surrounding it. Therefore, insurance companies dealing with cyber risk often exclude the following risk coverage (Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G. W.,):

1. Penal or administrative fines.

2. Risks arising from failure of maintenance or failure to maintain minimum safety standards.

3. Although cyber risk insurance contracts cover damage caused by the use of social engineering in cyber fraud, many coverage forms contain clauses that allow the insurer to avoid covering such damages when the cyber risk is caused by overriding the company's security controls. If the cyber hazard is realized by the insured, or when the telephone fraud is carried out instead of using the computer directly or when the losses incurred are "indirect" damages to the insured, such as losses to customers' funds.

4. Theft of data without damage will be excluded from insurance coverage.

5. Claims for contractual obligations incurred by the business company against others after the realization of the cyber risk such as regulatory fines imposed by some NGOs such as PCI.

6. Exceptions to war, terrorism and damage caused by ransomware if there is no doubt that extortionists are terrorists.

7. Dishonest behaviour: any deliberate, criminal, fraudulent or insecure act or omission, or intentional violation of any duty or contractual obligation, law or regulation, For example, the insured business company causes loss of business interruption, However, coverage can include voluntary closures associated with exceptional circumstances to reduce the spread of certain cyber hazards such as malware and viruses or to reduce the damage caused by these risks (Majid Mohammed Suleiman).

8. Cyber risk insurance contracts may sometimes include a retroactive effective date, so that pre-date accident losses are not retroactively covered by cyber risk coverage (Ma Abdullah Sadiq).

9. Exceptions associated with the theft of the company's employees' data. Most of these contracts involve the coverage of customer data only.

10. Some argue that insurance coverage cannot include breaches of confidentiality and privacy because it is often impossible to assess damage to the insured or his clients because of the difficulty of proof. We believe that the risk of infringing the confidentiality and privacy of businesses and their customers is almost the main reason why the need for cyberinsurance arises. The objective of these risks is primarily to breach privacy and confidentiality and to target data for the purpose of inflicting heavy losses on the business and its customers whether it is material losses to the company's funds or moral losses such as those to its business reputation. It is not conceivable to realize a cyber risk to a trading company without violating its privacy. So the exclusion of privacy violations from coverage will result in the lack of benefit from insurance for the rest of the cyber risk because all of them are entitled to through the occurrence of a privacy violation or data theft. However, this does not disprove the earlier view that it is difficult to estimate compensation for invasion of privacy and theft of data as a matter of differing judgement as to the nature and size of the company's business activity and what its customers are (Hanan Malika).

11. Cyber risk cannot be covered by insurance coverage if the source of risk is within the insured company such as network operators, service providers or maintenance workers because the possibility of achieving the risk is more likely than external sources. They possess the expertise that enables them to penetrate the business system as well as their knowledge of the company's business secrets because of their work within them, which makes it difficult to assess the risk due to the diversity of its sources (Habib Al Amarah and Maher Al Khaikani).

12. The insurance company always excludes from cyber risk those losses resulting from disruption of public utilities such as gas, water, Internet and satellite service providers. Insurance companies also exclude the cost of restoring the system to a higher functional level than it was. It should be noted that the cyber risk insurance policies exclude damage to physical property or bodily injury resulting from the verification of a cyber risk subject to the contract from being covered, but at the same time some traditional insurance contracts can indirectly cover damage to physical property and bodily injury resulting from a cyber risk in the commercial company through insurance from public liability. This is known as silent cyber risk coverage, which exposes traditional insurers to liabilities that burden them when compensating for damages arising from cyber risk without those risks being covered(Salah Hadi and Zeid Ismail).

Distinction of Insurance Contract from Cyber Risk to Suspected Contracts.

Given the novelty of the cyber risk insurance topic, we find it necessary to distinguish between the cyber risk insurance contract and contracts that may provoke some kind of confusion and ambiguity for the recipient at first sight because there is some convergence and overlap between them, such as the electronic insurance contract and cyber security contracts.

3.1. Distinguishing Cyber Risk Insurance Contract from Electronic Insurance.

The traditional form of an insurance contract is the paper form, that's what insurance companies used to do when contracting with their clients. However, with the invasion of modern electronic means for all sectors of life, especially business, these means have had a significant

impact on streamlining insurance procedures in terms of time and effort, As a result, the contract could be emptied electronically through the use of Internet networks and related information technologies to produce and distribute insurance services and products (Fatiha Belt).

Since e-insurance is a relatively modern legal term where insurance services are offered, negotiation, application and conclusion of the contract in a flexible electronic manner away from administrative complexities, Thus, the e-insurance contract is only a contract to which the insured is obliged to provide his insurance services and related offers, negotiations, contracting or paying premiums through electronic means, and by reference to the Electronic Signature and Electronic Transactions Act No. (78) For the year 2012, an electronic contract is generally understood in accordance with article 1, paragraph (11), thereof: "The affirmative issued by one of the contractors is linked to the acceptance of the other in a manner evidenced by its effect in the contract, which is made by electronic means" (Habib Al Amarah and Maher Al Khaikani). The above law is granted to electronic contracts with legal authorization granted to paper contracts in accordance with article (13/I) of the same law provided that the information contained in the contract is storable and preservable and can be recovered at any time, The information contained therein may be kept in a manner that is easy to establish at the time of the establishment, dispatch or receipt of the electronic contract without modification and that the information contained in the contract shall indicate who created or received the contract with the date and time of the transmission and delivery. Although no law on electronic insurance has been legislated in Iraqi law, it is possible to refer to the provisions of the Electronic Signature and Electronic Transactions Act No. 78 of 2012 in order to arrive at the main rules by which an electronic insurance contract can be concluded. We can define an electronic insurance contract as "an insurance contract concluded or executed through any electronic means"(Mohammed Said Ismail).

The Electronic Insurance Contract with the Cyber Risk Insurance Contract shares that both contracts are acquiescence contracts. The insured agrees to specific terms according to pre-prepared forms and does not have the right to discuss these terms. They are also unnamed contracts where they are governed by the general rules contained in the laws governing contracts, transactions, electronic commerce and related regulations and there are no legal rules specializing in electronic insurance or cyber risk insurance so they cannot be considered among the so-called contracts. In addition, the Cyber Risk Insurance Contract is shared with the Electronic Insurance Contract as cross-border contracts. Electronic means of contracting have been able to exceed the political boundaries of States, facilitating the contracting process, especially those of which the parties are affiliated with more than one State. So is the cyber risk insurance contract where the insurance contract can cover commercial companies with their branches spread across more than one country around the world.

They are also regarded as good faith contracts based on mutual trust between the parties through which the parties to the insurance contract are obliged to disclose all information and data necessary for the insurance process during the negotiation phase or the conclusion of the contract (Islam Mustafa Juma).

Although the concept of an e-insurance contract is simple, we find that some have fallen into confusion by launching the term cyberinsurance and making them synonymous. This may

be due to the novelty of the terminology in the jurisprudence and perhaps due to the inaccurate translation of cyber risk insurance from foreign languages into Arabic. We find that cyber risk insurance is translated as a synonym for the term electronic insurance, although there is a significant difference between electronic insurance, which is only a regular insurance contract arising by electronic means(Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G. W).

The cyber risk insurance contract is an insurance contract whereby a new type of often intangible risk, located in a cyberspace and called cyberspace risk, is covered by ransomware, denial-of-service attacks, phishing, fraud, social engineering, intermediary attack, information bombs, viral attacks and other risks previously researched. Insurance coverage includes a new type of damage caused by the company's previously uncovered liability recovery costs, such as intellectual property violation legal resulting from breach of privacy, confidentiality, IT security, losses resulting from electronic extortion and other damages that may vary by different document concerned with securing this type of cyber risk. There is no legal impediment to the electronic conclusion of the cyber risk insurance contract. The contract is done electronically to cover electronic risks. So we can conclude that the electronic insurance contract is a normal insurance contract that is characterized by the method of its electronic conclusion regardless of the nature of the risks it covers. A cyber risk insurance contract is an insurance contract that covers non-traditional risks and may be done in paper or electronic form (Chadha Abdul Juma Musa).

3.2. Distinguishing a Cyber risk Insurance Contract from a Cyber Security Contract.

Cybersecurity, or so-called cybersecurity, is one of the branches of technology that protects operating systems, digital property, networks and software from cybersecurity that can often damage data, extort customers, or control companies' business operations, is a set of tools, policies, cybersecurity concepts, guidelines and risk management methods to provide best practices and safeguards to protect the digital environment and user assets and has multiple definitions. The term is used from a legal perspective to refer to the totality of laws and texts on security, ways of administering hazards and technological practices and everything related to ICT security, whether used to protect States, organizations or persons (Cartwright, A., Cartwright, E., & Edun, E. S Grzebiela, T).

While some give a broader concept of cybersecurity, it relates to all actions on cyberspace, whether in the owner's knowledge or without his knowledge, as well as all technologies, products and efforts to defend against cyberspace, It is also defined as a case where ability is granted to address everything that interferes with the integrity of stored, processed or transmitted data for espionage, alteration or damage. Cybersecurity expands into multiple areas such as commercial cybersecurity issues and cybersecurity contracts. Digital currencies, digital intellectual property issues, cyber laws, privacy protection laws, cyber crimes, as well as their overlap with international jurisdictions such as holding governments accountable for cyber attacks and other fields. The U.S. Department of Defense defined cybersecurity as "all necessary regulatory measures to ensure the protection of information in all its electronic and physical forms from various crimes, attacks, sabotage, espionage and accidents. The UK's National Cyber Security Centre (NCSC) also defined it as "the way individuals and institutions reduce the risk of cyberattacks." Previously, the Egyptian Insurance Federation's bulletin was defined as an

umbrella term for a wide range of issues starting from information technology security to security measures aimed at combating Internet abuse and cybercrime (Salah Hadi and Zeid Ismail).

It should be noted that maintaining a good level of cybersecurity may necessarily require contracting with cybersecurity companies or hiring IT professionals in commercial companies for the purpose of protecting operating systems and software from cybersecurity exposure. This is a course that constitutes an obstacle to many of these companies, especially small or medium-sized companies, because of the high cost of cybersecurity contracts.

We conclude from the foregoing that cybersecurity is the defense of computers, servers, mobile devices, electronic systems, networks and data, From cyberattacks directly or indirectly regardless of whether they arise from within or outside the organization and are called electronic information security or information technology security. Cybersecurity companies provide many cybersecurity services such as cybersecurity governance, which consists of two phases, the first is the security department and the second is security governance. Security management ensures that cybersecurity risks are adequately reduced through the deployment of security controls, while security governance easily links public security strategies with key business objectives and core regulations (Majid Mohammed Suleiman).

We believe that the cybersecurity contract is similar to the cybersecurity contract in the following ways (Even Langfeldt Friberg):

1. The Cyber Security Contract and the Cyber Risk Insurance Contract are a tool taken by business companies to reduce or eliminate cyber risks and damages.

2. The place of the contract in both is cyber hazard.

3. In both decades, we need engineering expertise in cyberspace and cyberrisk.

4. There is no legal regulation of both contracts so far in Iraq's legislation and comparative legislation.

We also see that the concept of cybersecurity is broader than the concept of insurance from cyber risks, as cyber security, it is a set of preventive or defensive measures that may be exercised by the state or private natural or legal persons to maintain the security and integrity of data and information that are dealt with within cyberspace. As for insurance against cyber risks, it is a non-preventive treatment method, a contract aimed at transferring the responsibility of cyber risks to the insurance company, through which losses resulting from the failure or weakness of the insured's cyber security procedures are covered, whether intentional or unintentional, as it exposes information and data systems. The insured companies and their vital infrastructure are damaged, so the goal of the coverage is to repair the damage caused by a defect in the cybersecurity of companies operating within cyberspace (Cartwright, A., Cartwright, E., & Edun, E. S Grzebiela, T).

Conclusion

First: Results:

1. The Cyber Risk Insurance Contract is a contract that covers the damage caused by risks directly or indirectly associated with IT that are aimed at every natural or moral person operating through cyberspace.

2. Cyber risk insurance contracts are technically complex, relatively high, and require specific pre-insurance requirements. They are also ambiguous. They contain broad and flexible terminology, allowing easy avoidance of contractual obligations on the pretext of vagueness of terms under the terms of the contract. Doubt is always interpreted in the debtor's interest.

3. The cyber risk insurance contract covers many costs: Costs of crisis management and interruption of intangible business, costs of specialists in the field of electronic extortion and legal liability arising from breach of privacy, confidentiality, IT security and others, Insurance companies dealing with cyber hazard often exclude insurance from penal or administrative fines. Physical injuries, risks of war, terrorism and damage caused by ransom programs if there is no doubt that extortionists are terrorists and others.

4. The term cyber risk insurance may be mixed with other legal terms such as cyberinsurance and cybersecurity terms because of some similarity between them, but the fact is that the electronic insurance contract is only an insurance contract made by electronic means - i.e. paperless - as required by the law of electronic signature and electronic transactions. The cybersecurity contract is a security measure taken by individuals and companies to protect and minimize the harm of cybersecurity.

Second: Recommendations:

1. We recommend that the Iraqi legislator not merely meet the general rules of insurance set out in the rules of the Iraqi Civil Code and legislate a law on the cyber risk insurance contract that specifies the risks from which it can be insured and those excluded from coverage, because the specificity of this contract compared to traditional insurance contracts makes it difficult to satisfy the general rules.

2. We recommend the need to establish specialized cyber risk insurance companies and to include this type of risk in the insurance insurers' insurance risk categories at least because of the lack of a company specializing in the insurance protection of commercial companies against cyber risk in Iraq to date.

WORKS CITED

Cartwright, A., Cartwright, E., & Edun, E. S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. Computers & Security, 131, 103288.

Chadha Abdul Juma Musa, (2019). "Digital Intellectual Property Infringement Risk Insurance", New University House, Alexandria.

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.

Fatiha Belt, (2021) "Provisions Related to Electronic Insurance Services", Muhammad Boukara Boumerdas University Magazine, Vol. (14), Issue (1).

Grzebiela, T. (2002). Insurability of electronic commerce risks. In Proceedings of the 35th Annual Hawaii International Conference on System Sciences (pp. 9-pp). IEEE.

Habib Obaid Marzeh Al Amarah and Maher Mohsen Aboud Al Khaikani, (2018), "Legal Organization of Electronic Insurance", Journal of Babylon University of Humanities, Volume (26), Issue (8).

Hanan Malika, (2022), "Electronic Insurance Contract", Damascus University Journal of Legal Sciences, First Issue Vol. (2).

Islam Mustafa Juma, (2022). "Cybersecurity Offence and Protection of the Use of Data and Information in Egyptian Law", Legal Journal, Volume (12), Issue (3).

Ma Abdullah Sadiq, (2008), "Council of Electronic Contract", Master's thesis presented to the Graduate School/National University of Success.

Majid Mohammed Suleiman, (2009), "Electronic Contract", T1, Al Rashid Library, Riyadh.

Mohammed Said Ismail, (2021) "Cyber Insurance: Legal Problems and Proposed Solutions - A Study in Country and Comparative Law", International Law Journal, vol. 10, No. 3, "A Law Conference Issue in the Face of Global Crises - Means and Challenges".

Salah Mahdi Hadi and Zeid Mohammed Ali Ismail, (2020), "Cyber Security as a New Anchor in Iraqi Strategy", Faculty of Political Science University of Nahrin, Journal of Political Issues Issue (62), Year (12).

Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G. W., Sofronov, G., & Trück, S. (2023). The nature of losses from cyber-related events: risk categories and business sectors. Journal of Cybersecurity, 9(1), tyac016.