Received: 06 April 2021 | Accepted: 01 May 2021
DOI: 10.52898/ijif.2021.1

ORIGINAL ARTICLE

Cyber Insurance - Turkish Practice

Mahmut YAVAŞİ
Elif Banu VARLI

Abstract
Cyber insurance is an integral asset to adjust market motivating forces for improving internet security. We follow the advancement of cyber insurance from customary protection approaches to early cyber risk protection approaches and to current exhaustive cyber insurance items. Cyber insurance approaches have become more comprehensive as insurers gain a better understanding of the risk landscape and job vacancies. All the more explicitly, cyber insurers are tending to some unfavorable issues such as adverse selection, asymmetric information and moral hazard that could prompt a disappointment of market solution.

Although some execution issues remain, we recommend the future advancement of cyber insurance will resolve these issues as proven by protection arrangements in other risk domains. The study has established that there is a growing need for cyber insurance in Turkey.

Keywords
Cyber risk, cyber insurance, economics of information security.

JEL Classification
G22; K24

Authors Notes:
Correspondence
Marmara University of İstanbul,
ORCID: 0000-0003-0236-2403,
yavasi@yahoo.com

Social Sciences University of Ankara,
Private Law Ph.D. Student,
ORCID: 0000-0002-8416-2079,
banu.varli@asbu.edu.tr

1. INTRODUCTION

Cyber insurance is a form of insurance designed to protect policyholders from the effects of cyber attacks such as malware, ransomware, phishing, denial-of-service attacks, contaminated drives, and unauthorized access to computer systems by outsiders, or any other approach used to compromise an organization's network/sensitive data.

As associations become more reliant on their arranged PC resources, the weaker they become to hurt from expanding continuous and harming assaults empowered by availability. Insurance from hurt on any organized PC framework won't ever be 100%. In the previous decade, assurance methods from an assortment of software engineering fields, for example, cryptography and programming have constantly made enhancements but Internet assaults keep on expanding. (Majuca, Yurcik, & Kesan, 2006, s. 1)

With the development and transformation of IT, Big information, Cloud Computing, Internet of Things and Smart Cities there has been a blast of information and more current innovations are concocted each day that will in general simplify our life. Online administrations like web based shopping, net banking, booking of taxis, instructive administrations and IT benefits our life has gotten a lot simpler however at the expense of thorough difficult work of the representatives who guarantee that the administrations run impeccably. Be that as it may, as everything has its advantages and disadvantages, so has IT. Cyber crime risk is increasing immensely in Turkey.

At this point is the lack of experience in providing assurance against cyber risk insurance for the basic problems developing markets such as Turkey. Therefore, the purpose of this study is to test the effectiveness of the Turkish insurance system, which has followed the European Union harmonization process and has successfully managed this process since 2007, in providing assurance to cyber risks.

Companies in Turkey are progressively enduring colossal misfortunes because of a rising number of digital assaults prompting interference of business and loss of client information. As a component of Business Continuity Planning for the Organization companies need to embrace Cyber-Risk Insurance as a feature of Risk Transference. Monetary area dealing with gigantic measures of Customer Personally Identifiable Information and monetary exchanges is among the high-hazard targets, however most banks in Turkey, accepting a couple of enormous private moneylenders, don't have digital danger protection.

Objective of the study is to understand about Cyber-Risk Insurance (CRI), state of adoption of CRI in Turkey, barriers to growth of CRI in Turkey and finally recommending solutions to the issues faced. The main component in the management of cyber events is understanding the risk and preventing the risk.

1.1. What is Cyber Risk?

It is the probable loss that we call risk. We measure the likelihood of a defined severity of loss occurring within a given time period to quantify risk. For example, the chances of a large US healthcare organization suffering a cyber attack that costs it $10 million or more in direct costs in the next 12 months are around 1 in 100. Its odds of experiencing a more serious incident with a higher expense, such as $100 million, are much lower: about 1 in 700. The less probable an incident is, the more serious it is. There is a continuous scale of cost from low to high, and with each degree of failure, there is a corresponding spectrum of probability, with the lowest being the most common and the highest being the least probable. (Coburn, Leverett, & Woo, 2019, s. 22)

The expanding utilization of advanced innovations in financial exercises - while making huge advantages as far as accommodation, profitability and proficiency - is likewise prompting huge dangers. Among them are "digital security risks" which, when they emerge, can upset the accomplishment of monetary and social goals by bargaining the classification, trustworthiness and accessibility of data and data frameworks. It is generally accepted that most organizations have been, will be or don't realize they have been influenced by such "cyber" episodes. Records of the recurrence and extent of (revealed) digital occurrences consistently find critical development as far as the quantities of episodes, the portion of organizations they influence, just as the effect of these episodes on organizations' tasks. The developing extent of advanced innovation in economic exercises implies that this danger is probably going to increment soon. However, the affectability around revelation of cyber episodes and restricted history of misfortune experience, the developing idea of the danger and potential for gathered misfortunes just as the expanding reconciliation of digital innovation into operational frameworks make digital danger an especially challenging risk to gauge - and manage.

(OECD, 2017, s. 11)

There is the potential for many entities to be affected in a single incident, which we call a cyber catastrophe, in addition to a significant loss to an individual organization. The threat of cyber catastrophes is a key factor in deciding how much effort we can put into reducing cyber risk as a society. While the likelihood of a catastrophe is low, the possible effects on our economy, living standards, and way of life may be devastating. It, too, spans a spectrum of magnitude, from incidents like WannaCry and NotPetya, which cost billions of dollars, to future scenarios in which cyber attacks cost trillions of dollars and destabilize our way of life.

The inexorably quick passage into cyberspace has effectively prompted a critical increase in operational risks and the risk of cyberattacks. Cybercrime has progressively become a general public-wide issue that is accepting a ton of consideration from governments across the globe. Activities around cyber insurance and the subsidizing of examination into data protection represent the difficulties around cyber risk and furthermore their significance. Further technological advancements, like the web of things, artificial intelligence, health-tech, advanced robotics and 3d-printing, for instance, will additionally increment cyber risks and lead to the rise of new and unforeseen risks. Also, with changing risks comes the requirement for better insurance. (Wieren, 2016)

Cyber risk was recognized as the danger of highest (or second-highest) concern to working together in more than 33% of OECD countries in the World Economic Forum's 2017 Global Risk Report (and among the five risk of most noteworthy worry in the greater part of OECD countries, a higher offer than either terrorist attacks or catastrophic events). (OECD, 2017, s. 11)

Insurance agencies are accustomed to managing numerous territories of vulnerability and risk. They offer inclusion for catastrophic events, business interference, and even damage from terrorist attacks; nonetheless, insurance agencies are not used to managing a considerable lot of the new occurrences of digital danger. (Siegel, et al., 2018, s. 13)

In any case, digital episodes don't just happen with high seriousness, they can likewise happen with high recurrence. In this sense, the idea of a digital episode is distinctive to that of a cataclysmic event (for example tremor). In light of numerous long stretches of perceptions and authentic records, we realize that cataclysmic events happen with a specific recurrence. For instance, the probability of having a few concurrent seismic tremors all throughout the planet is exceptionally little, however cyberattacks can happen to quite a few associations at the same time. The new WannaCry assault embodies the worldwide and unconstrained nature of a far reaching cyberattack. Encountering an assault doesn't really keep a similar organization from encountering a second assault following the first. This will rely upon the speed of distinguishing proof, investigation, and alleviations, and whether the subsequent assault focuses on the first weaknesses or new unidentified ones. While it is improbable that a solitary quake will happen all throughout the planet (in spite of the fact that zones could be influenced past the prompt tremor zone), the equivalent can't be said for a cyberattack.

Cyberattacks and other digital occasions are made by people. Assaults are generally aimed at explicit focuses considering an unmistakable result (for example benefitting from the assault, causing harm, reacting to political indications). Cyberattacks could really be incited by the conduct of focused organizations or governments. In that sense, digital danger may expect highlights of endogeneity, in this manner losing its quirk. Assaults may likewise have spontaneous ramifications. Digital danger needs to address both pernicious cyberattacks and accidental occasions brought about by machine or human disappointment. Until now, most digital occasions have been supported or abetted by people purposefully or unexpectedly. In examination, cataclysmic events are not the immediate consequence of human action. Furthermore, the normal misfortunes from numerous cataclysmic events can be preferably anticipated over cyberattacks in light of the fact that conditions and areas presented to explicit kinds of catastrophes are notable and continually checked. Verifiable cyberattack information is restricted and not well structured (except for some restricted zones like penetration/classification protection), while catastrophic events are exceptionally examined and inventoried in broad records. Digital dangers, then again, are moderately new occasions, and the current models to survey hazard and the data accessible are as yet restricted. (Siegel, et al., 2018, s. 12)

1.2. What is Cyber Liability Insurance?

Cyber liability insurance is a wide term for protection strategies that address first and third party losses because of a PC based attack or breakdown of an association's data innovation frameworks. For instance, one transporter's approach characterizes PC assaults as, "A hacking occasion or other occurrence of an unapproved individual accessing the PC framework, assault against the framework by an infection or other

malware, or a forswearing of administration attack against the insured's system." (Romanosky, Ablon, Kuehn, & Jones, s. 2)

Cyber insurance permits organizations to move a portion of the financial risk related with cyber episodes to an insurer. (Gordon, Loeb, & Sohail, 2003) It is proposed to cover business obligations, including first-party costs, and is regularly introduced as a basic segment of digital danger the executives approach inside associations. Notwithstanding, insurance agencies incorporate additional administrations for their clients that are planned to improve cyber insurance approaches inside an association. Such administrations are in light of a legitimate concern for the insurance agency, as they are planned to improve a safety net provider's danger profile. They run the array from introductory assessments of cyber insurance weaknesses and admittance to consultancies to improve their generally cyber security act, to a scope of administrations to help organizations in case of an episode. (Sullivan & Nurse, 2020, s. 4,5)

Despite the solid development of the cyber insurance market over the previous decade, protection transporters are as yet confronted with various key difficulties: how to create serious strategies that cover regular misfortunes, yet in addition prohibit dangerous occasions; how to evaluate the variety in changes across expected insureds; and how to make an interpretation of this variety into a proper estimating plan?

Since protection in the US is directed at the state level, protection transporters are needed to document notification to state protection commissions depicting each new protection item. These filings incorporate the full content of the approach (inclusion, rejections, triggers, and so forth), a security application poll, and a rate plan describing the equation for determining insurance expenses. Accordingly, these filings give a remarkable chance to see how insurance agencies comprehend and value risks, and explicitly, the business, innovation and cycle controls that are considered in a digital protection, in another defining cyber insurance, rate estimations. (Gordon, Loeb, & Sohail, 2003, s. 2)

Along these lines, some governments all throughout the planet have tried to investigate the role that cyber insurance could play in boosting better cyber safety practices. The UK's NCSC (National Cyber Security Center), for instance, as of late delivered point by point direction on how organizations should approach buying cyber insurance. (Centre, 2020) It features seven network protection addresses that organizations ought to consider prior to purchasing insurance. (Centre, 2020) However, lacking decisive examination has been led to sufficiently investigate whether digital protection creates such certain network protection results. As it is a moderately new contribution for insurance agencies, guarantors as of late have invested a lot of energy explaining what digital protection is, the thing that it does a lot not cover, and how to best form productive portfolios. A portion of those issues are canvassed in this segment. What's more, there are further inquiries concerning the reason for digital protection, how it works by and by and the remarkable difficulties it contains to turn into a completely developed protection area with high take-up. (Sullivan & Nurse, 2020, s. 5)

It is critical to take note of that cyber insurance can ordinarily be bought as either an independent cyber strategy or as a feature of a more extensive insurance bundle that oversees different risks. A devoted cyber insurance strategy is frequently more costly, yet in addition may offer more significant compensation out of cutoff points should an episode occur. (Bernard, 2020) This sort of strategy is additionally bound to incorporate the cyber risk apparatuses that are planned to improve cyber safety inside an organisation. (CISA, 2021) Meanwhile, digital protection strategies that are important for a more extensive bundle can be an appealing recommendation as far as effortlessness and affordability. (Bernard, 2020)

1.3. How US and UK Regulate Cyber Risk Insurance?

Regulatory provisions that control reporting requirements, penalty fees, and compensation to victims account for a large portion of the cost of cyber risk. Data breaches are most costly in countries with the strictest rules, with losses in highly regulated countries more than double those in countries with relaxed data control. The regulatory environment is rapidly evolving. (Coburn, Leverett, & Woo, 2019, s. 183)

The United States has been at the forefront of cyber regulation growth. As a consequence, it has been a complicated patchwork of rules. State-specific cyber breach laws have developed, with many of them being somewhat different from one another, and often even contradicting one another. Most states require reporting to the government and the media if the data breach affects more than 500 people; and some states set thresholds for the warning requirement, such as a fair basis to assume the breach would cause damage. Most states have penalties in place, and some also have legal recourse. (Coburn, Leverett, & Woo, 2019, s. 186)

There are also different applications of federal laws that vary different requirements. The Health Insurance

Portability and Accountability Act (HIPAA) of 1996 governs the privacy of personal health information, while the Gramm–Leach–Bliley Act (GLBA) governs the privacy of financial information, with differing conditions and penalty powers. (Coburn, Leverett, & Woo, 2019, s. 186,187)

The story of the computer genius kid is part of hacking mythology, and it has influenced the adoption of cyber-crime legislation in the United States. In the 1983 Hollywood film War Games, a teenage computer-games enthusiast who doesn't believe any device is fully safe breaks into a US military supercomputer designed to predict potential nuclear-weapons-of-mass-destruction outcomes and nearly starts a world war. This was harmless fun for a kid, but it was a crime for policymakers on Capitol Hill. (Coburn, Leverett, & Woo, 2019, s. 187)

The United States, like other major world forces, has a stockpile of powerful electronic arms that are delivered invisibly. Consider the Windows Eternal Blue attack, which was discovered in the Shadow Brokers' complete control in 2016. It had been an extremely effective method of infiltrating NSA-targeted PCs until it was stolen. One member of the team compared its use to dynamite fishing. Since the US government engages in covert hostile hacking operations on a regular basis in the pursuit of its public interest, its digital security must be maintained at an extremely high standard. Enactment is needed for this.

The Federal Information Security Management Act (FISMA) of 2002 was enacted to provide a basis for the feasibility of data security controls for government data frameworks, as well as to allow for the enhancement of least controls for obtaining these frameworks. The National Institute of Standards and Technology (NIST) was chosen to develop the standards and guidelines for implementing and maintaining data protection systems for the board of directors. The Federal Information System Modernization Act of 2014 is a proposed update to FISMA that would give the government a mechanism to review and ensure its data protection controls. (Coburn, Leverett, & Woo, 2019, s. 189)

The Cybersecurity Information Sharing Act (CISA) of 2015 tends to an all around perceived issue: corporate casualties of digital assaults, while regularly the best assets for significant data to forestall future assaults are reluctant to share data that may open them to common or criminal responsibility, shame, loss of trust, or serious dangers. CISA is an endeavor to lighten a considerable lot of these obstacles in order to cultivate more prominent participation and joint effort to battle digital dangers. CISA approves privately owned businesses to share cyber safety danger data for cyber insurance purposes with the central government, and with other private elements. (Coburn, Leverett, & Woo, 2019, s. 189)

The accumulation risk is one of the most difficult aspects of the cyber security landscape. There has been a lot of research done on this topic. For example, the CRO Forum's "Loss Accumulation Risks," which explores the consequences of accumulation risk, is still in its early stages. (Siegel, et al., 2018, s. 13)

Insurance firms have made accumulation risk a top priority, but many consumers are still unaware of its possible consequences. One of the main cloud providers is Amazon Web Services (AWS). Many businesses that use AWS will be impacted in the event of a hypothetical attack. Business interruption, PP&E injury, and casualties are all possible consequences. Because of the complexities of accumulation risk, it's unclear who's insurance will cover what in the event of an assault. (Siegel, at al., 2018, s. 13)

With the European Union guidelines from the 1990s, which were redesigned in the European General Data Protection Regulation of 2018, (GDPR). This greatest update of European information insurance rules in twenty years changes how organizations and public-area associations can deal with the data of clients. Indeed, organizations all throughout the planet that hold information about European residents are dependent upon GDPR. (Coburn, Leverett, & Woo, 2019, s. 190)

GDPR-affected businesses will be held more accountable for their processing of personal data. This can incorporate having information insurance approaches, leading information assurance sway appraisals, and having applicable archives on how information is handled. Under GDPR, the annihilation, misfortune, adjustment, or unapproved divulgence of, or admittance to, individuals' information must be accounted for to a country's information assurance controller. This can incorporate, however isn't restricted to, monetary misfortune, secrecy penetrates, harm to notoriety, and that's only the tip of the iceberg. (Coburn, Leverett, & Woo, 2019, s. 190) GDPR violations will result in fines of up to €20 million, or 4% of a company's annual turnover. (Coburn, Leverett, & Woo, 2019, s. 191)

The US National Association of Insurance Commissioners (NAIC) has endorsed an Insurance Data Security Model Law, which establishes industry standards for information security that will extend to a wide range of meetings, including backup plans, experts, and brokers, recognizing that digital privacy is more important now than at any point in recent memory. Associations are needed to have a composed data security program for ensuring delicate information, including episode reaction and information recuperation intended to

show their readiness for digital occasions. Organizations need to guarantee consistency yearly to their state protection officials and advise magistrates of information breaks inside 72 hours of a network safety occasion. The American Insurance Association expressed satisfaction with the adopted model legislation, stating that it was risk-based and consistent with New York's digital security law. (Coburn, Leverett, & Woo, 2019, s. 193,194)

The fundamental distinction between the U.S. furthermore, Europe is the job that guideline has played in the advancement of the digital danger market. There are two pertinent turns of events. The first, thus far generally all around cutting edge advancement, concerns the treatment of digital episodes in the corporate area (counting monetary administrations) and the assurance of purchasers as for the security and respectability of information put away in the internet. The second identifies with the guideline of guarantors as suppliers of hazard answers for their clients. This administrative improvement is as yet in its earliest stages. (Siegel, et al., 2018, s. 15)

The legal landscape around cyber risk is still incomprehensible and unpredictable. Across the globe, administrators, regulators, and courts are creating new rules and points of reference for identifying cyber danger on a responsive premise. This has resulted in a tangle of rules, guidelines, case law, litigation trends, and a climate that makes it difficult to estimate potential costs that could arise from the inevitable digital misfortunes. The legal environment around digital threats is currently incoherent and uncertain. A company that is the victim of a successful cyber attack may be liable to its customers for breach of contract. Companies can face aggressive lawsuits if, as a result of an attack and the ensuing disruption, they fail to meet legally binding obligations insignificant cyber security. (Coburn, Leverett, & Woo, 2019, s. 195)

Cyber insurers have a competitive incentive to reduce the number of cyber accidents and minimize the effects of events in order to restrict the amount they would pay out to customers. Although most businesses consider cyber events to be a low-probability, high-impact occurrence, research shows that cyber insurers deal with them on a daily basis as part of their business model. (HM Government, 2015, s. 3) As a result, cyber insurers can assist in the identification of specific experts who can help reduce risk. (Woods & Moore, 2020)

Cyber insurance, according to some researchers, allows enterprises to evaluate their cyber risk exposure. (OECD, 2017, s. 7) Cyber insurers, for example, can help raise risk management awareness by establishing consistent benchmarks for businesses looking to enhance their cyber security. (OECD, 2017, s. 7) Insurance firms may also help businesses understand their exposure and assist them by evaluating the risks they pose on a regular basis. (Estlin, Saluja, Greensmith, & Tuplin , 2019, s. 12) The experience and knowledge that cyber insurance firms have will help people learn more about risk reduction strategies. (Sullivan & Nurse, 2020, s. 19)

1.4. Why Do We Need Cyber Liability Insurance - Turkey Practice?

Turkey suffered most cyber attacks across the country in 9th place while the IRA, cyber attacks are occurring in the world 556 million years. It is stated that cyber attacks increase by 50% every year. In addition, the cost of cybercrime to the global economy is 445 billion USD annually. Turkey was the victim of more than 10 million people and it is estimated that the total net cost to be 556 million USD. (Altuntaş, Kara, Soylu, & Kırkbeşoğlu, 2018, s. 10)

Cyber attacks have reached such a point today that both public institutions and private companies have become the biggest nightmare. According to researchers, the number of cyber attacks in our country in the first three months of 2017 has increased by 50% compared to the first three months of last year. In our country, an average of 75 thousand cyber attacks occur daily and this number is increasing at an increasing rate. Number of cyber attacks in Turkey, 5th in the world, and ranks 4th in Europe. When looking at the types of cyber attacks, data leakage attempts are 40% and Trojan horse attacks are around 30%. Universities and the Ministry of National Education take the lead when looking at where the most cyber attacks are made. These serious numbers actually make the importance of cyber risks even more remarkable. (Altuntaş, Kara, Soylu, & Kırkbeşoğlu, 2018, s. 10)

First time in Turkey in 2010, it has emerged that there is a need for cyber risk insurance. While in Turkey the first time against the demand for this insurance coverage overseas markets, after 2012 some Turkey offices of global firms began to offer such a guarantee. Thus, the insurance company in Turkey since 2012, began offering coverage in the country. The concept of cyber risks in Turkey, only "data loss" is limited to events considering that, once in place it should be understood that the damage was the result of a much

more comprehensive cyber risks and insurance coverage. With the increase in attacks and increased awareness, many companies have accelerated their efforts in this regard. As the first step of these studies, they made expansion in specifications and guarantees. (Altuntaş, Kara, Soylu, & Kırkbeşoğlu, 2018, s. 12)

There are many types of attacks for cyber risk. The five most common types of cyber attacks in Turkey are as follows: Ransom software, phishing attacks, credit card fraud, DOS / DDOS attacks, mobile threats. (Altuntaş, Kara, Soylu, & Kırkbeşoğlu, 2018, s. 10)

In the latest incident has occurred on the 25th March 2021. Following the cyber attack on Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik AŞ, which was stated by the Personal Data Protection Board (KVKK), which affected 21 million 504 thousand 83 people, an investigation was initiated for data breach. The Information Technologies and Communication Authority (BTK) managed to seize the IP addresses that carried out cyber attacks on Yemeksepeti. In addition, the authorities, who directly contact the companies at risk, also provide information about the measures that can be taken within the institution.

The most important feature that distinguishes cyber risk insurance from other insurers is not the deletion of data, loss or theft. Because data to be damaged in cyber risk insurance is not insured. Data has no monetary value in cyber risk insurance. The request of the third parties arising from the loss of the insured data is insured. Another feature that makes cyber risk insurance different from other insurances is the difficulty in predicting the actual risk as an effect. Because when the damage occurs, it is very difficult to measure this damage. Due to all these complex and difficult determinations, it is not easy for insurers to easily popularize their products in this field and to offer affordable policies to their customers. There is no package policy specified in cyber risk insurance. Therefore, policies with additional coverage are prepared according to the demands and needs of each insured. Cyber risk liability policies cover many risks associated with electronic data and internet use.

Cyber risk insurance can be divided into two as individual cyber risk insurance and commercial cyber risk insurance for the person covered. Under the individual cyber risk insurance coverage; legal counseling service, identity theft, damage to online reputation, online shopping disputes, theft or fraudulent use of payment instruments. In commercial cyber risk insurance; defenses against the public authority and fines, data protection damage of the insurant, cyber ransom damage, information security and confidentiality responsibility, data breach costs, and interruption of work by the insurant are covered.

Another point to be considered here is the issue of taking necessary precautions. Just as traffic insurance does not provide coverage in case of drunk driving and specifies this in its terms, it is necessary to take necessary and certain level security measures in cyber risk insurance. (Çotak, 2019, s. 20)

CONCLUSION

In both contexts result in semi-structured interviews conducted between risk perception and risk assessment perspective of Turkey and the EU insurance companies have been observed that there are huge differences. However, the awareness of businesses related to the potential problems created by cyber risks in Turkey differs from the EU. Although the development of cyber applications in our country is in parallel with developed countries, it has been observed that the awareness and risk perception regarding the risks that will arise as a result of these cyber applications are still at a low level. It can be said that cyber risks also take their share from the relatively low individual risk perception in our country. It is clear that the low risk perception will create some restrictions for insurers to offer coverage for such risks. Risk management or protection from possible damages and taking precautions depends primarily on the development of the insured's awareness and risk awareness. Therefore, as long as risk awareness is not created socially, it will be difficult for insurers to ensure that cyber insurances are sustainable. In other words, cyber insurance sales are far from being a common practice in our country.

According to statistics, attackers continue to access the target system for 299 days without interruption as a result of a successful cyber attack. In other words, institutions can recognize or prevent them after an average of 299 days.

Bank accounts, e-mail addresses and passwords used in every online transaction are opportunities for cybercriminals. In recent years, global crises have occurred with hackers breaking the passwords of public institutions' servers, mobile banking passwords of individual users and even game console passwords.

According to statistics, 91 percent of attacks against internet users are carried out through phishing emails. The most important of these is ransomware that harms both individual users and companies. In attacks carried out with ransomware, which is the most preferred by cybercriminals to make money, criminals de-

mand to decrypt the password for money by encrypting the sensitive files they find on the network and / or the relevant device.

When insurance companies in terms of awareness and efforts in providing their cyber security compared to the EU and Turkey, significant investments in this regard the EU is seen that the insurer did. Most of the EU insurance companies direct 8-12% of their IT investments to security investments. (O'Connor, 2017) No matter how good the cyber security software and firewalls of insurance companies are, security will not be fully ensured if IT workers have insufficient knowledge, skills and awareness. (O'Connor, 2017)

Cyber insurance companies are of great importance in terms of protecting personal data. Therefore, it is equally important for companies to take precautions against possible cyber attacks today. Although insurance companies do not have serious infrastructure, security and education investments of these dimensions in our country, it is seen that awareness regarding the correct direction of these investments is developing in the future. Although best practices in risk analysis processes differ, the problems are similar between the EU and Turkey. However, the extent to which these common problems occur can be further clarified in future studies with the help of quantitative methods, and their levels and effects can be revealed more concretely.

Education is of great importance in protecting individuals from cyber attacks. Regardless of size, industry and geography, cybercrime knows no boundaries. Educating users and increasing their awareness will enable them to recognize and prevent cyber risks and protect themselves against cyber attacks. Considering that internet usage is down to the age of 9, adding cyber security-related courses to the school curriculum may contribute to the measure. As the world evolves into a huge digital age, we need to determine cyber security-related measures from the beginning.

REFERENCES

Altuntaş, E., Kara, E., Soylu, A. B., & Kırkbeşoğlu, E. (2018). Cyber Insurance: Recent Developments, Implementations and Challenges. Journal of Banking and Insurance Research, 8-22.

Bernard, J. (2020, March 16). Overcoming challenges to cyber insurance growth Expanding stand-alone policy adoption among middle market businesses. Deloitte: https://www2.deloitte.com/us/en/insights/industry/financial-services/cyber-insurance-market-growth.html

Centre, N. C. (2020, August 6). Cyber Insurance Guidance.

CISA. (2021, march 28). CYBERSECURITY INSURANCE. https://www.cisa.gov/cybersecurity-insurance adresinden alındı

Coburn, A., Leverett, E., & Woo, G. (2019). Solving Cyber Risk Protecting Your Company and Society. Wiley.

Çotak, A. (2019). CYBER SECURITY INSURANCE SECTOR, THE INVESTIGATION OF DEVELOPMENTS IN TURKEY AND THE WORLD. Unpublished Master's Thesis.

Estlin , A. P., Saluja, S., Greensmith, P., & Tuplin , J. (2019). The Global Future of Cyber Insurance and the London Market's Pivotal Role . THE GLOBAL FUTURE OF CYBER INSURANCE, 1-20.

Forum, C. (tarih yok). Casualty Accumulation Risk . https://www.thecroforum.org/wp-content/uploads/2015/10/CROF-Casualty-Accumulation-Risk-FINALv11-2.pdf

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A Framework For Using Insurance For Cyber-Risk Management. Communications of the ACM, 81-85.

HM Government. (2015). UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk. UK.

Majuca, R., Yurcik, W., & Kesan, J. P. (2006). The Evolution of Cyber Insurance. University of Illinois at Urbana-Champaign, 1-16.

O'Connor, A. (2017, November 15). 5 Ways the Insurance Industry Can Improve Cybersecurity: Former U.S. Security Chief Clarke. https://www.insurancejournal.com/news/national/2017/11/15/471130.htm.

OECD. (2017). Enhancing The Role of Insurance in Cyber Risk Management.

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (tarih yok). Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk? 1-40.

Siegel, M., Bartol,, N., Pulido, J., Madnick, S., Coden, M., Jalali, M., & Bernaski, M. (2018). Cyber Insurance as a Risk. The Geneva Association, 1-33.

Sullivan, J., & Nurse, J. R. (2020). EMERGING INSIGHTS Cyber Security Incentives and the Role of Cyber Insurance . Royal United Services Institute for Defence and Security Studies, 1-20.

Wieren, M. v. (2016). Cyber insurance: What you need to know, and how to seize the opportunities. Netherlands.

Woods, D. W., & Moore, T. (2020, 1). Does Insurance Have a Future in Governing Cybersecurity? Security and Privacy, s. 21-27.

How to cite this article: Yavaşi, M. & Varlı, E.B. (2021). Cyber Insurance - Turkish Practice. International Journal of Insurance and Finance, 1(1), 1-8. https://doi.org/10.52898/ijif.2021.1