Artigo original

http://dx.doi.org/10.18623/rvd.v23.n3.4297

INSURANCE AGAINST CYBER RISKS: COMPARATIVE STUDY

SEGURO CONTRA RISCOS CIBERNÉTICOS: ESTUDO COMPARATIVO

Article received on: 9/2/2025
Article accepted on: 12/1/2025

Elsoghair Mohamed Mahdy*
*Faculty of Law, Abu Dhabi University, Al Ain City, Emirate of Abu Dhabi, United Arab Emirates
Orcid: https://orcid.org/0000-0002-8702-9724
elsoghair.mahdy@adu.ac.ae

The authors declare that there is no conflict of interest

Abstract
The digital community faces a myriad of legal challenges, among which a particularly significant issue is the matter of insurance against the risks associated with digitization. These risks encompass cyber-security threats, the implications of digital advancement, electronic attacks, digital hacking, infringements on digital privacy, and a host of other related vulnerabilities. In recognition of the significant challenges faced by digital institutions and their stakeholders in preserving privacy policies, protecting data, and ensuring information security, cyber insurance—also referred to as insurance against digital risks or electronic insurance—has emerged as an innovative and crucial solution. This form of insurance has arisen in response to the needs of companies to safeguard their interests and mitigate the damages resulting from cyberattacks aimed at data breaches and privacy violations. Accordingly, this research endeavors to analyze the legal issues associated with the provisions of insurance against the risks of digitization, commonly referred to as electronic insurance against cybersecurity threats. This analysis is particularly conducted given the escalation of cyberattacks and the increasing demand for electronic insurance solutions. Furthermore, this study seeks to highlight the urgent need of establishing a coherent and well-structured legal framework governing contracts related to digitization risks or electronic insurance within national legislations.

Keywords: Insurance Against Digitization Risks. Electronic Insurance. Cyber-Risks. Digital Risks. Cyber Liability. Digital Insurance. Digitization Risks.

Resumo
A comunidade digital enfrenta uma infinidade de desafios jurídicos, entre os quais uma questão particularmente significativa é a do seguro contra os riscos associados à digitalização. Esses riscos abrangem ameaças à segurança cibernética, as implicações do avanço digital, ataques eletrônicos, pirataria digital, violações da privacidade digital e uma série de outras vulnerabilidades relacionadas. Em reconhecimento aos desafios significativos enfrentados pelas instituições digitais e suas partes interessadas na preservação das políticas de privacidade, proteção de dados e garantia da segurança da informação, o seguro cibernético — também conhecido como seguro contra riscos digitais ou seguro eletrônico — surgiu como uma solução inovadora e crucial. Essa forma de seguro surgiu em resposta às necessidades das empresas de proteger seus interesses e mitigar os danos resultantes de ataques cibernéticos voltados para violações de dados e privacidade. Assim, esta pesquisa se propõe a analisar as questões jurídicas associadas às disposições do seguro contra os riscos da digitalização, comumente referido como seguro eletrônico contra ameaças à segurança cibernética. Essa análise é realizada especialmente devido à escalada dos ataques cibernéticos e à crescente demanda por soluções de seguro eletrônico. Além disso, este estudo busca destacar a necessidade urgente de estabelecer um marco jurídico coerente e bem estruturado que regule os contratos relacionados aos riscos da digitalização ou ao seguro eletrônico nas legislações nacionais.

Palavras-chave: *Seguro Contra Riscos de Digitalização. Seguro Eletrônico. Riscos Cibernéticos. Riscos Digitais. Responsabilidade Cibernética. Seguro Digital. Riscos de Digitalização.*

1 INTRODUCTION

The contemporary world is undergoing a qualitative transformation characterized by an intensified reliance on the Internet as a fundamental aspect of daily existence. This digital space presents extensive opportunities for communication and the exchange of information. However, this growing dependence is accompanied by formidable challenges concerning privacy and data theft. Recent studies have yielded that violations of digital privacy are on the rise, thereby affecting individuals' trust and behavior towards organizations involved in such breaches. (Wanjugu, C., Mutiso, J., and N. Kariuki. 2022),(Bartol, K. 2023).

The millennial generation is recognized as the most cognizant of the risks associated with data protection, as research demonstrates that this generation actively employs proactive strategies to fortify the security of their personal information(Alkire, L., G. O'Connor, and F. Wynstra. 2019). Nonetheless, a significant number of users still exhibit a limited comprehension of the complexities inherent in the risks linked to online data sharing. This discrepancy gives rise to what is termed the "privacy paradox," a phenomenon wherein actual behaviors are at odds with articulated concerns. (Lutz, C., C. P. Hoffmann, and G. Ranzini. 2020).

The challenges associated with digital privacy protection have significantly intensified during global crises, particularly in the context of the COVID-19 pandemic, which has known an unprecedented rise in reliance on digital technology. Studies indicate a surge in cyberattacks during this period, manifesting the urgent need for advanced data protection strategies .(Cheng, L., F. Liu, and D. Yao. 2020)& (Krishna, A., R. Nayak, and M. Poojary. 2021). In this context, technologies such as machine learning and blockchain have demonstrated promising potential in enhancing cybersecurity and safeguarding privacy in online environments, including the Internet of Things. (Waheed, A. 2020). These threats are not only limited to individuals alone; they extend to encompass organizations and nations. Research has demonstrated that cyberattacks increasingly target critical infrastructure, posing a significant risk to national security. (Deep, A., N. Sharma, and P. Verma. 2020)&(Yahuza, M., B. Usman, and T. Adewale. 2021).Consequently, it has become imperative for both companies and governments to adopt comprehensive strategies aimed at enhancing security awareness and fortifying

cybersecurity practices. (Torre, L., R. Smith, and P. Gomez. 2023)&(Elrawy, M., A. Abdelhamid, and A. Sallam. 2018).

The phenomenon of remote work has also contributed to the exacerbation of cyber risks, with studies demonstrating a significant increase in cyberattacks in 2020 compared to the previous year. The Global Risk Report published by Allianz in 2023 confirmed that cyberattacks have become more sophisticated, targeting companies that rely on the collection and utilization of customers' personal data, resulting in substantial economic losses and undermining trust in digital services.(Sithole, P., K. Mabunda, and T. Dube. 2023). Statistics indicate that global cyberattacks surged by 38% in 2022, driven by the evolution of attack tools based on artificial intelligence technologies, thereby complicating efforts to address these threats .(Sithole, P., K. Mabunda, and T. Dube. 2023).

Many countries, including those in the European Union, are facing increasing challenges related to a shortage of qualified personnel in the field of cybersecurity. For instance, statistics reveal that over 80% of European institutions experience a deficiency in specialized competencies in this area (Kuzior, A. 2023). Reports emphasize the necessity of developing a comprehensive legal framework to enhance cybersecurity and data protection, alongside strengthening cooperation among nations to address shared challenges.(Bermanns, J. 2023)&(Salvaggio, L., and M. González 2022).

In the Arab region, cyber challenges are prominently evident, with reports indicating a 30% increase in cyberattacks on critical sectors during 2022 and 2023, particularly targeting healthcare and education.(Al-Fraihat, M. 2023). Studies highlight that the shortage of qualified personnel and inadequate legal frameworks pose significant challenges to the efforts aimed at countering these threats.(Duraye, M. 2023).

From this perspective, it has become essential to raise awareness of the importance of cybersecurity and digital risk insurance as an effective tool for covering losses resulting from cyberattacks. Accordingly; this study aims to examine the legal issues associated with insurance against digital risks, highlighting the obstacles that hinder the development of this market, and proposing legal and regulatory solutions to strengthen data protection in future contracts.

Accordingly, this study raises several questions, the most prominent of which are:

1. Are the existing legal frameworks sufficient for the successful and effective regulation of insurance against digital risks, such as coverage for cyberattack risks, violations of digital privacy, and artificial intelligence-related risks?
2. Can insurance companies provide adequate protection for individuals and businesses against digital risks, including cybersecurity threats?
3. To what extent can insurance against digital risks or electronic insurance enhance the economic and digital security of nations?
4. Does the development of the digital or electronic insurance market contribute to reducing the legal uncertainty associated with cybersecurity risks?

The research focuses on analyzing the legal frameworks for digital or electronic insurance against cyber risks, employing a variety of scientific methodologies, including:

- The analytical legal method to address relevant legal texts.
- The comparative method to explore electronic insurance legislation in the UAE and comparative laws.
- The Practical and Deductive Method: To extrapolate future challenges and provide practical solutions.

2 METHODOLOGY

2.1 The concept of insurance against cyber risks

Cyber and digital risks refer to threats that target information systems and networks through cyberattacks or illegal activities aimed at data and information. These risks include a variety of threats, such as hacking aimed at unauthorized access to systems, malware that infects systems to cause damage or steal data, as well as cyber fraud, espionage, and data loss, which can cause significant harm to individuals and businesses.

Despite the growing significance of addressing cyber and digital risks, the digital or electronic insurance sector remains relatively new, exhibiting a developmental lag in comparison to more established commercial insurance products. This market necessitates enhanced efforts to devise effective insurance solutions that are commensurate with the dynamic and evolving nature of digital and cyber threats. The primary objective of such

insurance is to provide comprehensive protection against damages or losses arising from the inherent risks associated with digitization and information technology vulnerabilities.

2.1.1 Cyber risks

Etymologically, the term (cyber) is derived from the word "Cybernetics" which is defined as "the science of automatic control,". The term was first introduced by the American mathematician Norbert Wiener in 1948. The linguistic roots of the term "Cyber" can be traced to the ancient Greek verb (Kybereo), meaning "to steer" or "to govern." However, some legal and linguistic scholars suggest that the term has Latin origins, where "Cyber" is linked to the notion of "cyberspace" or the "information domain" (What does cyber mean?).

Cyber risks are defined in many different ways. Some scholars define them as "potential threats that compromise the confidentiality, integrity, and availability of information and information systems, potentially leading to financial losses, data breaches, or reputational harm to organizations"،.(Al-Rubaie, A. 2024).& (Al-Zyoud, M. 2020). This definition emphasizes that cyber risks extend beyond mere financial repercussions to include detrimental effects on institutional reputation and business continuity. Accordingly, it demonstrates the critical need for the implementation of effective risk management strategies to mitigate their impact on organizational stability and operational resilience.

In another definition, cyber risks are described as "any risk arising from the occurrence of an electronic incident related to the use of information and communication technology, which negatively impacts the capacity, availability, integrity, or traceability of data or services. Such incidents may lead to the impairment of operational technology, business disruptions, infrastructure failures, as well as physical harm to individuals and property."

Based on the aforementioned definitions, it becomes apparent that cyber risks encompass a broad range of threats arising from the use and exchange of electronic data. These risks include not only material damages resulting from cyber incidents but also fraud related to the misuse of data and legal liabilities associated with data storage and confidentiality. Such risks are clearly manifested in the event of cyber incidents that cause

operational disruptions, whether these disruptions result from accidental occurrences or intentional actions by unauthorized entities—excluding errors committed by companies or individuals themselves.

2.1.2 Types of cyber risks

The contemporary digital environment is characterized by a wide range of electronic and cyber risks that pose significant threats to both individuals and businesses. These risks can be categorized into the following key types, as outlined by scholars such as Corbett & Hadwin.(Corbett, M. 2021)&(Hadwin, S., and J. Monck-Mason. 2020).

-Cyberattacks: These include attacks that target systems and networks with the aim of causing damage or obtaining sensitive information in an illegal manner. The most prominent of which are Ransomware attacks which are used to encrypt data and demand ransom money in exchange for decryption. Hacking attacks is another example aimed at getting unauthorized access to systems or networks, threatening the integrity and security of data.(Duraye, M. 2023).&(Al-Suhaili, M. 2023).

- Electronic forgery: It is regarded as one of the most significant cybercrimes, encompassing the falsification of electronic documents or digital signatures. This type of crime necessitates the fulfillment of specific legal elements, namely: the material element, which refers to the physical act of forgery, and the moral element, which is manifested in the criminal intent motivating the perpetrator to commit the offense.(Duraye, M. 2023).&(Al-Suhaili, M. 2023).

- Electronic Fraud: this involves the use of deceptive methods to obtain sensitive information, such as credit card details or personal data. One of the most prominent forms of electronic fraud is:

- Email Fraud (Phishing): This occurs when fraudulent emails are sent that appear legitimate, with the intent of deceiving individuals into disclosing their sensitive information.(Duraye, M. 2023).
- Cyber Espionage: This type of threat refers to the illegal acquisition of information about individuals or companies, either through hacking electronic systems or using spyware specifically designed for this purpose..(Duraye, M. 2023).

- Data-Related Risks: This category pertains to the loss or leakage of sensitive data, whether due to cyber breaches or human errors. These risks are reflected in the loss of customer trust, as well as the significant legal costs associated with addressing the resulting damages.(Duraye, M. 2023).
- Legal Risks: These risks encompass the challenges faced by companies in managing electronic data, particularly regarding non-compliance with national and international data protection laws, such as personal data protection regulations (GDPR).(Ismail, N. 2021).
- Infrastructure-Related Risks: These risks refer to cyberattacks targeting critical infrastructure, such as electricity networks, transportation systems, or water systems, leading to the disruption of essential services.(Duraye, M. 2023).

In addition to the aforementioned risks, we can also mention fist-party and third-party risks, namely those related to losses incurred by companies or other parties interacting with individuals from the digital community, reputational risks; that arise as a result of cybercrimes or data breaches, potentially damaging the reputation of the affected company, and intellectual property infringement risks that involve the unauthorized access to systems or the theft of digital content, which can lead to violations of intellectual property rights. Furthermore, cyber extortion risks are also common and involve threats directed at companies or individuals, where sensitive information may be exposed, or cyber damage inflicted unless financial demands are met. Similarly, data theft or loss risks occur due to system intrusions or human errors, resulting in unauthorized access or the disappearance of critical information. Additionally, business interruption and cyber system downtime are also risks that should be noted. These risks can cause severe financial losses by disrupting essential operations. Finally, fines and regulatory compliance risks stem from non-compliance with data protection laws, leading to significant financial and legal repercussions.

2.2 Insurance

Insurance is a tool for managing risks that provides financial protection against potential losses or damages. It involves an agreement between an insured (the

policyholder) and an insurance company (the insurer), where the policyholder pays a premium in exchange for the insurer's promise to cover specific losses or accidents.

The primary objective of insurance is to facilitate the transfer of financial loss risk from individuals or organizations to the insurance company. This mechanism enables policyholders to safeguard themselves against unforeseen and potentially catastrophic events, such as accidents, illnesses, natural disasters, or other emergencies. In exchange for this protection, the insurance company aggregates the risks associated with numerous policyholders and utilizes the pooled premiums to disburse claims when covered events arise. (Inyang, Uduakobong, James Onyiyechi Orji, Vincent Chukwuka Okparaka, and Daniel Chukwudi Okeke. 2023).

In Egypt, insurance is regulated by the Insurance Supervision and Control Law No. 10 of 1981 and its amendments, which establishes the general principles for conducting insurance activities, whether life insurance or general insurance, such as property and liability coverage. Insurance companies are controlled by the Financial Regulatory Authority to ensure financial stability and fulfill their obligations to policyholders. The types of insurance available in Egypt are diverse, including personal insurance, property insurance, health insurance, compulsory insurance, and liability insurance. One of the emerging forms of insurance is coverage against cyber risks, which addresses financial damages resulting from cyberattacks and breaches. With the rise of cyber threats, cyber risk insurance has become an integral part of modern insurance in Egypt, as companies are required to cover damages caused by cyberattacks, data breaches, and disruptions to digital systems.

Similarly, the insurance system in UAE law closely aligns with that of Egypt, particularly regarding emerging forms of insurance. In both the Egyptian and Emirati systems, insurance serves as a fundamental tool for risk management, safeguarding individuals and institutions from both material and moral damages. With the rapid technological advancements, cyber risk insurance has emerged as a modern solution to tackle electronic attacks, enhancing the effectiveness of insurance systems in protecting the digital economy.

2.2.1 Digital insurance

Digital insurance differs from insurance against digitization risks, cyber risks, or electronic insurance. Digital insurance refers to insurance conducted through modern technological means, and the insurance industry has undergone a significant digital transformation, driven by the emergence of InsurTech.(Barbera, M. 2023).&(Šoša, M., and A. Montes . (2022).& (Susanto, R. 2022). This transformation involves the integration of various digital technologies, such as artificial intelligence, big data analytics, blockchain, and electronic insurance platforms, into the insurance value chain.(Herrmann, F., and R. Masawi. 2022).&(Kapadiya, S., M. Eling, and R. Owens. 2022).

One of the key aspects of digital insurance is the use of artificial intelligence (AI) algorithms and machine learning to enhance various insurance operations, including risk assessment, subscription, fraud detection, claims management, and customer service.(Herrmann, F., and R. Masawi. 2022).&(Kapadiya, S., M. Eling, and R. Owens. 2022).These technologies enable insurance companies to benefit from vast amounts of data, improve decision-making processes, and provide more personalized and efficient services to policyholders.(Mullins, P., and A. Kagwanj. 2021).&(E Eling, M., Schnell, W., and Sommerrock, F. 2016).

Another key advancement in digital insurance is the use of e-insurance platforms and online insurance services. These tools enable policyholders to buy, manage, and engage with their insurance policies via digital channels. (Susanto, R. 2022). This shift has enhanced convenience, accessibility, and transparency for customers while also cutting down administrative expenses for insurance providers. (Susanto, R. 2022).

In general, digital insurance marks a major transformation in the insurance sector, driven by the integration of diverse digital technologies. Although this shift brings many advantages, it also demands thorough attention to potential risks and the introduction of necessary measures to ensure ongoing policyholder confidence and satisfaction.

In the context of the current study, insurance against cyber risks or electronic insurance specifically refers to insurance coverage for cyber risks and digital risks as insurable subjects themselves, rather than as a means of conducting insurance transactions. Therefore, it does not include insurance that is merely conducted through digital platforms. As previously explained, digital insurance in this latter sense applies to

all types of traditional insurance, with the primary distinction being that the insurance contract is concluded electronically. This places it within the realm of electronic contract studies, as discussed in the preceding paragraphs.

2.2.2 Insurance against cyber risks

Insurance against digitalization risks, or electronic insurance against cyber risks can be described as a modern insurance product aimed at assisting companies in reducing potential losses and the severe impacts of cyberattacks and cyber threats. This form of insurance is significant for its varying scope across different insurers, with coverage terms and policy conditions substantially differing. Broadly speaking, insurance against cyber risks or electronic insurance is categorized as a targeted coverage designed to reimburse losses arising from damage or loss of information caused by deficiencies in IT services or networks, along with the general risks associated with digitalization. Insurers are obligated to offer electronic liability coverage to protect policyholders from digitalization risks or electronic hazards.

2.2.3 Risk in the context of Insurance

The risk covered by insurance is a core component of insurance contracts, referring to the accident or situation that could cause a loss or damage to the insured. Risk plays a crucial role in setting insurance premiums, as insurers evaluate the risks incurred by the client or property before determining the insurance value. (Al-Saati, J. 2016) . Risks are categorized into various types, such as insurable risks, which can be identified and quantified, and non-insurable risks, which are unpredictable or difficult to measure precisely.(Kalfin, K., S. Sukono, S. Supian, and M. Mamat. 2022).

For a risk to be an insurable one, or a subject of insurance, certain conditions must be met:

- The probability condition; which requires that there be a realistic chance of the risk occurring, allowing it to be statistically estimated.
-The verification condition; which requires the risk to be limited to a specific time period, making it possible to determine when it might occur.

- The financial loss condition; which requires that the risk's occurrence lead to a financial loss for the insured, justifying compensation.(Nofita, C. 2024).
- The assessability condition; which requires that the potential losses from the risk's realization be measurable.(Khater, S. 2007).

Insurable risks can manifest in multiple ways, including natural risks, like natural disasters (earthquakes, floods); human risks, such as mistakes or theft; economic risks, such as market fluctuations impacting property or investment values; and technical risks, like failures in machinery or equipment.(Orofuke, P. 2023).

2.3 Risk in the context of cyberspace

Digital risks denote the challenges and threats stemming from the growing dependence on digital technology in all sectors, especially in the insurance industry. These risks include a range of threats, such as cyberattacks, data breaches, privacy violations, and unreliable technologies. For instance, while telematics in auto insurance offers precise insights into driver behavior, it also sparks privacy concerns and questions about data usage.(Tsyganov, A. and Брызгалов, Д. 2018).

2.4 Cybersecurity

Cybersecurity is defined as "a set of tools, policies, security principles, safeguards, guidelines, risk management strategies, procedural measures, training protocols, best practices, assurances, and advanced technologies designed to protect the digital environment, organizational assets, and users from potential threats and vulnerabilities." In other words, cybersecurity refers to a collection of strategies, tools, and policies designed to protect information systems, networks, and data from cyber threats and attacks.

Cybersecurity is an essential element for protecting sensitive information, maintaining data integrity, and ensuring confidentiality. It involves securing critical infrastructure, including both public and private networks, as well as personal data, to uphold privacy and prevent misuse.

2.4.1 Essential components of cybersecurity

Cybersecurity encompasses several significant components some important of which are:

- Confidentiality: It refers to protecting information from unauthorized access, ensuring that sensitive data remains protected and is only accessible to authorized individuals.
- Integrity: It refers to protecting data from unauthorized alteration or manipulation, ensuring that the information remains accurate, correct, and unaffected by any unlawful changes.
- Availability: It involves ensuring that information and systems are always available when required, thus ensuring the continuity of operations and the uninterrupted delivery of services, especially during emergencies or cyberattacks.

2.5 Cyber attacks

An "electronic attack" is generally defined as the intentional disruption of the confidentiality, integrity, or availability of an information system. This term encompasses a wide range of actions aimed at unlawfully or unauthorizedly breaching or destroying information systems and electronic networks.

The legal definition of a "Cyber Attack," as outlined in legal studies, refers to any action or attempt to illegally or without authorization penetrate, disrupt, or destroy information systems or electronic networks. This definition includes a range of harmful electronic activities, such as:

– Hacking: Refers to unauthorized attempts to access computer systems or electronic networks with the intent to take control or steal data.(Daraji, A. 2024).
– Malware: Involves the introduction of harmful software, such as viruses, worms, and trojans, into electronic systems with the goal of disrupting or exploiting them.(Al-Karim, A. 2022).

– DDoS Attacks: Aim to overwhelm systems with a large volume of internet traffic, hindering their operational capacity or preventing user access.(Al-Asali, M. 2024).

- Cyber Espionage: Involves the unauthorized collection of confidential or sensitive information by infiltrating electronic systems.(Joshua, A. 2022).

– Cyber Terrorism: Refers to the use of electronic technology to carry out terrorist acts that target critical infrastructure or aim to instill fear and panic among individuals.(Rahayu, M., Sahiruddin, S., Risdianto, F., Rusdiah, R., Rabiah, S., and Taufiqurrochman, R. 2023).

In conclusion, cyber attacks pose a fundamental threat to digital infrastructure and sensitive data, necessitating a precise and comprehensive legal approach to ensure the protection of systems and information. This should include a flexible legal liability framework that encourages the enhancement of cybersecurity without compromising technological innovation efforts.

2.6 Legal framework for protecting information and personal data

Some countries and regional entities, notably the European Union, have enacted strict obligations for companies to ensure the protection of information and personal data. A key piece of legislation in this context is the General Data Protection Regulation (GDPR) No. 679/2016, which was adopted by the European Parliament and the Council of Europe on April 27, 2016. This regulation is designed to protect individuals concerning the processing of personal data while facilitating its free movement(Regulation (EU) 2016/679(2016)). Moreover, national data protection legislations have established obligations to uphold information security and personal data protection. This is exemplified by the UAE Personal Data Protection Law, issued under Federal Decree No. 45 of 2021, as well as the Egyptian Law No. 151 of 2020. The following sections will elaborate on the specific provisions of these obligations.

2.6.1 Obligations for personal data protection under section two of the GDPR

The General Data Protection Regulation (GDPR) serves as a comprehensive legal framework aimed at enhancing data security and protecting individuals' rights, while providing sufficient flexibility for companies in managing their data. This framework imposes clear obligations related to technical and organizational security to ensure that personal data is processed in a secure and responsible manner. This, in turn, contributes to reducing cybersecurity risks and fostering trust in the digital environment. Among these obligations are:

- Adherance to norms of personal data processing: The EU regulation mandates that both the controller (EU 2016/679, controller) and the processor (EU 2016/679, processor) adhere to a set of technical and organizational measures that consider the latest technological developments, implementation costs, the nature, scope, context, and purposes of data processing, as well as the potential risks associated with personal data processing and their impact on individuals' rights. These measures include(Regulation (EU) 2016/679(2016):
- The use of pseudonymization (EU 2016/679, Pseudonymisation) and the encryption of personal data. Additionally, there is a requirement to ensure ongoing confidentiality, integrity, and resilience of processing systems and services.
- The ability to restore personal data and access it promptly in the event of a technical or physical incident.
- Conducting regular tests and assessments of the effectiveness of technical and organizational measures to ensure the security of processing.
- Assessing the appropriate level of security, and when determining the required security level, the following risks must be considered: accidental or unlawful destruction of data, loss, alteration, or unauthorized disclosure of data, as well as unauthorized access to data that is transmitted, stored, or processed in any other form.
- Control of access to personal data: The controller and processor must implement measures to ensure that individuals who have access to personal data process it only in accordance with specific instructions from the controller, unless national law or Union law requires otherwise.

Compliance to these norms can be demonstrated through codes of conduct and certification mechanisms. Companies can prove their adherence to cybersecurity requirements by using an approved code of conduct in accordance with Article 40 of the regulation, and by obtaining an accredited certification mechanism as outlined in Article 42 of the regulation.

2.6.2 Obligations for personal data protection in Egyptian and UAE law

In both the Egyptian and UAE data protection laws, similar obligations are imposed on data processors and controllers(Articles 5 and 8 of the UAE Personal Data Protection Law and Articles 4 and 8 of the Egyptian Personal Data Protection Law). Some important of which are:

- Obligating controllers and processors to protect personal data: The controller and processor are required to take all necessary precautions to protect personal data from loss, damage, alteration, disclosure, and unlawful use. These measures must be proportionate to the nature and significance of the data that needs to be protected.
- Reporting Security Breaches: The processor must notify the controller of any breach of security measures or any risk that may affect the security of personal data. Additionally, the controller is obligated to inform the affected individual and the relevant authority if the breach is likely to cause significant harm to the personal data or the privacy of the individual.
- Transparency and accountability in case of significant harm: If personal data suffers significant harm due to a breach of preventive measures, the controller must notify the affected individuals and the relevant authorities. This notification is essential to take necessary actions to mitigate negative impacts.
- Prohibition of actions restricting cross-border data flow

The controller is prohibited from taking any actions that restrict the flow of personal data across borders, unless the processing of the data violates local laws or results in significant harm to the data or the privacy of individuals.

2.7 Insurance coverage for damages resulting from cyberattacks

Cyber insurance is considered one of the modern solutions to address the increasing risks posed by cyberattacks. Historically, the first online insurance policy emerged in the spring of 1997, co-authored by Stephen House. Initially, this policy targeted information technology companies responsible for managing the networks and systems used by organizations and consumers.

In light of the advancement of technology and the increase in cyber threats, insurance companies began, in the mid-2000s, to offer written coverages that included first-party expenses. Subsequently, these coverages expanded to encompass any company that relies on technology in its operations. Additionally, cyber insurance evolved to include written coverage for third-party liabilities, ensuring that businesses are protected from the legal and financial responsibilities arising from cyberattacks(The Federal Reserve Bank of Chicago, Essays on Issues). Furthermore, risks known as "silent internet risks" have manifested, representing a third type of coverage related to electronic damages. Although these risks are not part of a standalone cyber insurance policy, they refer to potential electronic losses that may arise from traditional assets not specifically designed to cover cyber risks(Baker, T. 2019). Thus, cyber insurance coverage has become an urgent necessity for companies and organizations, given the increasing reliance on technology and the rising cyber threats.

2.8 Growth of cyber attacks

During the period from 2005 to 2010, there was a gradual rise in the number of cyber attacks coinciding with the expansion of internet and digital technology usage. From 2011 to 2015, attacks significantly increased with the emergence of new technologies and organizations' reliance on cloud services. Between 2016 and 2020, cyber attacks doubled, with 2,244 attacks recorded daily in 2020. In the period from 2021 to 2024, this escalation continued sharply, with 1.7 million ransomware attacks occurring daily in 2023. The following charts illustrate the evolution of cyber incidents and the financial losses resulting from them, as well as the development of ransomware attacks during the period from 2005 to 2024.

Figure 1

Growth of Cyber Incidents (2005-2024)

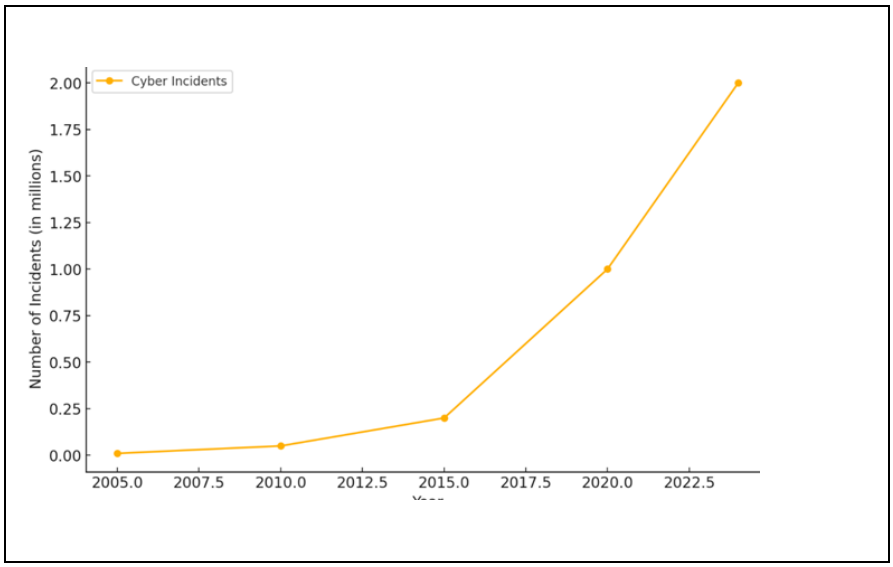


Figure 2

Growth of Financial Losses from Cyber Incidents (2005-2024)

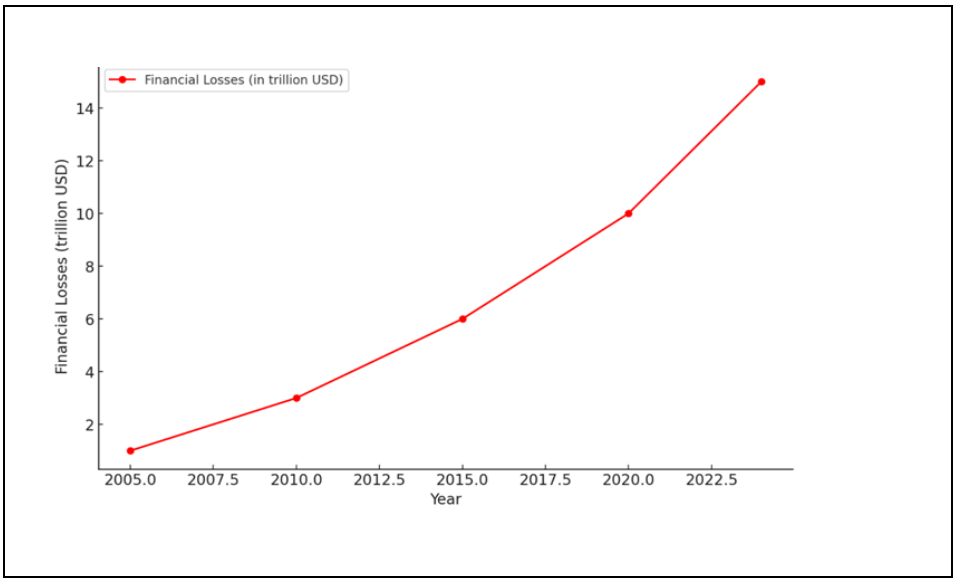
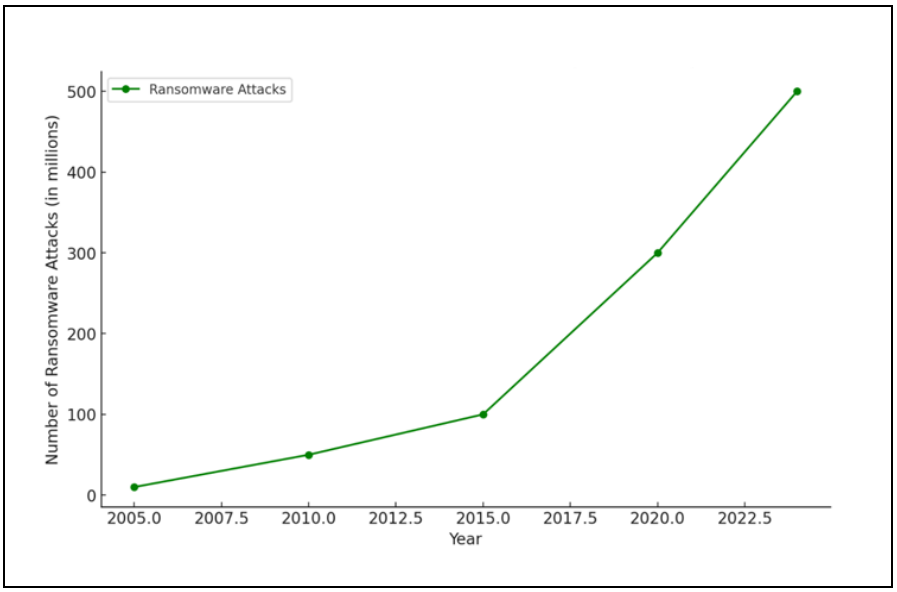


Figure 3

Growth of Ransomeware Attack (2005-2024)



2.9 Efforts to combat cyber incidents

Extensive efforts have been made to combat cyber incidents. In Saoudi Arabia, there has been an increase in spending on cybersecurity, the cybersecurity market reached 13.3 billion riyals in 2023, which reflects the total spending by both the public and private sectors on security solutions and services. Additionally, there has been the development of legislation and policies, with many countries enacting new laws and guidelines aimed at enhancing cybersecurity and protecting data. Furthermore, awareness and training programs have been implemented to raise awareness about cyber risks and how to address them.

Future predictions for electronic and cyber attacks demonstrate an increase in complex attacks, with expectations that these sophisticated threats using advanced technologies like artificial intelligence will continue to rise. Cyber defense tools are also set to evolve, as organizations will keep developing innovative solutions and techniques to address emerging threats. Furthermore, international cooperation is anticipated to strengthen in order to tackle cross-border cyber threats more effectively.

2.10 E-insurance policies

Cyber insurance policies include certain exceptions and limitations, along with additional clauses aimed at protecting insurers from high risks. Some of these exceptions include issues related to cloud service providers, unencrypted devices containing personal data, and software failures resulting from coding errors. These policies also provide coverage for business interruption compensation, which encompasses losses incurred by the insured during the recovery and waiting periods. Furthermore, they include compensation for internet threats, where the insurance company covers expenses related to ransom response, including financial payments and costs associated with emergency experts(Palsson, K., S. Gudmundsson, and S. Shetty . 2020). In terms of coverages, most cyber policies include the following core coverages:

- Data breach expenses: which cover essential response costs, such as hiring lawyers and notifying customers whose information has been compromised.
- Privacy costs and network security liability: which include defending against class action lawsuits and settling third-party claims.
- Regulatory claims: which cover legal fees for responding to government investigations, as well as civil fines and penalties.
- Network interruption: which includes coverage for lost profits and additional expenses resulting from network shutdowns.
- Optional coverages: where cybersecurity insurance companies offer a range of optional coverages that address specific risks, such as ransomware attacks, data recovery, and payment card liability.

Indeed, the scope of coverage varies significantly between different policies. The elements included in the document are determined based on the wording of the insurance contract at the time of its conclusion. These documents clarify the losses that can be submitted to the insurance company in the event of cybersecurity risks, helping to ensure effective protection for businesses against cyber threats.

2.10.1 Cyber coverage exceptions

Despite the broad coverages mentioned earlier, some electronic policies contain exclusions and limitations that include the following(Palsson, K., S. Gudmundsson, and S. Shetty . 2020):

- Exception related to infrastructure: Coverage excludes failures related to power, utilities, or telecommunications (including the internet) and services beyond the control of the insured.
- Exceptions related to voluntary closure coverage: Coverage may apply only to voluntary closures aimed at mitigating the spread of malware or minimizing damage, and does not extend to enhancements in network performance.
- Exceptions related to the computer operating systems or networks: Policyholders must review operating systems to ensure coverage for systems that are owned, operated, leased, or managed by third parties.

Exceptions related to system failure: Certain policies require the presence of a "human" or software "error" along with a proof of testing or corrections to activate coverage(Palsson, K., S. Gudmundsson, and S. Shetty . 2020).

2.10.2 Legal challenges of cyber coverage policies

There is a clear relationship between electronic insurance and cybersecurity, with electronic insurance closely linked to cybersecurity. Writing cyber coverage policies and defining the controls governing them necessitates coordination at international, regional, and national levels. This requires collaboration between insurance companies and relevant government entities to achieve suitable solutions for insurance documents against cyber risks, as well as with institutions focused on cybersecurity. As for the challenges in drafting cyber insurance policies, they are diverse and include the following:

- Determining pricing and premiums for e-insurance: Insurance companies face significant challenges in pricing e-insurance policies compared to traditional insurance policies (such as auto insurance), which rely on a long history of data and statistics. In a rapidly evolving market like cyber insurance, companies

depend on market estimates, expert surveys, and attempts to deduce the expected costs of cyber attacks. This approach often lacks precision and sufficient expertise. Currently, coverage is limited to three main models: First-Party Coverage; Third-Party Coverage; and Implicit (Silent) Coverage(Talesh, S. A. 2017).

- Evaluation of cyber risks: With the continuous development of hackers' capabilities, it is difficult for insurance companies to accurately assess cyber risks. For instance, the average cost of a cyber attack rose by 29% from $21.2 million in 2017 to $27.4 million in 2018. By 2024, the cost of cyber attacks is estimated to reach $14.5 trillion, with prediction of rising to $17.6 trillion by 2025.
- The evolving nature of cyber attacks: Cyber attacks are characterized by continuous evolution, enabling them to affect thousands of companies simultaneously, resulting in significant interconnected losses for insurance companies. As a result, insurers may be compelled to pay substantial compensations to all policyholders at the same time.
-The ongoing failure of cyber attacks: Cyber attacks targeting specific components of infrastructure, such as service providers, can result in the systemic disruption of the entire network. A pertinent example of this phenomenon is the dissemination of self-replicating malware across interconnected device networks, which can lead to extensive and far-reaching damage.
- Legal uncertainty : The cyber insurance market is characterized by a state of "ambiguity" due to a lack of accurate and up-to-date data. This uncertainty compels insurance companies to raise premiums in anticipation of unforeseen risks, thereby making it difficult for clients to access affordable insurance policies. Additionally, limited competition among insurers further hinders the development of effective and cost-efficient solutions.

3 THE FUTURE OF INSURANCE AGAINST DIGITAL RISKS AND E-INSURANCE

Every reported incident of data breach or system failure inevitably results in financial losses or damage to the commercial reputation of companies. Given that traditional insurance contracts currently do not encompass coverage for cyber risks, there

is an urgent need to adopt electronic insurance contracts. The novelty, complexity, and dynamic nature of cyber risks pose a legal threat to insurance agents, as these experienced agents will understand that accurately predicting coverage for cyber risk insurance contracts is inherently challenging. This uncertainty may discourage agents or brokers from offering these new products. Consequently, only a limited number of specialists may be willing and able to sell electronic insurance products. This lack of expertise does not represent a direct legal constraint; however, it creates legal uncertainty for clients regarding what constitutes an insurable cyber risk and what does not, which will in turn affect the development of the market.(Biener, C., M. Eling, and J. H. Wirfs. 2021).

At present, the cyber insurance market provides coverage only for a small proportion of the total losses incurred as a result of cyber attacks, making it challenging to measure the full economic impact of such incidents on national economies (The Council of Economic Advisers, February 2018).

In order to mitigate the damages resulting from cybersecurity risks, some legal scholars and experts in cybersecurity and electronic insurance have discussed the feasibility of imposing mandatory electronic insurance on companies, viewing it as an obligation necessary for the protection of privacy and the safeguarding of client and user data and information. On the other hand, another trend posits that it may not be appropriate to mandate electronic insurance for small and medium-sized enterprises, as such requirements may not align with their operational capacities. Furthermore, e-insurance generally encompasses coverage for damages incurred by both the insured party and third parties; thus, cyber insurance is not solely a means of liability coverage. Consequently, the imposition of mandatory electronic insurance cannot be justified in all circumstances. Therefore, a consensus among most experts and legal scholars advocates for the establishment of mandatory electronic insurance specifically for certain companies and industries that are particularly vulnerable to cyber attack risks, including insurance companies, law firms and banks.

Mandatory e-insurance can be predicated on two types of electronic liability:

- First: The system of liability based on fault, wherein the insurer compensates for the damages incurred by the insured party in accordance with the degree of fault. This applies to both contractual fault (contractual liability) and tort liability, which is established either on the basis of fault that must be proven in relation to personal

acts or on presumed fault concerning the acts of others. According to some experts, mandatory insurance based on fault would enable compensation for the aggrieved party in most instances, except in cases where the insured company itself has committed a fault.

- Second: The system of strict liability, also known as no-fault liability, whereby the insurer compensates the insured party, often up to a specified amount, regardless of whether the latter has committed a fault. Experts argue that no-fault insurance may lead companies to become less motivated to enhance their cybersecurity measures, potentially affecting efforts to mitigate the risks of cyber attacks.(de Werra, Jacques, and Yanic Benhamou. 2020).

4 CONCLUSION

before outlining the key findings and recommendations of the study, it is essential to emphasize the importance of collaboration between the insurance industry and other stakeholders to enhance awareness of cybersecurity risks and educate clients on how to address them. Insurance companies should adopt effective risk management policies, providing clients with tools and procedures that contribute to the protection of data from electronic threats. Additionally, insurance companies need to acquire the necessary technical knowledge in information technology security and leverage the expertise of specialized firms to ensure a deeper understanding of cybersecurity risks and to offer effective insurance solutions.

5 RESULTS

The study concluded that traditional legal frameworks are insufficient for comprehensively regulating insurance against digitalization risks due to several reasons, the most significant of which is the lack of precise definitions of digitalization risks. Additionally, the rapid and complex evolution of digital life makes it difficult for legal regulations to adequately comprehend and manage these challenges. The study also indicated that insurance against digitalization risks, or e- insurance, has the potential to enhance the economic and digital security of countries, institutions, and individuals,

provided that its governing provisions are aligned with the nature of these relationships. One of the key findings of this study is that insurance companies possess the adequate capacity to provide sufficient protection for individuals and businesses against digitalization risks, such as cybersecurity threats and electronic attacks, when they offer coverage models that align with the coexistence and nature of the digital community and its risks. This, in fact, contributes to enhancing the economic and digital security of nations and achieves legal certainty for participants in the digital insurance sector in general, and specifically for insurance against digitalization risks. Insurance against digitalization risks, or electronic insurance, along with cybersecurity, occupies a prominent position among the interests of the financial sector, commercial enterprises, and governments. And in light of the dominance of digital life globally, coupled with the COVID-19 pandemic, has led to a significant increase in cyber attacks, which in turn has contributed to the growing demand for electronic insurance against cybersecurity risks. Nevertheless, these companies play a vital role in providing reliable solutions to address these threats. However, the study also demonstrated that the cybersecurity insurance market remains immature, as the coverage options and policies available vary significantly among insurance companies. Cumulative risks represent one of the biggest challenges in the field of cybersecurity insurance, as a single electronic event can impact multiple companies simultaneously, leading to substantial losses that insurance companies may struggle to bear alone. Building a business reputation takes years of effort, while a single cyber attack can destroy it in minutes. Therefore, there is a pressing need to reassess electronic risks as insurance companies still incapable to cover large-scale electronic incidents affecting a significant number of clients. It is important to emphasize that the current coverage is limited to a narrow scope of losses, such as data breaches and network disruptions. Additionally, governments lack the capacity to bear unlimited liabilities in the event of large-scale attacks that threaten the national economy.

5.1 Recommendations

Based on the aforementioned findings, this study recommends the following:

- Organizing the legal framework for insurance contracts against digital risks or e-insurance in national legislations is essential to ensure adequate protection and liability management for all stakeholders involved.
- Ensuring legal protection for companies, clients, and users in the e-business sector through appropriate legal, technical, and technological means.
- Enhancing international cooperation through global agreements aimed at curbing cyber attacks, developing electronic databases, and adopting standards to reduce digital risks.
- Encouraging governments to establish a regulated cybersecurity insurance market is vital for facilitating the transition to a digital economy and raising awareness about cyber risks.
- Supporting national insurance companies and encouraging the issuance of e-insurance policies against digital risks through effective public-private sectors.
- Enhancing the exchange of knowledge and expertise among insurance companies at the international level.
- Organizing and issuing a standardized e-insurance policy against digital risks, with the participation of experts and specialists in the field of insurance.
- Involving the academic community in the global dialogue on preventing digital risks, including cyber threats, and promoting electronic insurance is crucial. Their insights and solutions can contribute significantly to addressing these challenges.

ACKNOWLEDGEMENT

The author declare no conflict of interest and no personal circumstances or interest may be perceived as inappropriately influencing the representation or interpretation of the reported research results. And The author conducted this research independently and is solely responsible for all aspects of its content. No external funding or assistance was provided by other individuals, organizations, or institutions.

REFERENCES

Al-Asali, M. "Denial of Service Attacks and Their Legal Implications." Digital Security Journal 7, no. 3 (2024): 78-90.

Al-Fraihat, M. "Cybersecurity Challenges in the Arab World: An Analysis of the Current Reality." Arab Cybersecurity Journal 5, no. 2 (2023): 45-62.

Al-Karim, A. "Malware: Risks and Legal Measures." Journal of Information Technology and Security 12, no. 5 (2022): 65-84.

Alkire, L., G. O'Connor, and F. Wynstra. "Understanding Millennials' Data Privacy Behaviors." Journal of Business Research 105 (2019): 123-135. https://doi.org/10.1016/j.jbusres.2019.05.019.

Al-Rubaie, A. "Definition of Cyber Risks and Their Dimensions." Journal of Legal Studies 11, no. 2 (2024): 123-145.

Al-Saati, J. "The Risk in the Insurance Contract: An Analytical Study." Civil Law Journal 4, no. 2 (2016): 45-70.

Al-Suhaili, M. "Analysis of Cyberattacks and Their Impact on the Private Sector." Arab Cybersecurity Journal 10, no. 1 (2023): 34-50.

Al-Zyoud, M. "Legal Challenges of Cyber Risks in the Arab World." Digital Law Journal 8, no. 4 (2020): 89-102.

Articles 5 and 8 of the UAE Personal Data Protection Law and Articles 4 and 8 of the Egyptian Personal Data Protection Law.

Baker, T. "Back to the Future of Cyber Insurance." Faculty Scholarship at Penn Law, no. 2184 (2019). Retrieved March 14, 2021, from https://scholarship.law.upenn.edu/faculty_scholarship/2184.

Barbera, M. "The Future of Cyber Insurance: Challenges and Solutions." Journal of Financial Technology 20, no. 1 (2023): 89-110. https://doi.org/10.1234/jft.2023.00110.

Bartol, K. "Privacy Challenges in the Digital Era: A Global Perspective." Cybersecurity Journal 12, no. 3 (2023): 45-58. https://doi.org/10.1234/csj.2023.12003.

Bermanns, J. "Toward a Unified Cybersecurity Framework in the European Union." European Journal of Information Systems 18, no. 4 (2023): 231-246. https://doi.org/10.1080/0960085X.2023.1200184.

Biener, C., M. Eling, and J. H. Wirfs. "Insurability of Cyber Risk: An Empirical Analysis." Geneva Papers on Risk and Insurance - Issues and Practice. https://doi.org/10.1057/gpp.2014.19. Retrieved March 14, 2021, from https://www.researchgate.net/publication/2657727415_insurability_of_Cyber_Risk_An-Empirical_Analysis.

Cheng, L., F. Liu, and D. Yao. "Cybersecurity During Global Crises: Lessons from COVID-19." Computers & Security 96 (2020): 101923. https://doi.org/10.1016/j.cose.2020.101923.

Corbett, M. "Ransomware, COVID-19 and Cyber Insurance: The Big Disconnect." Gen Re Blog. Published March 14, 2021. https://www.genre.com/knowledge/blog/ransomware-covid-19-and-cbyer-insurance-the-big-disconnect-en-html.

Daraji, A. "Cyber Damages and Civil Responsibility: A Legal Study." Journal of Digital Law 16, no. 2 (2024): 45-62. https://doi.org/10.1234/jdl.2024.01602.

de Werra, Jacques, and Yanic Benhamou. "Cyberassurance: Instrument Utile Pour la Cybersécurité des Entreprises?" Jusletter, August 24, 2020. ISSN 1424-7410.

Deep, A., N. Sharma, and P. Verma. "National Security Risks in Critical Infrastructure: Cybersecurity Implications." Defence Technology Review 14, no. 2 (2020): 203-220. https://doi.org/10.1234/dtr.2020.140203

Duraye, M. "Cybersecurity Capacity Building in Arab Countries: Challenges and Prospects." Arab Journal of Information Security 5, no. 2 (2023): 87-102. https://doi.org/10.1234/ajis.2023.05002.

Eling, M., Schnell, W., and Sommerrock, F. 2016. Ten Key Questions on Cyber Risk and Cyber Risk Insurance. The Geneva Association.

Elrawy, M., A. Abdelhamid, and A. Sallam. "Internet of Things Security: Challenges and Solutions." Future Generation Computer Systems 82 (2018): 67-82. https://doi.org/10.1016/j.future.2017.12.022.

Hadwin, S., and J. Monck-Mason. "Cyber Insurance: An Overview." Practical Law, 2020.

Herrmann, F., and R. Masawi. "Digital Transformation in Insurance: Challenges and Opportunities." Journal of Digital Innovation 17, no. 3 (2022): 144-167. https://doi.org/10.1234/jdi.2022.01703 .

Inyang, Uduakobong, James Onyiyechi Orji, Vincent Chukwuka Okparaka, and Daniel Chukwudi Okeke. “Perceptive Influence of Purchasing Motor Vehicle Insurance Policy from Non-Regulated Firms on the Performance of Insurance Industry in Nigeria: A Customer-Based Sentiment Analysis.” International Journal of Current Science Research and Review 06, no. 09 (September 27, 2023). https://doi.org/10.47191/ijcsrr/v6-i9-39.

Ismail, N. "Data Protection Laws: A Comparative Study Between Egypt and UAE." International Journal of Law and Technology 19, no. 2 (2021): 54-73. https://doi.org/10.5678/ijlt.2021.12002.

Joshua, A. "An Assessment of International Law on the Use of Cyber-Espionage as a Substitute for Traditional Spying." European Journal of Law and Political Science 1, no. 4 (2022): 1-8. https://doi.org/10.24018/ejpolitics.2022.1.4.21.

Kalfin, K., S. Sukono, S. Supian, and M. Mamat. "Insurance as an Alternative for Sustainable Economic Recovery after Natural Disasters: A Systematic Literature Review." Sustainability 14, no. 7 (2022): 4349. https://doi.org/10.3390/su14074349.

Kapadiya, S., M. Eling, and R. Owens. "AI in Insurance: Trends and Challenges." Insurance Technology Review 18, no. 1 (2022): 56-73. https://doi.org/10.5678/itr.2022.01801.

Khater, S. "Insurance in the Digital Environment: Risks and Responsibilities." Journal of Insurance and Law 5, no. 1 (2007): 98-115.

Krishna, A., R. Nayak, and M. Poojary. "Digital Resilience in the Face of Pandemics." Journal of Digital Transformation 9, no. 3 (2021): 142-157. https://doi.org/10.1234/jdt.2021.09003.

Kuzior, A. "Cybersecurity Skills Shortage in Europe: Causes and Solutions." European Journal of Information Management 15, no. 1 (2023): 34-48. https://doi.org/10.1234/ejim.2023.15001.

Lutz, C., C. P. Hoffmann, and G. Ranzini. "Privacy Paradox 2.0: Revisiting Privacy Behavior." Telematics and Informatics 49 (2020): 101375. https://doi.org/10.1016/j.tele.2020.101375.

Mullins, P., and A. Kagwanj. "Artificial Intelligence in Insurance: A Forward-Looking Study." Journal of Tech Development 9, no. 3 (2021): 122-139. https://doi.org/10.5678/jtd.2021.09003.

Nofita, C. "The Effect of Market Value Ratio and Activity Ratio on Financial Distress in Technology Sector Companies Listed on the IDX 2021–2023." Ekombis Review Jurnal Ilmiah Ekonomi Dan Bisnis 12, no. 2 (2024). https://doi.org/10.37676/ekombis.v12i2.5382.

Orofuke, P. "Investigating the Causal Relationship between Insurance and Economic Growth in Nigeria." International Journal of Management Studies and Social Science Research 5, no. 5 (2023): 230-247. https://doi.org/10.56293/ijmsssr.2022.4720.

Palsson, K., S. Gudmundsson, and S. Shetty. Analysis of the Impact of Cyber Events for Cyber Insurance. The Geneva Association, 2020. https://doi.org/10.1234/geneva.2020.12004.

Rahayu, M., Sahiruddin, S., Risdianto, F., Rusdiah, R., Rabiah, S., and Taufiqurrochman, R. 2023. "“The Sum of All Fears” from Novel to Film: Shifting the Discourse of Terrorism." World Journal of English Language 13 (7): 186. https://doi.org/10.5430/wjel.v13n7p186.

REGULATION (EU) 2016/679

Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

Salvaggio, L., and M. González. "Enhancing International Cooperation for Cybersecurity." Global Policy Journal 13, no. 2 (2022): 215-230. https://doi.org/10.1111/1758-5899.13022.

Sithole, P., K. Mabunda, and T. Dube. "The Evolving Complexity of Cyberattacks: AI-Driven Threats." Global Cybersecurity Outlook 22, no. 1 (2023): 33-49. https://doi.org/10.1234/gco.2023.22001.

Šoša, M., and A. Montes. "Blockchain Applications in Insurance: Case Studies." Journal of Distributed Technologies 14, no. 4 (2022): 121-138. https://doi.org/10.1234/jdt.2022.01404.

Susanto, R. "InsurTech: Disruption and Opportunities." Journal of Financial Technology 20, no. 2 (2022): 110-129. https://doi.org/10.5678/jft.2022.02002.

Talesh, S. A. "Insurance Companies as Corporate Regulators: The Good, the Bad, and the Ugly." DePaul Law Review 66 (2017): 463.

The Federal Reserve Bank of Chicago, Essays on Issues.

Torre, L., R. Smith, and P. Gomez. "Enterprise-Wide Strategies for Mitigating Cyber Risks." Journal of Cyber Risk Management 17, no. 3 (2023): 78-95. https://doi.org/10.1234/jcrm.2023.17003.

Tsyganov, A. and Брызгалов, Д. (2018). Digitalization of the insurance market: tasks, problems and prospects. Economics Taxes & Law, 11(2), 111-120. https://doi.org/10.26794/1999-849x-2018-11-2-111-120.

Waheed, A. "Machine Learning for Enhanced Cybersecurity: Challenges and Solutions." Journal of Advanced Computing 14, no. 2 (2020): 215-230. https://doi.org/10.1234/jac.2020.14002.

Wanjugu, C., Mutiso, J., and N. Kariuki. "Digital Privacy Breaches and Public Trust." Journal of Digital Ethics 8, no. 1 (2022): 15-29. https://doi.org/10.1234/jde.2022.08001.

Yahuza, M., B. Usman, and T. Adewale. "Cyber Threats to National Infrastructure." Journal of Cybersecurity Studies 9, no. 4 (2021): 123-137. https://doi.org/10.1234/jcss.2021.09004.

Authors' Contribution

All authors contributed equally to the development of this article.

Data availability

All datasets relevant to this study's findings are fully available within the article.

How to cite this article (APA)

Mahdy, E. M. (2026). INSURANCE AGAINST CYBER RISKS: COMPARATIVE STUDY. *Veredas Do Direito*, 23(3), e234297. https://doi.org/10.18623/rvd.v23.n3.4297