Canadian Journal of Educational and Social Studies
Vol. 6(1), 2026, pp. 144-160

A Comparative Analysis of Insurance Protection Strategies Against Cyber Threats in Türkiye and the European Union

Pelin Atila Yörük[1]

[1] PhD, Ankara University Faculty of Law, School of Justice, Türkiye
https://orcid.org/0000-0001-9474-4454
Email: pelinatila@gmail.com

DOI: 10.53103/cjess.v6i1.454

Abstract

The purpose of this study is to investigate insurers' legal responsibilities under cyber risk insurance policies in the event that cyberattacks violate personal data. It contrasts EU regulations (like GDPR and the German AVBC framework) with Turkish laws, especially the Turkish Commercial Code and the Turkish Personal Data Protection Law (PDPL). According to the study, the insured company's compliance with PDPL regulations determines the insurers' liability. These include implementing appropriate administrative (like staff training) and technical (like encryption) measures. Claims may be partially or completely rejected if the business fails to fulfill these responsibilities, which is viewed as negligence. In contrast to the EU's more transparent documentation (such as KID), Türkiye faces a number of major issues, including inconsistent policy terms, a lack of actuarial data, unclear coverage of indirect damages (such as reputational harm), and regulatory gaps.

Keywords: Cyber Insurance, Personal Data Breach, Insurer Liability, PDPL, GDPR

Introduction

Digitalization has recently become increasingly pervasive, so both businesses and public institutions are going through heightened susceptibility to cyber threats. Cyber risk insurance has emerged as a crucial instrument aimed at underwriting the financial losses and legal liabilities precipitated by such incidents (Şekeroğlu & Özüdoğru, 2019). Defining 'cyber' as an all-encompassing term for activities executed by means of computer networks and digital platforms (Şağban, 2021), the concept involves a wide variety of threats, such as data breaches, unauthorized access, and malware, causing major risks to long-term organizational sustainability (Karadağ, 2021).

Among the most common types of cyberattacks today are malware, ransomware,

phishing, and DDoS (distributed denial-of-service) attacks (KPMG, 2022). A data breach is generally defined as the compromise of the confidentiality and integrity of electronic data (Öztürk, 2018) and causes not merely data loss but to massive economic loss on an international scale as well. For example, in Germany, annual losses on account of cyberattacks are reported to have reached approximately 200 billion euros by the year 2024 (Bitkom and Strategy& data), and these figures are increasing year by year. The annual cost of cybercrime was nearly $6 trillion in 2021 globally and is estimated to reach approximately $10.5 trillion in 2025 (Cybersecurity Ventures and various 2025 reports). These damages include direct financial losses, business interruption, loss of reputation, and legal sanctions (Cobalt, 2025; while your reference is in line with current estimates, the most widely accepted figure is about $10.5 trillion). At this stage, cyber insurance policies can help reduce the financial and operational loss following an attack, and many organizations have made protecting sensitive and personal data a priority (Çetin & Alpay, 2020). As the number and complexity of cyberattacks increases, the insurance industry is evolving, expanding, and refreshing itself (Gönen & Kaya, 2023).

Over the past few decades, the rise of high-value digital assets such as NFTs has further expanded the scope of cyber insurance. The potential for very high losses in the event of theft or loss of such assets has paved the way for the development of blockchain-based insurance products and has embarked on innovative applications by enhancing transparency and data security in the industry (Şağban, 2021).

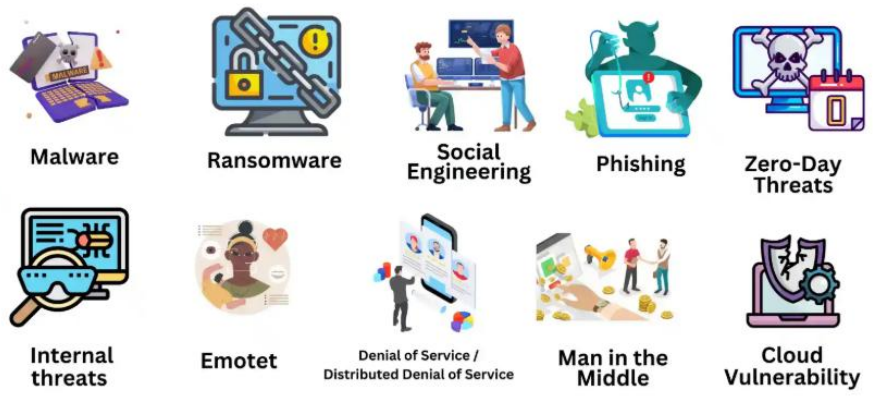

Figure 1: Cybersecurity threats

The insurance sector is not simply a sector that provides a risk transfer mechanism but it also contributes to the economy through employment, contributing to tax revenues, and supporting macroeconomic growth by transferring resources to capital markets (Uğurlu Keskin, 2023). Technological advances, such as innovative applications like

blockchain-based policies, are changing the scope and functioning of insurance products in transactions by increasing data security in a transparent manner (Oyal, 2024). Digitalization has diversified sales and distribution channels and facilitated access to insurance services via the internet, bank branches, and brokerage firms (Dönmez & Başar, 2016).

According to several studies, Turkish enterprises are less aware of cyber dangers and insurance than those in European nations (Cebeci, 2021). The successful growth of policy coverage and the diversification of insurance products are severely hindered by this circumstance. Increasing employers' understanding and fortifying regulatory frameworks are essential for the sector's advancement (Altuntaş et al., 2023). This study aims to investigate cyber insurance practices and insurers' responsibilities in Türkiye in a multifaceted way. By making recommendations based on a comparison analysis with EU regulations, it will help the industry grow.

The Increase in Cyber Risks and Their Impact on Businesses

Globalization and technological advancements have increased the scope and complexity of cyber hazards. Cyber risks have progressed from being merely a security concern to becoming a strategic threat in terms of business continuity, reputation management, and long-term sustainability as companies' reliance on digital infrastructure grows every day (Scheuermann, 2018). Due to their low financial resources and technological capabilities, small and medium-sized businesses (SMEs) in particular are in the greatest risk category and are still the main target of cyberattacks (Alkan, 2023).

According to multiple independent assessments, the worldwide cost of cybercrime reached $10.5 trillion in 2025 (Cybersecurity Ventures, 2025), making it the third largest economy in the world. According to IBM's 2025 Cost of a Data Breach Report, the average cost of a data breach is predicted to be $4.44 million, a 9% decrease from the previous year. This decline is ascribed to the widespread use of AI-powered rapid detection and response systems (IBM, 2025). Although data encryption rates have decreased (to 50% in 2025), recovery costs average about $1.53 million (Sophos State of Ransomware, 2025). According to recent reports, 50–60% of organizations have been vulnerable to ransomware attacks. The healthcare sector has seen a significant decrease in data breach costs compared to the previous year, falling to an average of $7.42 million – a reflection of security improvements and faster response times in the sector; however, healthcare remains the costliest sector (IBM, 2025).

Cyberattacks not only result in immediate financial losses but can permanently harm a company's brand. A company that has a data breach loses its competitive advantage, permanently erodes its brand value, and loses the trust of its customers (Gönen & Kaya, 2023). The commercial sector and governmental institutions are equally threatened by

common tactics like fraud, data theft, and particularly phishing in the digital environment (Öztürk, 2018). Systematic risk analysis can be used to quantify such attacks, and methods like "attack-defense trees" make it possible to quantify the efficacy of both technical and user-focused defenses. Research demonstrates that antivirus and spam filters alone are insufficient; however, when combined with technical measures and intensive user training, the risk can be reduced by up to 98% (Ertem & Ozcelık, 2024).

Conducting regular risk analyses to conserve businesses from cyber risks is no longer an option but an urgent requirement. Legal responsibilities, business processes, and data protection obligations must be carefully reviewed; appropriate cyber risk insurance coverage must be determined, and policy terms must be evaluated in detail (Tekin, 2020). While low-cost, effective solutions and government-supported training programs are critically important, especially for SMEs, large organizations should prioritize AI integration, Zero Trust architectures, and robust backup strategies.

As a consequence, in this era of rapidly changing cyber threats, proactive risk management and comprehensive insurance strategies enable businesses not only to survive but also to gain a competitive advantage. While threats are bound to become even more complex in the future, the steps taken today will determine tomorrow's security – therefore, cybersecurity should no longer be viewed as a cost item but as a strategic investment.

Cyber Insurance Policies and the Obligations of the Parties

An insurance contract is a legal relationship established between the insurer and the insured, imposing obligations on both parties. In accordance with Article 1401 of the Turkish Commercial Code (TTK), the insurer undertakes to pay compensation in the event of a predetermined risk occurring, in return for the insured's obligation to pay premiums (Ayhan et al., 2021). Risk refers to events that have the potential to cause harm, and in today's digital world, these risks are rapidly evolving and taking on new dimensions, such as cyber threats.

After the insurance contract is established, the insured is obligated to pay the premiums specified in the contract on time. Failure to pay premiums or late payment of premiums results in default, and the insurer's liability may be partially or completely eliminated (Can, 2005). However, insurance companies, may only engage in insurance activities and are required to conduct these activities in accordance with the regulations set forth in the Insurance Law No. 5684. These regulations aim to protect the financial strength of companies and the rights of policyholders, and they directly affect the risk assessment and premium determination processes, especially in cyber risk insurance (Ayhan et al., 2021).

Life insurance and property and liability insurance are the two primary categories of insurance contracts. According to Šekeroğlu and Özüdoğru (2019), cyber risk insurance

is categorized under property and casualty insurance and covers a variety of digital threats that businesses may encounter as well as the resulting damages. Major risks like data loss, information security breaches, system disruptions, third-party liability, business interruption, multimedia liability, and regulatory penalties are typically covered by policies (Yüce, 2024). On the other hand, some conditions are not covered. Terrorist and war crimes, deliberate infractions (e. (g). Nuclear risks, damages resulting from financial market fluctuations, bodily injury, physical risks, wrongful acts, and damages caused by the insured's own fault are typically not covered; these exclusions should be specified in the general terms and conditions of the policy (Kender, 2015). It is important to specify the coverage limits.

Cyber risk insurance policies are intended to pay for damages from a wide range of incidents that occur in digital spaces, including the costs of data recovery and lost revenue, such as when a business system is hacked and customer data is stolen. The most recent information available puts global cybercrime costs at $10.5 trillion by 2025 (Cybersecurity Ventures, 2025) and reports numerous confirmations of this. The average cost of a data breach, according to the IBM 2025 Cost of a Data Breach Report, is $4.44 million, a 9% decrease from the previous year, and this decrease is due to the effect of AI-driven rapid detection and response systems (IBM, 2025).

Türkiye has a Personal Data Protection Law (PDPL) that places heavy responsibility on data controllers to implement technical (encryption and firewalls) and administrative (staff training and policy development) controls to ensure the security of the data, failure of which can result in the imposition of administrative fines in the case of data breaches and legal liability (Çetin & Alpay, 2020). Insurance companies need to review whether these obligations have been met and adjust the risk accordingly; data protection measures directly impact the level of the policy premiums and coverage limits. According to GlobalData (2025-2026 estimates), the global cyber insurance market is expected to reach $22.2 billion by 2025 and $35.4 billion by 2030.

In short, the insurance not only protects the business financially but also incentivizes the business to improve information security processes, especially in terms of PDPL compliance and proactive risk management. By 2026, with digital threats multiplying, cyber insurance strategies backed by adequate coverage will allow businesses to meet their legal responsibilities and remain competitive, making cyber insurance a strategic necessity rather than a luxury.

Protection of Personal Data

Sensitive data (special categories of personal data) may be interpreted differently in different legal systems and societies and can include data that may result in discrimination, harm, or damage to the dignity of individuals; Article 9 of the GDPR

(General Data Protection Regulation) in the EU gives this data a special category status (e.g., race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data [processed for the purpose of uniquely identifying an individual], health data, and data on sexual life or sexual orientation [GDPR-info.eu, updated text 2026]; technological advancements, especially in biometric data (such as facial recognition and fingerprints) and DNA databases, are constantly broadening the definition of sensitive data and complicating the legal frameworks (Kaya, 2011; GDPR Art. 4(14) definition).

The protection of personal data from the perspective of privacy and human rights and detailed regulations by international organizations such as the Council of Europe and the European Union are also regulated by international organizations. The criminal law protection of personal data in Türkiye is given in Articles 135-138 of the Turkish Criminal Code and the crime of failing to delete or anonymize data is stated in Article 17/2 of the PDPL (Dülger, 2016). Article 6 of the PDPL defines special categories of personal data through a limited enumeration that includes race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, attire, membership in associations/foundations/unions, health, sexual life, criminal convictions/security measures, and biometric and genetic data (PDPL official website, 2026 current definition). Because these data may result in discrimination or victimization if they were to become public, they are covered with greater protection than other personal data, and they may only be processed under certain conditions.

The Personal Data Protection Law (PDPL) in Türkiye is the first full-fledged regulation on data security and is of great significance, especially for the insurance sector, since the activities of the insurance sector are mostly based on the processing of personal (and often sensitive) data (Eren, 2019). This presents an important risk factor for entrepreneurs considering opening an insurance agency, because noncompliance with the PDPL can result in heavy administrative fines (the upper limit of administrative fines for data security violations as of 2026 has increased to approximately 17 million TL) and loss of reputation. In recent developments, the insurance sector is encouraged to base private health insurance contracts on legal obligations and contract performance to ensure in harmony with the PDPL, which offers sectoral practices more in line with the overall data protection framework (2025 Private Health Insurance Regulation amendments).

Not only do compliance with obligations concerning personal data protection mitigate criminal risks, but it also creates a competitive advantage and contributes to corporate sustainability, especially in highly sensitive, data-intensive sectors like insurance, where regular data inventories, compliance with disclosure obligations, consent processes on the basis of purpose, and robust technical/administrative measures (such as encryption, access controls, and regular training) are crucial (Çetin & Alpay, 2020). Although full compliance of the PDPL with the GDPR is expected to be completed by

2026, the steps taken today will determine tomorrow's competitive strength, which is why data protection has now become a strategic necessity.

Cyber Attacks and Organizations' Responsibility for Data Protection

The digitalization process leaves businesses vulnerable to cybercrimes originating both internally and externally. Attacks carried out internally are generally defined as “fraud” and are integrated into the audit processes of institutions. Cybersecurity auditing has now become an integral part of routine internal control systems, and process-based holistic auditing models ensure more effective risk management (Selimoğlu & Altunel, 2019). Data breaches are complex processes resulting from multiple factors coming together, and under the Personal Data Protection Law (PDPL), data controllers are required to take the necessary technical and administrative measures to protect personal data. Failure to take these measures is considered “negligence” and results in the data controller's liability (Badur & Konca, 2022).

Internal audit units are a key component to reduce the cyber risk, and a three-line defense approach (governance, risk management and compliance, operational controls, independent audit) provides an added layer of security to digital systems and minimizes the effects of an attack (Selimoğlu & Altunel, 2019). While ransomware attacks are still prevalent, with about 50-60% of organizations having experienced a ransomware attack by 2025, the data encryption rate has fallen to 50%, but recovery costs average $1.53 million (Sophos State of Ransomware, 2025). Thus, a holistic risk management strategy is required, beyond technical measures.

Negligence becomes a fault over time; for example, insufficient cybersecurity audits or failure to anonymize data can lead to administrative sanctions and liability for damages (Badur and Konca, 2022). When determining the scope of the policy, insurance companies evaluate whether the business has met these obligations, and if negligence is found, they may deny compensation in whole or in part (Yüce, 2024). In fact, the insufficiency in biometric and genetic data protection results in a higher assessment of the fault, and the insurance company\'s right to recover the compensation paid to the data controller (right of recourse) is brought into discussion (Yüce, 2024). Therefore, policies should include liability-reducing clauses to clarify the responsibility of the business to take precautions and to reduce the risk for insurance companies.

The illicit processing of personal data causes both material and moral damages, and claims for compensation are heard in various courts depending on whether the data controller is in the public or private sector, with jurisdiction determined by the relationship in which the data is processed (employment, consumer, or commercial) (Badur & Konca, 2022). The PDPL requires data controllers to take both preventive and corrective measures; insurance coverage may be restricted in cases of negligence.

Cyber risks are far more complicated and severe than conventional risks and have become a significant risk for businesses, leading them to seek protection through cyber insurance policies as well as technical measures to secure their digital assets (Karadağ, 2021). Insurance companies, including in Türkiye, are developing various practices in terms of policy coverage, pricing, and claims handling; SMEs, in particular, require more comprehensive policy terms because of the growing risk (Gönen & Kaya, 2023). The growing use of remote access during the COVID-19 pandemic has increased the likelihood of cyber attacks and heightened the demand for cyber insurance (Alkan, 2023).

According to industry reports (Cybersecurity Ventures, 2025), the global cost of cybercrime was $10.5 trillion in 2025 and is expected to increase to $12.2 trillion by 2031, while the average cost of a data breach was calculated at $4.44 million (IBM, 2025), a 9 percent reduction from the previous year, which can be attributed to the use of AI to achieve rapid detection and response. The total premium production of the Turkish insurance industry is forecast to grow to 1.15-1.20 trillion TL by 2025, with increasing demand for innovative products like cyber insurance (KPMG Insurance Sector Outlook 2025 and industry forecasts).

In insurance law, the "principle of interest" states that the property or assets are not the element to be protected in the insurance contract, but the economic interest or benefit arising from the property or assets, which could be the interest of the owner of the property or of another party, such as the carrier, broker, or pledgee (Avcı, 2020). Similar to other forms of insurance, this principle is also applied to new generation policies such as cyber insurance, and the insurable interest is expressed in economic terms such as material loss, reputational harm, business disruption, and legal liabilities that may be caused by data breaches or cyber attacks (Avcı, 2020). In this case, cyber risk insurance protects the interests related to the digital assets (data, systems, reputation) of the business and the amount of the insurance premium should not exceed the value of the potential economic loss that might occur from a cyber risk event.

The insurance sector depends heavily on the processing of personal data for its operations and must therefore approach the obligations of the Personal Data Protection Law (PDPL) with the utmost sensitivity. In the event of a personal data breach, data controllers face both administrative penalties (with an upper limit of approximately 17 million TL as of 2026) and material and moral damages claims that data subjects may file. Therefore, entrepreneurs operating in the insurance sector must take into account the obligations of the PDPL (preparing a data inventory, providing information, taking technical/administrative measures, managing consent processes) from the very beginning of their business plans (Eren, 2019). The protection of personal data is not only a legal obligation but also a critical requirement for institutions to maintain their reputation and customer trust (Çetin & Alpay, 2020).

Insurance contracts are shaped by judicial decisions and legislative provisions, and

legal oversight ensures that insurance companies conduct their activities within a specific framework (Ayhan et al., 2021). The Insurance Law contributes to the orderly functioning of the sector by requiring contracts to be drawn up only in accordance with legislation. While cyber insurance policies aim to cover damages arising from data breaches, the insurance company's liability is not the same in every case. The scope of the policy, exclusion clauses (such as war, intentional breaches, nuclear risks), and the company's compliance with GDPR obligations directly determine the effectiveness of insurance protection (Yüce, 2024). Since the insurance sector's experience in this area is limited in Türkiye, the scope of coverage and exclusions depend largely on the practices of insurance companies; this reduces the predictability of policies and creates a risk factor for entrepreneurs (Cebeci, 2021). Insurance contracts are shaped by judicial decisions and legislative provisions, and legal oversight ensures that insurance companies conduct their activities within a specific framework (Ayhan et al., 2021). The Insurance Law contributes to the orderly functioning of the sector by requiring contracts to be drawn up only in accordance with the legislation. While cyber insurance policies aim to cover damages arising from data breaches, the insurance company's liability is not the same in every case. The scope of the policy, the exclusion clauses, and the company's compliance with GDPR obligations determine the effectiveness of insurance protection (Yüce, 2024). Since the insurance sector in Türkiye has limited experience in this area, the scope of coverage and exclusions depend largely on the practices of the insurance companies. This situation reduces the predictability of the policies (Cebeci, 2021).

The Legal Aspects of Personal Data Protection against Cybercrime

The Personal Data Protection Law (PDPL), enacted in 2016, sets out extensive requirements for all entities and organizations handling personal data in Türkiye, but the reach of the PDPL in the area of cyber insurance policies is still limited, and policies are not designed to specifically address data breach risks (Tekin, 2020). During the process of PDPL compliance, insurance companies take into account the extent to which businesses meet their obligations (technical/administrative measures, data inventory, disclosure, etc.) and refrain from providing complete coverage to businesses that have not taken sufficient precautions (Yüce, 2024). As a result, insurance coverage becomes directly dependent on the preventive measures of the business, and interest in cyber insurance products is growing quickly because of the high administrative fines and compensation requirements imposed by the PDPL on data controllers.

Cyber insurance market in Türkiye is in its early stages of development, experience and awareness in the sector is insufficient, the market is growing despite low insurance penetration rates and growing cyber threats (TSB data, Jan-Nov 2025: 1.15-1.20 trillion TL, IBS Insurance and sector reports, 2025-2026 expectations). The demand for innovative

products, such as cyber insurance, has increased, especially after the COVID-19 pandemic as remote access and digital transformation have increased, but SMEs are not proactive: 23% have cyber insurance policies (Cebeci, 2021; current industry estimates). The leading companies in Türkiye, such as Aksigorta, Anadolu Sigorta, and Allianz, offer system repair, ransom payments, and business interruption coverage, awareness-raising training, data sharing agreements, and cyber insurance.

In accord with the "law of large numbers," a fundamental principle of the insurance industry, offering comprehensive policies without sufficient data and case accumulation is difficult. Therefore, for cyber insurance to become widespread, industry players need to prioritize education, promotion, and technology investments (Altuntaş et al., 2023). The global cyber insurance market is estimated to be around $22.2 billion in 2025 and is expected to reach $35.4 billion by 2030 (GlobalData estimates); in Türkiye, this growth has even higher potential due to low penetration.

Cyber insurance policies are policies that cover against cyber risks that businesses may encounter. The primary duty of the insured is to report any damage or loss to the insurer immediately, which is a condition for both the continuation of the contract and the commencement of the compensation (Can, 2005). While there are few judicial decisions on data breaches in Türkiye, in compensation cases filed post-PDPL (Data Breach Prevention and Placement), courts closely review the extent of the policy and the liability of the insurance company (Badur & Konca, 2022). The insurer is required to pay compensation within 45 days at the latest after the damage is recorded; unless the policy states otherwise, compensation is paid for negligence damages as well, and damages to third parties are also compensated (Ayhan et al., 2021).

One of the key criteria of the court rulings is the technical and administrative measures taken by the data controller. When gross negligence or fault is proven, however, insurance coverage is not applicable (Badur & Konca, 2022). Regarding data breaches in public institutions (e.g., large data controllers such as the Social Security Institution), administrative penalties and compensation responsibilities are considered; insurance policies constitute a critical component of the process (Işık, 2022). As of 2026, the maximum amount of the current PDPL administrative fines for the data security breaches is approximately 17 million TL (the 2025 end-of-year revaluation rate of 25.49%).

As a result, as the effect of PDPL on the insurance sector deepens, cyber insurance is still a growing sector in Türkiye but given the increased cyber threats and penalties, it is becoming an essential tool that businesses need to reduce criminal risks and financial exposure by strengthening PDPL compliance, proactive risk management, and comprehensive policies (low-cost solutions for SMEs), until 2026 when regulatory innovations (artificial intelligence, cyber resilience) and industry investments are expected to change cyber insurance from a strategic need to a tool for competitive advantage in Türkiye, the steps taken today will determine the security of tomorrow.

Comparison of Cyber Risk Insurance in Türkiye with the EU

The GDPR, which came into use in the European Union in 2018, has imposed extensive obligations on data controllers (Yüce, 2024). These obligations cannot be confined to administrative penalties, but they directly influence businesses' cyber insurance coverage. The high fines under the GDPR have led to an increase in coverage amounts in cyber insurance policies (Yüce, 2024). The GDPR has also strengthened the requirement for notification in the event of a data breach, and it is commonplace for insurance companies to offer incident management services as part of their policies, which are not routinely included in policies in Türkiye (Cebeci, 2021). From this perspective, it can be seen that EU practices demonstrate that policies should not only offer financial protection in the case of a crisis but also offer crisis management support, and that the transparency principle introduced by the GDPR should be translated into policy documents prepared in a simple and understandable manner, whereas in Türkiye the scope of policy coverage is not clearly stated, and consumers are not sufficiently informed (Dönmez and Başar, 2016), which reflects an important gap in the area of consumer rights and insurance reliability.

The Solvency II and IDD regulations, for instance, have increased transparency and consumer confidence in insurance in EU countries, while the often-changing legislation and uncertainty about the terms of the policy, on the other hand, weaken the rights of policyholders and have a negative impact on the stability of the sector in Türkiye (Cebeci, 2021). Policy guarantees are provided in comprehensive documents (e.g., KID documents) in European countries, while they are not adequately clear in the scope of coverage in Türkiye, and inflation-indexed policies, widely used in Europe, allow policyholders to reap the advantages of the long-term products, which has been limited in Türkiye due to inflation and economic instability (Cebeci, 2021).

Cyber risk insurance in Türkiye combines both property insurance and liability insurance features and therefore has a hybrid structure. Although not yet regulated by general terms and conditions, individual and commercial policies are available on the market (Şekeroğlu & Özüdoğru, 2019). The German AVBC system is a model that can be used as an example in Türkiye for regulating data security and legal liability (Yüce, 2024).

Table 1: Comparison of cyber risk insurance practices in Türkiye and the EU.[1]

Criteria	European Union	Türkiye
Regulatory Framework	Transparent system standardized with Solvency II and IDD.	No specific regulations for cyber insurance.
Policy Transparency	Consumer rights are guaranteed (KID documents are mandatory).	Frequently changing legislation and unclear policy terms.
Coverage Scope	Coverage is presented clearly and in detail with the KID (Key Information Document).	Coverage scope is unclear.
Inflation Indexing	Consumers can make informed decisions.	Consumers cannot fully understand the policy.
Preventive Services	Broad coverage including intangible damages (loss of reputation).	Intangible damages are excluded from most policies.
Actuarial Data Infrastructure	Direct material damages + third-party compensation.	Coverage is narrow and vague.
Coverage of New Risks	Long-term inflation-indexed policies are common.	Long-term products are limited due to chronic inflation.
Modeled System	Provides stability to businesses.	Economic instability hinders development.

Cyber insurance is one of the most standardized legal and corporate risk management practices within the European Union countries, thanks to Solvency II and IDD regulations, which require insurance companies to produce transparent policy documents and offer open information for consumers (Yüce, 2024), and the German AVBC regulations, which protect consumer rights with detailed documents created under the IDD (Yüce, 2024).

In Europe, insurance policies are typically all-encompassing, covering direct financial loss, third-party liability, and reputation loss of companies due to data breaches (Yüce, 2024). Also, inflation-indexed policies in EU countries reduce the long-term risks and stabilize businesses (Cebeci, 2021). This comprehensive approach enables cyber insurance to evolve into a security solution, whereas the cyber insurance market in Türkiye is in its infancy and full of ambiguity due to lack of actuarial data and regulatory complexity, which results in less comprehensive policy coverage than Europe (Cebeci, 2021), exclusion of intangible risks (Gönen & Kaya, 2023), and a limited ability to design long-term products due to chronic inflation and legal inconsistencies (Cebeci, 2021). In Europe, the transparency of documentation and the availability of inflation-indexed policies act as a buffer against long-term risks. Transparent documentation and inflation-

[1] Altuntaş et al., "Cyber insurance: Recent developments, applications and problems", p. 10. ; Gönen and Kaya, "Evaluation of cyber insurance in the Turkish insurance sector: A sectoral study", p. 715.; Karadağ, The role of cyber security insurance in cyber security management and risk reduction in the insurance sector, p. 45.; Scheuermann, "Cyber risks, systemic risks, and cyber insurance", p. 625. ; Şekeroğlu and Özüdoğru, "Guardians of the digital age: Cyber risk insurance", p. 12. ; Tekin, "Cyber risk insurance from a legal perspective", p. 675.; Yüce, "Cyber risk insurance: An examination within the framework of German cyber risk insurance general terms and conditions", p. 1620.; Dönmez and Başar, "The effect of information on insurance contract purchase preference: The case of comprehensive car insurance", p. 49.

indexed policies in Europe serve as a significant example for the Turkish insurance sector. Thus, adapting the German cyber insurance model (AVBC) to the Turkish legal system will increase policy transparency and contribute to broader coverage (Yüce, 2024). This would enable the cyber insurance market in Türkiye to mature and provide stronger protection for businesses.

International practices and experiences in Europe and the USA show that cyber insurance policies need to be based on a comprehensive risk analysis, but in Türkiye, these analyses are often incomplete due to insufficient data (Karadağ, 2021). Establishing pricing systems based on the law of large numbers will enhance policy reliability. Another key takeaway from international experiences is that policy documents must be straightforward, and although standard documents such as KID in Europe serve to inform the consumer, the vagueness of coverage in Türkiye undermines consumer rights (Dönmez & Başar, 2016). In this regard, increasing the level of transparency is a high-priority area for improvement. Finally, international examples demonstrate that insurance policies include not only financial protection but also incident management and consulting services. Expanding policy coverage in Türkiye will both strengthen the risk management capacity of businesses and increase confidence in the sector (Altuntaş et al., 2023).

In Türkiye, lack of clear standards for the extent of coverage in cyber insurance policies can result in narrow or vague coverage, which can cause confusion between what businesses expect to be covered legally and what the insurance company is obligated to cover (Cebeci, 2021). More detailed regulations, as seen in Europe, would help establish legal legitimacy in insurance products. The second important flaw is the lack of clarity in the definition of sensitive data, which can cause practical uncertainty about what data breaches are insured (Kaya, 2011). There is also a need to re-evaluate insurance coverage and compensation criteria for new data types, especially biometric and genetic data, which require clearer definitions in the law. Last but not least, the limited clarity of the details of coverage in the Turkish policy documents compared with European examples undermines the rights of policyholders. Insurers should streamline and standardize policy documents.

Conclusion and Recommendations

In Türkiye, the cyber insurance market is still developing, and the main challenges are inexperience, lack of actuarial data, and low penetration rates (around 1-2%), although by 2026, the sector has begun to transition to data and AI-based insurance and the cyber/digital risk ecosystem (Cebeci, 2021). The total insurance premium production is expected to be around TL 1.15-1.20 trillion by the end of 2025 (IBS Insurance and industry reports, 2025-2026 forecasts), and reinsurance capacity will become more selective due to cyber risks, geopolitical tensions, and threats to critical infrastructure. Companies like Aksigorta, Anadolu Sigorta, and Allianz are adding coverage to their individual and

corporate products for system repair, ransom payments, business interruption, and multimedia liability, with support from PDPL compliance and proactive risk consulting.

Consequently, cyber risk management has become more challenging and dynamic as digitalization accelerates and new technologies (e.g., artificial intelligence, IoT, and blockchain) emerge, so insurance policies must be comprehensive, transparent, and up-to-date, and preventive measures must be carefully put in place by conducting periodic risk analyses. In this new threat landscape, cyber insurance has evolved into a vital financial and operational protection for organizations

With stricter regulations like the GDPR in the European Union, cyber insurance products have developed to cover material/moral damages resulting from personal data breaches in detail (Yüce, 2024). With the introduction of the PDPL, the scope of data responsibilities has expanded and the maximum administrative fine will be around 17 million TL by 2026 (PDPL Official Announcements, 2025 revaluation rate 25.49%); this is putting pressure on the insurance sector to merge with PDPL compliance and creating a need for cyber insurance (Çetin & Alpay, 2020).

Cyber risk insurance is a robust protection against the financial, legal, and reputational damages associated with digital attacks, but the balance between the scope of coverage and the insurance industry's sustainable risk management must be carefully managed as the threats have become increasingly multidimensional (ransomware, AI, supply chain breaches), and regulatory stability (Solvency II and IDD-inspired regulations), technical infrastructure, and transparency will be increasingly important. However, insurance companies must provide clearer, standardized, and mandatory documents, such as KID (Key Information Document) for the healthy development of the sector (Yüce, 2024). Given the nature of cyber risks, pricing models should be continuously updated with sufficient data and advanced actuarial tools (Karadağ, 2021). Efforts to promote transparency by regulatory authorities, as inspired by European regulations, will lead to diversity in policies and long-term product development.

Managing the cyber risks will require awareness and cooperation, and not just insurance. Enterprises should not only buy insurance but also implement technical/administrative measures, conduct regular audits, and provide training to comply with the obligations for the protection of personal data under the PDPL (Çetin & Alpay, 2020). Insurance companies should provide preventive consulting, risk analyses, and incident response support in addition to financial guarantees to strengthen their customers\' resilience (Altuntaş et al., 2023). The demand will increase and the market will gain credibility with joint education/awareness activities by universities, professional organizations (e.g., TOBB SAİK), public institutions, and industry stakeholders.

In conclusion, the security of the digital economy and the reduction of the economic and legal risks posed by cyber threats will depend on strengthening the regulatory infrastructure (new cyber resilience regulations), increasing the technical

capacity of insurance companies (investments in AI and data analytics), and developing a data protection culture among businesses. By 2026, Türkiye will be a regional hub, and cyber insurance is no longer a luxury but a strategic necessity for digital existence.

References

Alkan, A. M. (2023). Sigorta sektöründe siber riskler. *Tokat Gaziosmanpaşa Üniversitesi Turhal Uygulamalı Bilimler Fakültesi Dergisi, 1*(1), 41-50.

Altuntaş, E., Kara, E., Soylu, A. B., & Kirkbeşoğlu, E. (2023). Siber sigortalar: Son gelişmeler, uygulamalar ve sorunlar. *Bankacılık ve Sigortacılık Araştırmaları Dergisi*, 12, 8-22.

Avcı, N. (2020). Nakliye sigortalarında sigortalanabilir menfaat kavramının değerlendirilmesi. *JOEEP: Journal of Emerging Economies and Policy, 5*(2), 91-98.

Ayhan, R., Çağlar, H., & Özdamar, M. (2021). *Sigorta hukuku: Ders kitabi*. Yetkin Yayınları.

Badur, E., & Kurt Konca, N. (2022). Kişisel verilerin hukuka aykırı işlenmesinden doğan zararların tazmini ve görevli mahkeme. *İnönü Üniversitesi Hukuk Fakültesi Dergisi, 13*(2), 476-490.

Can, M. (2005). Sigorta ettirenin sigorta primini ödeme borcunu ifada temerrüde düşmesinin sonuçları. *Bankacılık ve Ticaret Hukuku Araştırma ve Uygulama Merkezi Dergisi (BATİDER), 23*(1), 156.

Cebeci, İ. (2021). Türkiye'de Siber Risk Sigortalarina Iliskin Bir Degerlendirme. *Third Sector Social Economic Review, 56*(1), 163-188.

Cobalt. (2025). State of Pentesting 2025: Strategic Guide to Choosing the Right Security Partner. Cobalt.io. www.cobalt.io/resources/reports/state-of-pentesting-2025. Accessed 30 June 2025.

Cybersecurity Ventures. (2025). *Cybercrime to cost the world $10.5 trillion annually in 2025*. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Cybersecurity Ventures. (2026). *Global ransomware damage costs predicted to reach $250 billion USD by 2031* [Projection report]. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Çetin, A., & Alpay, S. (2020). Türk Sigorta Sektöründe Kişisel Veriler. *İstanbul Ticaret Üniversitesi Girişimcilik Dergisi, 4*(8), 81-94.

Çimen Bulut, İ. (2020). Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında getirilen yeni teknik ve yaptırım mekanizmaları. *Anadolu Üniversitesi Sosyal Bilimler Dergisi, 20*(2), 125-140.

Dönmez, P., & Başar, Ö. D. (2016). Bilgilendirmenin sigorta sözleşmesi satın alma tercihi üzerine etkisi: kasko sigortası örneği. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, 15*(29), 47-66.

Dülger, M. V. (2016). Kişisel verilerin korunması kanunu ve Türk Ceza Kanunu bağlamında kişisel verilerin ceza normlarıyla korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 3*(2), 101-168.

Eren, B. A. (2019). Kişisel verilerin korunması kanunu kapsamında finansal hizmetlerin pazarlanması. *Uluslararası Bankacılık Ekonomi ve Yönetim Araştırmaları Dergisi, 2*(2), 71-92.

Ertem, M., & Ozcelık, İ. (2024). Siber ağların risk analizi: Saldırı-savunma ağaçlarıyla temellendirilmiş niceliksel bir yaklaşım. *Journal of Innovative Engineering and Natural Science, 4*(1), 113-125.

GDPR. (2018/2026 güncel). *General Data Protection Regulation (GDPR) Madde 9: Özel kategori kişisel verilerin işlenmesi*. European Union. https://gdpr-info.eu/art-9-gdpr/ (Erişim tarihi: 12 Ocak 2026).

GlobalData. (2025). *Cyber insurance market size and forecast 2025-2030*. https://www.globaldata.com/store/report/cyber-insurance-market-analysis/

Gönen, N. V., & Kaya, E. Ö. (2023). Türk sigorta sektöründe siber sigortalara ilişkin değerlendirme: Sektörel bir araştırma. *Third Sector Social Economic Review, 58*(1), 708-726.

IBM. (2025). *Cost of a data breach report 2025*. Ponemon Institute. https://www.ibm.com/reports/data-breach

Işık, O. (2022). Kişisel verilerin korunması kanunu kapsamında veri sorumlusu olarak Sosyal Güvenlik Kurumu. *Erciyes Üniversitesi Hukuk Fakültesi Dergisi, 17*(2), 263-362.

Kara, E. (2020). *Sigortalanabilir Menfaat İlkesi*. Yetkin.

Karadağ, H. (2021). *Sigortacılık sektöründe siber güvenlik yönetimi ve riskin azaltılmasında siber güvenlik sigortalarının rolü* [Yüksek Lisans Tezi, Marmara Üniversitesi].

Karayazgan, A. (2021). *Hukuk gözüyle siber ve sigorta* (1. bs.). Aristo.

Kaya, C. (2011). Avrupa Birliği Veri Koruma Direktifi ekseninde hassas (kişisel) veriler ve işlenmesi. *Journal of Istanbul University Law Faculty, 69*(1-2), 317-334.

Kender, R. (2015). Türkiye'de Hususi Sigorta Hukuku, Sigorta Müessesesi Sigorta Sözleşmesi (Güncelleştirilmiş 14. Baskı). İstanbul.

Keskin Uğurlu, İ. (2023). *Türkiye'de sigortacılık, sigortacılığın gelişimi, ekonomik işlevleri ve sorunları* [Yüksek lisans tezi, İstanbul Kültür Üniversitesi].

Kişisel Verilerin Korunması Kanunu. (2016, 7 Nisan). Resmi Gazete (Sayı: 29677).

Kişisel Verilerin Korunması Kurumu. (2025). *2025 yılı idari para cezaları yeniden değerleme oranları* [Resmi tebliğ]. Resmi Gazete. https://www.PDPL.gov.tr/

(Erişim tarihi: 12 Ocak 2026).

KPMG Yönetim Danışmanlığı A.Ş. (2022). Siber Güvenlik Sigortası Risk Değerlendirme Hizmetleri: Siber Tehditler ve Sigorta Çözümleri. İstanbul. www.kpmg.com.tr.

Lorenz, E. (2015). § 1. Einführung. In R. M. Beckmann & J. Matusche-Beckmann (Eds.), Versicherungsrechts-Handbuch (3rd ed., pp. 1-24). C. H. Beck.

Mercan, A. (2023). Sigorta sektöründe siber riskler. *Tokat Gaziosmanpaşa Üniversitesi Turhal Uygulamalı Bilimler Fakültesi Dergisi*, *1*(1), 43.

Oyal, A. B. (2024). Parametrik sigorta sözleşmeleri (gösterge temelli sigorta sözleşmeleri). Türk-Alman Üniversitesi Hukuk Fakültesi Dergisi, 6(2), 133-185.

Öztürk, M. S. (2018). Siber saldırılar, siber güvenlik denetimleri ve bütüncül bir denetim modeli önerisi. *Journal of Accounting and Taxation Studies*, 208-232.

Prölss, J. (2018). Prölss/Martin, Versicherungsvertragsgesetz. Rechtswissenschaft und Rechtsliteratur im 20. Jahrhundert. Verlag CH Beck.

Scheuermann, J. E. (2018). Cyber risks, systemic risks, and cyber insurance. *Penn State Law Review, 122*(3), 613-644.

Selimoğlu, S., & Altunel, M. (2019). Siber güvenlik risklerinden korunmada köprü ve katalizör olarak iç denetim. *Denetişim*, 19, 5-16.

Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ. (2013, 11 Kasım). Resmi Gazete (Sayı: 28818).

Sophos. (2025). *The state of ransomware 2025*. https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-state-of-ransomware-2025.pdf

Şağban, E. E. (2021). NFT'ler özelinde siber sigortaya bir bakış. Bilişim Hukuku Dergisi, 3(2), 430-493.

Şekeroğlu, S., & Özüdoğru, H. (2019). Dijital dönemin koruyucuları: Siber risk sigortaları. International Research Congress on Social Sciences.

Tekin, U. (2020). Hukukî açıdan siber risk sigortası. Genç Hukukçu Araştırmacılar Sempozyumu, 11-12 Ekim 2019, İstanbul, 671-683.

Türk Ceza Kanunu. (2004, 12 Ekim). Resmi Gazete (Sayı: 25611). Madde 135-138.

Türk Dil Kurumu. (2025, 10 Ocak). https://tdk.gov.tr/ adresinden alındı.

Türk Ticaret Kanunu. (2012, 14 Şubat). Resmi Gazete (Sayı: 27846). Madde 1401, 1427, 1429, 473.

Türkiye Sigorta Birliği. (2025). *Türkiye sigorta sektörü 2025 prim üretimi raporu*. https://www.tsb.org.tr/ (Erişim tarihi: 12 Ocak 2026).

Uğurlu Keskin, I. (2023). *Türkiye'de Sigortacılık, Sigortacılığın Gelişimi, Ekonomik İşlevleri ve Sorunları* [Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi].

Yüce, A. A. (2024). Siber risk sigortası: Alman siber risk sigortası genel şartları çerçevesinde bir inceleme. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 32*(3), 1611-1655.