Pakistan Journal of Criminology
Vol. 16, No. 02, April—June 2024 (585-600)

Legal Regulation of Insurance against Cyber-Attack Risks

Sanaa Freihat[1] & Majd Al-Manasra[2]

Abstract

The Internet has recently witnessed significant growth to become an important part of our daily lives, as it has grown to become the main part of our business as well. Nowadays, anything we do on smart devices can be seen by others, either with our knowledge or consent or without, it may seem obvious, as we can share our work on social networking sites. At first glance, however, it appears to represent a serious threat, including privacy breaches and data theft, and threats become even more important when these breaches directly affect businesses, customers, and the general public. It became necessary to protect the requirements of this development from those cyber risks to minimize the negative effects that these attacks and intrusions can have on facilities and infrastructure. The world has witnessed a technical development in the use of Internet devices and electronic networks, and this use has exposed these networks and devices to the risks of cyberattacks, data breaches, obtaining personal, financial, and commercial information, and using them to blackmail companies and individuals electronically.

Keywords: cyber-attacks, cyber risks, cyber insurance, data theft, cyber networks.

Introduction

Due to the surge in cyberattacks on enterprises (e.g., cybercrime, IT failures or outages, data breaches, ransomware occurrences), cyber risks will top the Allianz Risk scale: European, American, Asian, African, and Middle Eastern specialists participate in the yearly poll. It includes the perspectives of risk advisers and specialists from Allianz worldwide Corporate Specialty and other subsidiaries, worldwide company decision makers, mediators, and industry trade associations (Metwally, 2022).

Studies and data show a significant rise in cyberattacks for the first time in 2020 as these organizations are targeted because they collect and use a lot of customers' personal data and data breaches have become larger and more expensive due to the COVID-19 pandemic (Al -Ajmi, 2014).

It was necessary to protect the requirements of this development from those

[1] The Author is a Lecturer at the Faculty of Law at the Applied Science Private University, Al Arab St 21, Amman, Jordan, Amman, Jordan. He can be accessed on Sanaafriehat744@gmail.com
[2] The Author is an Associate Professor at the Faculty of Law at the Applied Science Private University, Al Arab St 21, Amman, Jordan, and the author is a practicing lawyer in Jordan as well. He can be accessed on m_manasra@asu.edu.jo

cyber risks to minimize the negative effects that these attacks and intrusions can have on facilities and infrastructure. The world has witnessed a technical development in the use of Internet devices and electronic networks (Deeb Mahmoud, 2009).

This use has put these networks and devices in danger of cyberattacks, data breaches, collecting personal, financial, and commercial information to blackmail corporations and individuals, and hacking electronic payment systems. Cyber dangers and risks associated with company data and information technology include credit and debit cards. As people rely more on electronic communications and online shopping, the public is exposed to these risks (Al -Baraisa, 2021).

The maintenance of privacy, data protection, and information security policies provide important issues for businesses today, and in response to these risks, insurance companies have stepped in and launched cyber insurance, often known as cyber insurance, a relatively new product, as it is an answer to business demands to protect and reduce them (Dahiya, 2020).

The Arab countries have developed an agreement among themselves known as the Arab Convention on Combating Cybercrime (Technical and Electronic) of 2012, which aims to enhance Arab cooperation in protecting information technology from attack.

This study examines the extent to which cyber insurance can protect companies and economies of institutions and companies within the legal framework against the risks of cyberattacks in Jordanian legislation, as well as the positive and negative effects of institutional factors for insurance companies on the one hand.

On the other hand, security and the privacy and data protection practices of commercial companies may have the ability of the market to develop legally. The problem with the study is that there is an urgent need for the existence of legal controls governing the process of insurance against cyber risks through the existence of controls to determine the material value of losses, and this affects the ability to determine the appropriate price for insurance and determine the scope of insurance coverage and appropriate experience.

The relationship between cybersecurity and insurance so that cybersecurity depends on the request for continuous improvement of security and protection systems, and this requires continuous costs and efforts. In addition, the relationship between the cybersecurity force and the available insurance costs and structures must be determined, and therefore the problem of the study lies in the statement of the legal regulation of insurance against the risks of cyberattacks following Jordanian legislation.

This study seeks to demonstrate the following factors. This study aims to assess

the efficacy of insurance in mitigating cyber threats. Enumerate the legal obstacles linked to cyber risk insurance. Enumerate the assurances and prerequisites necessary in cyber risk insurance agreements. Enumerate the legal provisions encompassed under domestic and global statutes and regulations about insurance coverage for cyber threats. Create legal suggestions and suggestions aimed at enhancing the legal oversight of cyber risk insurance.

The study of the legal regulation of cyber risk insurance is of vital importance for several reasons:

First, cyber risks are increasing and evolving rapidly, and pose a significant threat to individuals and institutions.

Second, insurance can play an important role in providing financial protection and fair compensation to individuals and institutions that are victims of cyberattacks.

Third, the legal system needs to keep pace with emerging challenges in the field of technology and cybersecurity and develop and update effective legal frameworks to meet these challenges.

Therefore, the subject of the legal framework for insurance against cyber risks is one of the modern and important topics that have a significant impact on practical reality, and we will in this study discuss this topic in-depth and extensively, and we will pay attention to all aspects of the topic, whether theoretical or practical. As a result, the importance of the study lies in addressing the increasing vulnerability of institutions and individuals to cyber-attacks due to the rapid development of technology.

Methodology

The descriptive and analytical approach will be used by collecting data from various sources, including the laws and legal regulations in force in the selected countries. It also revises previous research in this field, where the available literature will be reviewed and analyzed in a manner and analyzed all legal texts related to the organization of the insurance contract in accordance with the general rules contained in the Jordanian Civil Code. It examines their adequacy and conformity to the insurance contract against cyberattacks, in order to identify their contents, implications and objectives. Through this research, we aspire to renew and enhance our understanding of the legal and regulatory challenges facing cyber risk insurance, and to provide a valuable scientific contribution to improving legislation and policies related to this important topic.

Legal regulation of cyber risks

The legal regulation of cyber risks includes a set of legislation that works to protect and regulate digital information and data from cyber threats, so that this

legal regulation aims to hold individuals and institutions responsible for protecting against cyber-attacks and enhancing digital security (Al -Qassab, 2011; Al-Billeh, 2022a).

The legal regulation of cyber risks varies from country to country and is usually regulated through a set of legislations such as data protection and privacy laws that define the rights of users to maintain their privacy and protect their data. Cybersecurity protection laws, which include requirements to secure networks and devices used in digital technology, anti-cybercrime laws, which regulate the mechanism for dealing with cybercrimes, and finally intellectual property protection laws, which aim to prevent digital piracy and infringement of intellectual property rights (Chase et al., 2019; Al-Billeh, 2022b).

What are cyber risks?

The term 'cybersecurity' has gained widespread over the past few years, so the use of this term has expanded significantly as many governments of countries around the world began to use the e-government model to provide services to their populations. This means that each person must be connected to the information space of the Internet through his account through which he deals either with e-government or with other parties depending on the type of transaction (Gee & Ford, 2011; Al-Billeh, 2022c).

Therefore, due to the revolution brought about by scientific and technological developments, which have led to many changes at all levels and in all professions, cybercrime has increased so that the distinctive features of modern technological crimes are that they differ from traditional crimes in that they can be easily committed on electronic devices. In addition to the challenges associated with regulating the Internet and trying to hold it accountable for the content published there, publishing it only takes a few minutes or even seconds, and as a result, the Internet has become a base for operations for hackers. By engaging in these actions, hackers aim to weaken security and in other cases seek to overthrow systems and steal people's assets, both physical and personal (Gordon et al., 2003).

There is no doubt that the rapid progress in technology has pushed the international community to a new stage in which cybersecurity plays a decisive role, both in obtaining its basic components and in maximizing its power. It is vital to consider that the new determinants in terms of their nature, patterns of use and the nature of their actors, as well as the reflection of that power on the capabilities of countries and their external relations, are what created this cyber environment (Al-Billeh, 2023a).

Hence, cyberspace has forced a rethinking of the concept of security, which relates to the degree to which the state can become immune from the risks it is exposed to. It also protects the infrastructure of vital facilities from the illegal use of communication and information technology to try to control devices and steal

information, corrupt or disable it (Al -Baraisa, 2021; Al-Billeh & Abu Issa, 2023a).

Cyber insurance has recently become a critical element of the risk management strategy of businesses due to the steady rise in cybercrime. Bearing in mind that cyberattacks have a significant financial impact on companies, also have an impact on the brand, and inevitably affect the behavior of customers, as cybersecurity in companies aims to protect against damage or loss caused by information technology risks (Al-Billeh, 2023b).

Definition of cyber risks from the point of view of jurisprudence, law, and the judiciary

Cyber risk is meant as threats involving the Internet, and in fact, the term 'cybernetics' seems to have been first used by the American mathematician Norbert Weiner in 1948. In addition, the term 'cyber' is derived from the word ‘cyber’, which means 'cyber' in English (Al -Baraisa, 2021).

Therefore, the word cyber is not a translation of the modern word cyber; it is an Arabization to create a name that refers to networks and computers, the word 'cyber' is added to another well-known word. This phrase (cyber risk) has been translated from its French counterpart, which is frequently used in the insurance industry (Al-Billeh, 2024a).

The word cyber is also derived from the Latin term 'cyber', which means (virtual or virtual), referring to the space that includes computerized Internet networks, communication, and information systems, as well as remote control systems known as 'cyberspace'. It refers to anything related to computers, information technology, and virtual reality. It is also the source of the term cybernetics, which means 'control science' or 'cybernetics'. It also means 'communication science and automatic control systems for both machines and living organisms', as well as 'leadership and direction' (Gumenyuk, 2021).

The term 'cyber' refers to an imagined conflict that takes place in the intangible network space, perfectly simulates reality, and its means of warfare are summarized in digital battles, technical software, virtual soldiers, keyboard bullets, and programmers' clicks, in the form of a virtual environment whose effects extend to aspects of physical life as it is. Operations carried out using digital data streams against or through a computer or its system are referred to as 'bloodless warfare' (Al-Billeh, 2024b).

The term 'cyber risk' has many different definitions, but they all agree that it refers to two things: first, the effects of a data breach without an attack on the information system, or second, the effects of an attack on the information system, i.e. unauthorized access to the information system (Pournader et al., 2019; Al-Billeh & Al-Qheiwi, 2023).

Cyber risk is defined as a series of actions that are regularly performed to combat and resolve cyber risks by tracking, identifying, and assessing them. Effective risk management requires a thorough understanding of these risks and the cooperation of all employees, including those working in risk management as well as those in other departments.

From a jurisprudence point of view, cybercrime is a category of criminal activities that involve the use of electronic tools or devices connected to the Internet. Cybercrime requires specialized control over computer technology and information systems to be committed, investigated, prosecuted, and held accountable (Khashashneh et al., 2023; Al-Billeh & Abu Issa, 2023b).

It also means that any action that harms the capabilities of the computer network and its operation for personal or political gain by taking advantage of a certain flaw that makes it possible for an attacker to influence the system.

On the other hand, cyber risk is defined as any action or inaction that uses a particular information system to harm a legal interest or right subject to criminal penalty, regardless of whether these legal interests or rights represent new information models or were previously covered by legal interest or rights. Regardless of whether the attack took place within the borders of a state or crossed it to a group of states, which results in harm that poses a risk to the safety of people, the environment, and human communities, but will either occur or has already occurred and can be stopped if it does not become worse. It is also any threat that targets state institutions, uses ideology, or uses parts of the powers of one state against another state that poses a threat to the territory, independence, or security, and threats can arise from within and outside the state (Al-Khawajah et al., 2023).

Therefore, it is necessary to learn more about cyber risks and legal requirements set by the Jordanian legislator in the Cybersecurity Law No. 16 of 2019. Cybersecurity is the most effective wall in protecting all information on the network, and its importance increases with the high rate of cyberattacks launched by hackers on websites and information systems, in addition to the entanglement of transactions that take place in cyberspace (Al-Hammouri et al., 2024)

As Jordanian law pays great attention to cybersecurity due to the risks surrounding this sector, legal legislation has been developed in this regard, and a cybersecurity center has been established within the Cybersecurity Law of 2019. It aims to protect Jordan from the threats of cybersecurity incidents and build capabilities that ensure facing threats to information systems and infrastructure (Jacobs, 2016).

As for the technical issues of cybercrime risks in terms of nature, impact, and classification, they have not been addressed by the Jordanian legislator. Thus,

it is difficult to ensure protection from cyber risks as intended or required.

Stealing financial and strategic data from customers and suppliers, destroying data, deleting it, and damaging a company's reputation are just a few of the consequences of a data attack. The consequences of an attack on the information system are manifested through unauthorized access, closure, deletion, or infection with viruses (virus-infested work). or use the information system incorrectly (Al-Ajmi, 2014).

According to the provisions of criminalization and punishment, it is an illegal act that affects an interest or right related to the material and intangible components of cyber means. As a result, the Jordanian legislator has determined that the attack and its failure to protect it constitutes a crime subject to punishment under the provisions of the laws in force (Al -Qassab, 2011).

An important definition of cyber risk is 'any illegal conduct or action that involves accessing, altering or deleting data or information stored on the system, or involving automated processing that leads to illegal data transformation or transfer

Many Jurisprudences have agreed that cyber risk is any illegal behavior in which the computer is used as a criminal tool, or the computer is a tool or subject of illegal activity, or it is any act or omission that would lead to an attack on material or moral assets (Deeb Mahmoud, 2009).

The Jordanian legislator has chosen to use the term cyber risk in legislation related to insurance provisions, using the term harm to automated data processing systems to describe the risk of crime, taking into account both the information system itself and the data it contains. The automated data processing system is the first requirement that must be met to consider the presence or absence of criminal components in crimes committed against this system. Crime focuses on intangible elements (Chase et al., 2019).

Types of cyber risks

One of the global issues threatening the technological world is cyber risks. In addition to being a threat to personal security, it also provides a greater risk to global companies, banks, and important government networks. Therefore, coordinated cyber-attacks carried out by professional companies that employ professional programmers who are constantly developing new methods to carry out their cyberattacks have replaced cyber threats previously led by professional hackers (Dahiya, 2020).

There are now many mechanisms available. Thanks to advances in modern technology that make crimes easier and less dangerous for people. As a result, traditional crimes began to be committed on a large scale using technological

means without any kind of deterrence or punishment, as is the case when dealing with cybercrime. Due to the rise in the number of Internet users and the increasing dependence of people, companies, and countries on it, has led to a significant rise in the rate of cybercrime (Metwally, 2022; Al-Billeh & Al-Hammouri, 2023).

There are many types of cyber risks to which individuals, organizations, companies and countries are exposed, the most important of which are as follows:

Identity theft

Identity theft is one of the most prevalent and harmful types of cyber risk. Identity theft is a method by which a person's personal information regarding their identity is taken, used for fraud and other illegal activities, and then used for financial gain. A dangerous application that has infected your computer may pass through the system to obtain personal information such as the person's name, or details such as their address, place of birth, phone number, ID card number, credit card number, etc. that can be used to create ID cards (Al -Baraisa, 2021).

Online fraud

It is a type of fraud in which fraudulent activities are carried out to achieve financial advantages over the Internet and numerous media, including websites and email. The risk of exposure to online fraud for people, companies, organizations, and governments has increased as a result of the growing number of Internet users globally (Dahiya, 2020).

There are many different types of online fraud, but the top three are selling counterfeit goods to dishonest merchants, stealing credit card information and using it to defraud credit cards, and sending users to the wrong site to falsify information or phish. People are deceived by sending them to sites where they can collect as much information about them as possible and use it by the criminal to make money (Gee & Ford, 2011).

The legal nature of cyber risks

There is no doubt that data and information are money, and since funds may be legally owned and transferred, there is nothing to prevent them from being subject to financial rights as well. Contemporary legal thought has shifted in this direction, with some jurisprudence believing that electronic information has economic value because it may be legally owned and have an ethically acceptable form of transmission and possession (Al-Ajmi, 2014).

Consequently, when discussing the legal nature of cyber risks, the legal status of information or data and whether or not they have value in themselves is the main theme, or they gain their value from being a new set of values that may be attacked. Since

information and data are intangible and cannot be considered proprietary values, except in cases involving intellectual property, they have been excluded from the scope of abuse according to the theory of the first group, which states that only material things can be owned. This theory is based on (Dahiya, 2020).

Another aspect of jurisprudence is that knowledge and data are a new set of values that can be obtained without the use of tangible objects because data is positively related to its owner. That is, the author's relationship with data is very similar to information, which is money that can be owned or exploited based on its economic value and not based on its physical entity, and as such, it deserves legal protection and treatment like money (Metwally, 2022).

To make this study more comprehensive, we will assess cyber risks in the form of images that are the most prevalent, which differ from each other, and explain this in each image to be comprehensive enough:

Cybercrime against people

Nothing prevents crimes against known persons from being committed through technological methods. However, due to the method used, the scope of these crimes may be limited to defamation and slander, as well as crimes involving disclosure and crimes that pose a threat to personal safety online (Al-Qassab, 2011).

Cyber risks to funds

There are two forms of cyber risk to funds, where the first type of cyber risk to funds involves committing a crime directly on the computer, while the second type entails committing a crime while using the computer, such as forging official papers or creating fake money. The same applies to the use of computers for unwanted access to data and information (Dahiya, 2020).

Cyber risks to State security and crimes against public Morals

Due to the nature of those crimes that allow them to be carried out using written means, risks to state security may be one of the easiest risks that are committed by electronic means. Examples include crimes against the internal or external security of the state, including crimes such as espionage, incitement to riots, and disturbing the integrity of the country (Al-Baraisa, 2021).

The impact of cyber risks on individuals, companies, and different sectors

A successful cyberattack can cause serious damage to companies or institutions. Thus, it affects the company's profits, in addition to the status of the business and the confidence of individuals and consumers. The impact of cyber risks can be divided into three categories: the economic cost of cyber risk,

reputational damage, and the legal consequences of cyber risk (Al -Baraisa, 2021).

Legal consequences of cyber risks

Data protection and privacy laws require the security of all personal data held by you, whether that of employees or customers, in case such data is compromised by mistake or deliberately. The risk of loss resulting from internal and external incidents or third parties, such as theft, integrity breach, corruption of information or technology assets, internal and external fraud, and business disruption, is known as cyber risk, which is classified as a type of operational risk. This concept is generally in line with ongoing efforts by the commercial sector, such as the ORX Cybersecurity and Information Risk Initiative, to identify cyber threats. Cyber risk incidents may compromise the availability, confidentiality, and integrity of data and information as well as the efficient operation of the IT infrastructure (Khashashneh et al., 2023).

A single cyberattack may be linked to the interruption of various services within the target organization, data breaches, and theft of customer payments. Cyber risks have multiple impacts and losses, and all events associated with cyber incidents fall under the category of cyber risk, except for opportunity costs, lost income, expenses associated with risk management, and control upgrades made in an attempt to stop further losses (Metwally, 2022).

Legal bases of cyber risk insurance

Cyber risk insurance is carried out according to several bases, including:

First: Information of a personal nature

All organizations are interested in preserving this type of information. Article 2 of the French Information and Electronic Liberties Code (Chapter VIII: Personal Data) stipulates that information associated with each unique individual (known) or can be deduced directly or indirectly using a person's identification number or other associated numbers must be the majority of means of identification, such as personal data in the possession of that person. These should be known to determine whether the person can be identified or not.

Second: Strategic Data of the Organization

The strategic statements of the organization include the following:

Enterprise information: Hackers target information related to investment funds, and targeted institutions have information about companies that want to buy or sell them in case of due diligence or mandatory data auditing. R&D data development is another category of strategic data that can be targeted. There are some other data points that the company considers strategic, including:

- Contracts concluded with partners or entrepreneurs to provide a new product or service.
- Written contracts with service providers (franchisees).
- The development strategy or business plan of the organization.
- Respond to tender requests.

Cyber contract guarantees on risks and damages (subject matter of the contract) include:

1. Basic safeguards include theft of personal information, loss of exploitation, breach or damage to data (information), and legal liability of the insured (the institution) when consumers whose information has been taken claim that the organization has failed to protect its information system.
2. Additional safeguards include attempted cyber extortion (attempted threat), attempted cyber embezzlement, attempted industrial and commercial cyber espionage, attempted electronic damage to the reputation of the organization, attempted impersonation and speaking on behalf of the organization, dispute over Internet customers, and service provider.

Third: Effects of the Cyber Insurance Contract

This section explains the duties that the insured and the insurance company bear after the execution of the contract. Article 927/2 of the Jordanian Civil Code stipulates that 'the insured is obliged to disclose data that are influential to the insurer to determine the means he takes to prevent the risk to the insured. In addition, he has no obligation except to provide those important data only, and this is at the time of conclusion, as this time is tantamount to the formation of the consent of the insurer in accepting the insurance contract or not.

Fourth: In the cyber insurance contract, there is a condition for disclosing data to the insurance company:

Information cannot be disclosed to the insurance company due to its confidentiality, but these contracts allow disclosure of software, hardware, and other elements used, and the common denominator in traditional automated media contracts is the promise to recover information after data loss. They are very similar to contemporary cyber contracts in terms of information loss and retrieval challenges and include the following (Metwally, 2022).

- **Monitoring security systems:**
- Compared to other insurances, this liability is considered narrow for this type of insurance, whether in traditional automated information contracts or cyber insurance contracts (new contract) (Gumenyuk, 2021).
- **Traditional computer protection contracts are committed to security and**

prevention:

The insurance company can use specialists to inspect the institution's site to verify large installations of computer hardware and software to assess risks and provide preventive and security measures so that maintenance includes the maintenance of machinery, equipment, or other elements through maintenance and repair.

Finding, diagnosing, and repairing defects or replacing faulty components are all aspects of maintenance. Once the repair process is complete, its quality must be checked using all available tools and, if possible, calibrated by the quality standards now in force (Al-Ajmi, 2014; Al-Billeh, 2022d).

Legislation related to cyber risk insurance in different countries

There are several legislations related to cyber risk insurance in different countries, the most important of which are:

First: Legislation of the State of Kuwait:

About the development of a special penal policy to deal with the increased risks involved in crimes related to technology and communications along with the diversity of aspects of the problem of crimes related to technology and communications. The Kuwaiti legislator approved the Electronic Transactions and Cybercrime Law No. 37 of (2014) so that the Communications and Information Technology Regulatory Authority was established. 'The source of any radio waves to verify the license of that source without compromising the confidentiality of the messages'

As a result, the Executive Bylaws of Law No. 37 of 2014 were issued, which assigned the Chairman of the Authority several tasks, namely:

1. Setting laws and rules to control the ICT industries.
2. Keeping pace with the rapid development of the ICT industries when submitting draft legislation.

According to Law No. 63 of 2015 on combating information technology crimes, cybercrimes have been included in Kuwaiti law. The State of Kuwait has taken its first step towards criminalizing illegal conduct carried out through information and communication technology with this law. This law criminalizes access to a computer system or network, electronic data processing system, secure computer system, or information network without a permit.

Second: UAE legislation

To successfully address cybercrime, the UAE has implemented substantial amendments to its substantive, procedural, and executive legislation since 2006.

Federal Law No. 2 of 2006 was issued by the UAE legislator, while Law No. 1 of 2006 was linked to e-transactions and business. This decision was followed by the issuance of Ministerial Resolution No. 1 of 2008 regarding the publication of the list of certification service providers, and in light of the modernization of the United Arab Emirates of its legal framework, Federal Decree-Law No. 3 of 2012 was issued regarding the establishment of the National Electronic Security Authority, which includes several specializations. The most important of which are: (58)

- Combating all forms of cybercrime, information networks, and technology.
- Receive feedback and ideas on the country's technological security.
- •Proposed law on cybersecurity.
- •Enhance the value of cybersecurity while working with competent authorities.

According to Law No. 12 of 2016 amending Decree-Law No. 5 of 2012 regulating cybercrime prosecutions, anyone who evades the protocol address of an information network using a fake address or address is subject to a fine, and a fine for a short prison sentence is beneficial to others or is done in any other way to commit or prevent a crime.

The UAE legislator has issued Law No. 26 of 2015 regarding the regulation and dissemination of data in the Emirate of Dubai. Thus, in light of the protection of customer data, Article 13 of that law stipulates a dual obligation to take all necessary measures to achieve a balance between the process of publishing and exchanging data and maintaining its confidentiality and privacy. Followed by other objectives and protocols that must be followed to maintain the privacy and confidentiality of customer information during the dissemination and transfer of data.

Third: Legislation of the State of Qatar

The State of Qatar has strengthened its national legislation and operations to combat cybercrime through the issuance of Law No. 14 of 2014, which is an important step. Next, the legislation covers many forms of crime, including violation of the information system, software, and network, electronic fraud and forgery; and violation of intellectual property rights.

The State of Qatar concluded that to effectively combat cybercrime, legal frameworks at the national and international levels must be strengthened. In addition, to support peace and stability and promote an open, stable, and sound ICT environment, effective steps must be taken to make terrorist crimes committed using information technology criminal offenses (Al-Qassab, 2011).

In addition, the National Cybersecurity Strategy was published in 2014. Recently, in light of Qatar's hosting of the 2022 World Cup™, it called for the

creation of a unified international platform through INTERPOL to enhance cybersecurity communication and collaboration for sporting events, and this latest step demonstrates that Qatar recognizes the value of international cooperation in global cybersecurity initiatives.

Conclusion

Cyber risk insurance has become essential in the modern era, as cyber threats are constantly increasing. Companies and individuals can obtain a cyber insurance policy to protect their systems and data from malicious cyber intrusions and intrusions. Cyber risk insurance is important for businesses and individuals to protect themselves from cyberattacks and online breaches.

Individuals and businesses should follow some tips and guidelines to enhance and ensure their cybersecurity, including investing in cybersecurity programs that suit their financial needs and capabilities, enhancing security awareness among employees directing them to follow data security practices, using strong passwords, and updating them regularly. Perform regular backups of sensitive data. Also, update protection and maintenance programs.

References

Al-Ajmi, A. (2014). *Practical and legal problems for electronic crimes 'comparative study'*. Master Thesis. Middle East University.

Al-Baraisa, H. (2021). *Moral Corporation for Electronic Crime in accordance with the Jordanian Penal Code*. Master Thesis. Middle East University.

Al -Momani, Z. (2021). *The impact of the Korona's pandemic on work contracts*. Master Thesis. Middle East University.

Al-Qassab, S. (2011). *The role of reinsurance in guaranteeing the rights of the insured in the face of the original insured*. Master Thesis. Middle East University.

Al-Billeh, T. (2022a). Judicial oversight on the administrative contracts in the Jordanian legislation and the comparison: the modern qualitative jurisdiction of the administrative judiciary. *Indian Journal of Law and Justice*, 13 (2), 1-28. https://ir.nbu.ac.in/handle/123456789/4763

Al-Billeh, T. (2022b). The Correction of the Invalidity of the Civil Trials Procedures in Jordanian and Egyptian Legislation: The Modern Judicial Trends. *Kutafin Law Review*, 9 (3), 486-510. https://doi.org/10.17803/2713-0525.2022.3.21.486-510

Al-Billeh, T. (2022c). Legal Controls of the Crime of Publishing a Program on the Internet in Jordanian Legislation. *Pakistan Journal of Criminology*, 14 (1), 1-14. http://www.pjcriminology.com/wp-content/uploads/2022/08/1.-

Legal-Controls-of-the-Crime-of-Publishing-a-Program-on-the-Internet-in-Jordanian-Legislation.pdf

Al-Billeh, T. (2022d). Freedom of Religious Belief and the Practice of Religious Rites According to the Jordanian Legislation: Difficult Balance Between International and Regional Requirements as well as the National Legislative Controls. *Balkan Social Science Review*, 20. 117-137. https://js.ugd.edu.mk/index.php/BSSR/article/view/5503/4660

Al-Billeh, T. (2023a). Disciplinary Measures Consequent on the Judges' Misuse of Social Media in Jordanian and French Legislation: A Difficult Balance between Freedom of Expression and Restrictions on Judicial Ethics. *Kutafin Law Review*, 10(3), 681–719. https://kulawr.msal.ru/jour/article/view/224

Al-Billeh, T. (2023b). The Situations Related to the Functioning of the Administrative Judiciary in Jordan for the Year 2020: A Step Forward. *International Journal for Court Administration*, 14(3). https://doi.org/10.36745/ijca.453

Al-Billeh, T. (2024a). Jurisdiction Regarding Administrative Proceedings in Jordanian and French Legislation: Views on the Administrative Judiciary in 2021. *Int J Semiot Law*, 37, 189–215. https://doi.org/10.1007/s11196-023-10064-5

Al-Billeh, T. (2024b). Teaching Law Subjects by Using Educational Robots: Does the Use of Robots Lead to the Development of Legal Skills Among Law Staudents?. *Asian Journal of Legal Education*, https://doi.org/10.1177/23220058241227610

Al-Billeh, T., & Abu Issa, H. (2023a). The Role of the Environment Committees in the Nineteenth Parliament for the Year 2020 in Studying Matters Related to Environmental Affairs in Jordan. *Journal of Environmental Management and Tourism*, 1(65), 168-175. https://doi.org/10.14505/jemt.14.1(65).16

Al-Billeh, T., & Abu Issa, H. (2023b). Jordanian Women's Political Participation in The Nineteenth Parliament Elections (2020): The Beginning of the Political Rise of Jordanian Women?. *Dirasat: Human and Social Sciences*, 50(5), 244 -255. https://doi.org/10.35516/hum.v50i5.961

Al-Billeh, T., & Al-Hammouri, A. (2023). Guarantees of Juvenile Trial Procedures in Jordanian Legislation: The International Standards towards Reformative Justice for Juveniles. *Pakistan Journal of Criminology*, 15 (1), 1-16. https://www.pjcriminology.com/wp-content/uploads/2023/07/1.Tareq_Billa_Paper_Final_Draft.pdf

Al-Billeh, T., & Al-Qheiwi, M. (2023). OBJECTION OF THIRD PARTIES OUTSIDE THE LITIGATION IN ADMINISTRATIVE JUDICIAL JUDGMENTS IN THE JORDANIAN AND FRENCH LEGISLATION. *Revista Relações Internacionais do Mundo Atual*, 4(42), 76-101. http://revista.unicuritiba.edu.br/index.php/RIMA/article/view/e-5951

Al-Hammouri, A., Al-Billeh, T., Al-Billeh, H., Alhammouri, N., & Roua Belghit, R. (2024). International and Constitutional Efforts to Protect the Environment Through the Use of Artificial Intelligence Techniques. *Pakistan Journal of Criminology*, 16 (1), 387-398. https://doi.org/10.62271/pjc.16.1.387.398

Al-Khawajah, N., Al-Billeh, T., & Manasra, M. (2023). Digital Forensic Challenges in Jordanian Cybercrime Law. *Pakistan Journal of Criminology*, 15 (3), 29-44.

Chase, J., Niyato, D., Wang, P., Chaisiri, S., & Ko, R. K. L. (2019). A Scalable Approach to Joint Cyber Insurance and Security-as-a-Service Provisioning in Cloud Computing. *IEEE Transactions on Dependable and Secure Computing*, *16*(4), 565–579. https://doi.org/10.1109/tdsc.2017.2703626

Dahiya, R. (2020). *The impact of technological development on the systems and means of payment*. Master Thesis. University of Algeria.

Deeb Mahmoud, A. (2009). *Consumer Protection in Electronic Contracting*. Master Thesis. An -Najah National University.

Gee, G. C., & Ford, C. L. (2011). Structural racism and health inequities. *Du Bois Review: Social Science Research on Race*, *8*(1), 115–132. https://doi.org/10.1017/s1742058x11000130

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81–85. https://doi.org/10.1145/636772.636774

Gumenyuk, L. (2021). CYBER INSURANCE: MODERN REQUIREMENTS. *Economics & Education*, *6*(4), 33–36. https://doi.org/10.30525/2500-946X/2021-4-5

Jacobs, T. (2016). Industrial-sized Cyber Attacks Threaten the Upstream Sector. *Journal of Petroleum Technology*, *68*(03), 42–50. https://doi.org/10.2118/0316-0042-jpt

Khashashneh, T., Al-Billeh, T., Al-Hammouri, A., & Belghit, R. (2023) The Importance of Digital Technology in Extracting Electronic Evidence: How Can Digital Technology be used at Crime Scenes?. *Pakistan Journal of Criminology*, 15 (4), 69-85,

https://www.pjcriminology.com/publications/the-importance-of-digital-technology-in-extracting-electronic-evidence-how-can-digital-technology-be-used-at-crime-scenes/