Global Journal of Computer Sciences: Theory and Research

Volume 13, Issue 1, (2023) 46-58 www.gjcs.eu

# Corporate Cyber Security in Turkey Investigation Of Legal and Corporate Infrastructure : A Meta-Synthesis Study

Ezgi Pelin YILDIZ [a] *, Computer Technology Department, Kafkas University, Kars, Türkiye.
Oguzhan Simsekler [b], Management Information System, Kafkas University, Kars Türkiye.

**Suggested Citation:**

Yıldız, E., P. & Simsekler, O. (2023). Corporate Cyber Security In Turkey Investigation Of Legal And Corporate Infrastructure : A Meta-Synthesis Study. *13*(1), 46-58. https://doi.org/10.18844/gjcs.v13i1.8858

Received from; October 23, 2022, revised from; December 21, 2022 and accepted from February 09.
Selection and peer review under responsibility of Assoc. Prof. Dr. Ezgi Pelin YILDIZ, Kafkas University, Turkey.

## Abstract

Network technologies, which were created to serve military activities in the early days, have gained a civilized concept structure after the cold war period. In this context, the opening of internet technologies to civilian use has also made the use of information networks widespread. The spread of information networks has accelerated the information transformation in the social, commercial, military and cultural fields on a global scale. As an effect of this transformation, individuals and institutions perform almost all of their data storage, data transfer, instant communication and service provision in cyberspace. Although this situation creates advantages in terms of time, cost and energy, it has also brought important risks and security gaps due to the emergence of many attack methods, especially data theft, for cyber security. In parallel with this result, cyber attack methods have increased rapidly over time due to the rapid movement brought about by technological developments and have become a much larger, complicated and difficult to notice structure. Cyber security mechanisms developed to defend against attacks that seriously threaten personal data, such as cyber attacks, are also dynamic, just like cyber attacks. Today, it has become a necessity for every institution to develop and implement effective cyber security methods in order to be protected from cyber attacks and threats by structuring their own information systems in digital environments and to ensure the information and data security they have. Such unstoppable developments in technology result in the emergence of new types of threats to cyber security, just as it has been up to now. In this context, the sustainability and operability of cyber security mechanisms are essential. In the light of all this information, in this study, especially in the corporate field, the methods of activity that threaten cyber security, as well as legal and institutional infrastructures are discussed and the level of current cyber security awareness is tried to be determined. As the application dimension of the research, the format and standards determined by the Presidency Digital Transformation Office in military institutions and EYP-2.0 (Electronic Transformation) in the system in the background Correspondence Package) package examined and a demo of the relevant package program has been created. In addition to these issues, the methods that can be developed within the framework of cyber attacks and defense against these attacks are evaluated. It is foreseen that the study will contribute to the literature in this context and will be a useful resource for institutions and organizations in terms of gaining the functionality and sustainability of cyber security mechanisms.

**Keywords:** Corporate Cyber Security, Legal and Institutional Infrastructures, Risk and Vulnerabilities, Cyber Security Mechanisms.

* ADDRESS FOR CORRESPONDENCE: Ezgi Pelin YILDIZ*, Computer Technology Department, Kafkas University, Kars, Türkiye. *E-mail address*: yildizezgipelin@kafkas.edu.tr / Tel.: +0474 225 11 50

## Introduction

The Industrial Age, the first traces of which date back to the Middle Ages and lasted throughout the 19th century with the industrial revolution, left its place to the information age in the 20th century (Demirdögen, 2021; Unver et al. 2011). The borders and distances between countries have disappeared over time with the advancement of the internet and technology. As a result of the establishment of internet networks and the use of communication satellite systems; the information revolution, which takes its power from information, information processing and communication technologies, has left its mark on the 21st century (Karagün & Aras, 2022).

In the light of important technological developments after the information revolution, the possibility of encountering threats against information security and privacy has increased with the existence of the internet in almost every field today (Darılıcı, 2017). Along with the alarming current and possible increase in cyber security breaches, the necessity of taking precautions against the material and personal damages caused by these increases has come to the fore frequently. Because today, the security of electronic systems and the data stored there has become at least as important as the security of geographical borders (Gencoglu, 2021).

Cyber attack or, in other words, cyber security breach; it is expressed as attempts to eliminate the confidentiality, integrity and accessibility of the data within the information systems with the person/persons or information systems existing in the cyber space (Karasoy & Babaoğlu, 2021; Alway, 2018). The fact that institutions now store all their data electronically; it is clear that irreversible damages will occur unless necessary precautions are taken regarding cyber security against threats encountered in many areas from the breach of personal data to the security of important commercial and system secrets with the personnel working within the institution (Yıldız & Younes Gejam, 2022).

Cyberspace is also referred to as the "fifth dimension", which is a digital space created by human-made and integrated network technologies (Darılıcı, 2017). It is expressed as the sum of many software and hardware elements such as the Internet, communication networks, military networks closed to the outside world, power lines networks, facilities with software infrastructure for mobile phones, electronic command systems, satellite systems, unmanned aerial vehicle systems (Akyazı, 2013; Darılıcı, 2017 & Güngör, 2021). All activities related to cyber security take place in this field.

Cyber security is the whole activity and process of protecting all digital data, especially the assets, computers, servers, mobile devices, electronic systems and communication methods, networks, digital information, accounts, files and photos of institutions, organizations and users, from malicious attacks in cyber environments (Unver vd., 2011; Karasoy & Babaoğlu, 2021). All of the tools, plans, policies, security guarantees, methods and guidelines, risk management studies, trainings and practices used within the framework of these protection activities are considered within the scope of cyber security activities (Unver et al., 2011).

According to the 2022 World Economic Forum (WEF) Global Risks Report; With COVID-19, the dependency on technological systems has increased, with most of the workers shifting to remote work. At the same time, cybersecurity threats have grown (in 2020, malware and ransomware attacks have increased by 358% and 435%, respectively) and preventive activities have lagged, mainly due to the scarcity of cybersecurity professionals and fragmented governance mechanisms. According to the results of the 2021-2022 Global Risks Perception Survey; “cybersecurity issues” ranks 7th in the global risk perception with 12.4%, and the current status of risk reduction studies in the fields of “cross-border cyber attacks and mesenformation” is evaluated by most of the participants as “not yet started” or “in the early development stage”, that is, insufficient. (WEF Global Risks Report, 2022).

Main principles of generally accepted information security and cyber security; confidentiality, which is expressed as the protection of information from unauthorized access, ensuring the integrity that is violated by unintentional erroneous actions or maliciously changing or damaging information, accessibility which means that authorized users can access information without any interference or obstruction, accountability provided by keeping track of the transactions of the users of the system in order to identify the responsible for the damage when necessary, it can be explained as originality, reliability and auditability, which are important in terms of preserving the initial state of information (Güngör, 2021; Whitman & Mattory, 2017).

If the main causes of corporate cyber security inadequacy are discussed, the order of the relevant items is; the cost of the software and information required for cyber attacks is low and easily accessible, the lack of attention to security vulnerabilities, the openness of cyber space to uninterrupted communication and access, the fact that services and services that reach large masses and are frequently used are mostly provided by information systems, critical infrastructures of institutions are Being connected to the internet, the majority of internet users are insufficient in terms of cyber security awareness, lack of cooperation between institutions, the tendency of companies to hide the attacks against them due to the fear of loss of reputation and market due to the risks of significant reputational damage before solving them, the information security management in the institutions is not at an adequate level, It can be evaluated under the headings such as the lack of competent personnel, the weak configuration of the institutions, the inadequacy of cyber security audits and the inadequacy of secure production at the point of hardware and software (Chakraborty, 2020; Yıldız & Younes Gejam, 2022; Cakır & Yasar, 2015 ).

Many institutions and organizations have been assigned to cyber security in Turkey until today. Some of these are listed as the functions of generating ideas on how to strengthen the defense line of the country, some of them developing technological capacity in line with these ideas, and others of eliminating threats by fighting on the battlefield in the cyber space. The main ones of these institutions are; TÜBİTAK and its subsidiaries are Information Technologies and Communications Authority (BTK), Disaster and Emergency Management Presidency (AFAD), Presidency Digital Transformation Office and Ministry of Transport and Infrastructure (Karasoy & Babaoğlu, 2021).

As a result of all these vulnerabilities expressed, the methods of combating the cyber threats faced by the institutions; it can be considered under two main headings as technological and non-technological. Technological struggle methods; it is classified as providing hardware, software and network security. Non-technological methods of struggle are; acting within the framework of clear rules and guidelines created in accordance with the framework and the purpose of the organization, establishment of procedure and control components containing the steps on how to implement the cyber security policies and rules created with the participation of corporate senior management, existence of defense organizations trying to increase internet security and stability ( Gencoglu, 2021), in the event of a cyber security threat, accurate reporting by making risk analyzes, effective corporate communication, determining the right combat tools and methods accompanied by an effective action plan, comprehensive encryption support, supporting legal regulations and academic studies in this field, and It can be classified as assimilation and increasing awareness of the cyber security threat (Bozgeyik, 2021; Richard & Nurse, 2020; Chakraborty et al., 2020).

Implementing these solutions properly and consistently requires significant time, resources and costs; however, it should be kept in mind that these losses will be quite insignificant compared to the damages that may arise otherwise. The faster a cyberattack can be detected and contained, the lower the expected cost of the attack. (Krishan, 2018).

## 2. RELATED RESEARCH

Considering the studies conducted in Turkey within the scope of corporate cyber security, the existence of the following studies has drawn attention as a result of the literature review;

Cakır & Yasar (2015), have discussed the Threats and Measures to Corporate Cyber Security in their studies. In this study, it is presented (in a general framework) what can be done on an institutional basis against increasing and more complex cyber threats. Data collection methods such as interviews and document analysis were used in the study, which aims to help institutions in Turkey to protect their corporate cyber security against cyber threats. As a result of the study, it has been determined that there is not enough awareness about corporate cyber security. In addition, it was emphasized that an effective and robust process should be carried out as a result of the basic steps to increase corporate cyber security, which aims at the confidentiality, integrity and accessibility of data.

Karasoy, Babaoğlu (2021), presented their research titled Cyber Securıty In Turkey: Legal And Instıtutıonal Infrastructure. Within the scope of this study, cyber security studies in Turkey are discussed in the context of legislation and institutional structures. First of all, the studies in this field and their legal dimensions were evaluated, and then the responsible institutions were examined. Suggestions have been developed with the inferences to be made from the legal and institutional infrastructure. At the end of the research, legal regulations related to cyber security in Turkey, especially Electronic Communication Law; it has been determined that all kinds of laws are partly included in it. In this context, a proposal has been developed that Turkey needs an exclusive law on cyber security. It was emphasized that a holistic approach should be abandoned in the evaluation of the country's critical infrastructures immediately after the entry into force of the general law on cyber security, and it was emphasized that there should be different legal regulations regulating the procedures and principles of protection of each critical infrastructure sector against cyber threats.

### 2.1. Purpose of the research :

The aim of this study; To evaluate the cyber security threats in a general framework by increasing the awareness of the institutions against cyber threats and to determine the precautions and sanctions to be taken in order to ensure corporate cyber security. The basic questions that need to be answered in order to achieve this goal are:

- What are the benefits protected in corporate cybersecurity?
- What are the cyber threats and attacks on corporate cybersecurity?
- How can protection be provided against threats and attacks on corporate cybersecurity?
- In which areas can threats and attacks on corporate cybersecurity be combated?
- What are the consequences if corporate cybersecurity is not managed properly?

In addition as the application dimension of the research, the format and standards determined by the Presidency Digital Transformation Office in military institutions and EYP-2.0 (Electronic Transformation) in the system in the background Correspondence Package) package examined and a demo of the relevant package program has been created.

### 2.2. Important of the research :

The main contribution of this study on corporate cyber security to the literature is; It is anticipated that the methods of combating cyber security threats identified in this study can be closely followed by relevant institutions and that cyber threats and attacks are increasing day by day, thus contributing to future research and researchers.

## 3. RESEARCH METHOD

This research is a meta-synthesis study. Meta-synthesis studies are the qualitative findings of studies conducted in a particular field; these are studies that aim to interpret, evaluate, reveal similar and different aspects and make new inferences (Polat & Ay, 2016). In this research, corporate cyber security was conceptually discussed within the scope of meta-synthesis research method, quantitative and qualitative findings of the studies carried out within the scope of the related subject were evaluated, and in this context, new inferences were made on the subject. As the application dimension of the research, the format and standards determined by the Presidency Digital Transformation Office in military institutions and EYP-2.0 (Electronic Transformation) in the system in the background Correspondence Package) package examined and a demo of the relevant package program has been created.

## 4. FINDINGS

In the research, sub-objectives were answered within the scope of meta-synthesis research method. Accordingly;

Within the scope of protected benefit in corporate cybersecurity; benefits protected in cyber attack; data loss prevention, detecting data breaches, incident response, threat analysis, data analysis and threat intelligence sharing. In terms of Data Loss Prevention; a cyber threat intelligence system can monitor communication attempts with malicious IPs and domain domains, and detect possible phishing attacks against employees. Collecting and analyzing these data can be a precautionary measure for the same situations. Within the scope of Detecting Data Breaches; detection of data breaches and leaks is a precaution against both financial losses and loss of reputation of the institution. In terms of Incident Response; the information on which devices the data loss or leak is/is taking place helps to identify compromised systems. In this way, the measures to be taken in order to prevent the same violations can be structured more consciously. The threat analysis; gives an idea about the necessary defense mechanisms and the measures that can be taken. The aim is to understand the techniques, tactics and procedures of the attackers and to offer the right solutions to the points that may pose a threat. Data analysis; analyzing the collected data helps to obtain additional information against the threats that attackers have created / may create. The last dimension threat intelligence sharing; is the sharing of the threatening data obtained by the institutions with other institutions. Purpose; to assist in the development of countermeasures used against targeted attacks. Information sharing between communities is vital, as it is nearly impossible to individually combat emerging threats.

Within the scope of the cyber threats and attacks on corporate cybersecurity; making security a priority is a must to protect assets from the many cyber threats that exist today. Common cyber threats include: Malware: A program or file designed to harm a user's computer. Examples include computer viruses, spyware, trojans, and worms. Ransomware: Malware in which the attacker locks the victim's computer (usually with an encryption method) and demands a ransom to decrypt and unlock the victim's computer. Social Engineering: it is a form of attack carried out by using people to achieve the goal. Phishing: A type of scam in which fake emails are sent that appear to be genuine and appear to be from reputable sources. Positive responses to these fraudulent emails result in stolen personal data, including login and banking information. For example, a fake email that appears to have come from social media saying that our account has been stolen and asking you to log in to recover it.

Within the scope of protection be provided against threats and attacks on corporate cybersecurity; the cybersecurity framework is a system of standards, guidelines, and best practices for managing risks emerging in the digital world. In this context many organizations must comply with a mix of government-mandated, industry-specific and international cybersecurity regulations. For example, a business wishing to process credit card transactions must undergo an audit that certifies compliance with the Payment Card Industry Data Security Standards (PCI DSS) framework. On the other hand, there are frameworks that do not have to comply, but provide cyber security measures when implemented. The standards and frameworks directly or indirectly related to cyber security are not limited to those here (For example, COBIT, HIPAA, SOC2, FISMA, GDPR, KVKK, NIST, ISO etc.) but can give an idea. As needed, CIS Benchmark documents, #Cloud Control Matrix document, ISO 27017 implementation standard for ISO/IEC 27002 based information security controls in Cloud services, #OWASP Security documents, #NIST Special Publication 800-53 Security for Information Systems and Enterprises and # It would be helpful to review the Privacy Controls document, NIST Special Publication 800-82 Industrial Control Systems Security Manual, and NIST Special Publication 800-125 Security Guide for Virtualization Technologies. The American National Institute of Standards and Technology (NIST) offers many standards and frameworks for information security and cybersecurity. Only one of these, the “Critical Infrastructure Cyber Security Development Framework” was created in collaboration between industry and government. The framework provides an approach based on existing standards, guidelines and practices to mitigate cyber risks to critical infrastructure. But its principles can also apply to any organization seeking better security. Cyber Security Framework consists of three main components; Framework Core, Implementation Tiers, Profiles. The Framework Core is divided into 5 main functions (Define, Protect, Detect, Intervene, Recover) and consists of 23 categories and 108 sub-categories. Application Tiers are designed to take an inventory of the organization's cybersecurity risk management practices and develop plans to improve the organization's cybersecurity posture. Framework Profiles are the alignment of desired outcomes in the Framework Core section with the organization's own organizational requirements, objectives, risk appetite, and resources. Profiles are primarily used in an organization to identify and prioritize opportunities to improve cybersecurity. For this, the current profile and the target profile are compared.

Within the scope of areas can threats and attacks on corporate cybersecurity be combated; when some important statistics about cyber threats are examined; Issues or events that compromise the security of IoT were reported by 61% of organizations 92% of all malware is transmitted via email. Security problems in industrial control systems (SCADA) affected 54% of organizations. Ransomware attacks cost organizations an average of $5 million. Crypto mining is dependent on 90% of RCE (remote code execution) attacks. Compromised attacks were 77% undocumented in 2017. Data breaches are identified by organizations after an average of 191 days. According to 56% of corporate cybersecurity chiefs, their top security concern is targeted phishing attacks.

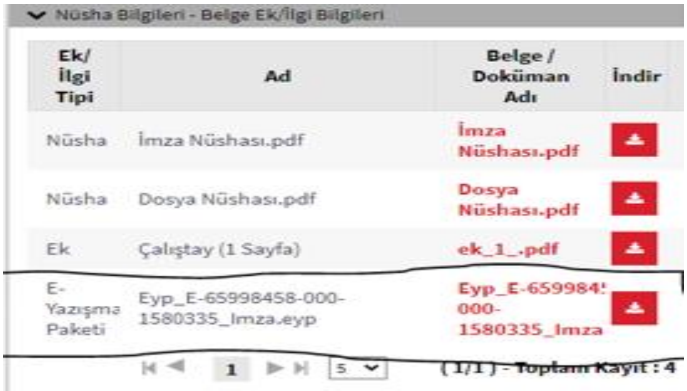
Within the scope of the consequences if corporate cybersecurity is not managed properly; today, as technologies develop, it is expected that the types of threats that can be encountered will decrease, but unfortunately, there is an increase in attacks. For today, hundreds of thousands of attack types, over billions of malware, tens of thousands of cyberweapon tools, over a hundred thousand new attacks every year, and nearly a hundred advanced persistent attack approaches, etc. exists. If the defense mechanisms are not managed properly to protect against these attacks and threats, institutions and organizations may experience APT, spyware infiltration, use of open ports, TCP/IP hacking, viruses, spyware, malware, mass e-mails, worms, phishing or phishing. Users will be exposed to attacks and threats such as botnets, social engineering attacks, artificial intelligence attack tools.

## Electronic Signature Demo Study :

Electronic signature is defined as electronic data added to another electronic data or logically linked to electronic data and used for authentication purposes. With the widespread use of e-signature and e-government structure, the relations of the state with the citizen, the citizen with the state, the citizen with the citizen and the state with the state will be transferred to the electronic environment and create a secure communication channel. With the identification of state units and institutions, the private sector and individuals in electronic environment, our lives will become easier and perhaps more livable (Sagıroglu & Alkan, 2018).

One of the important measures of cyber security is integrity and originality. While the efforts of data owners to prevent data from being changed beyond their control and wishes are considered as protecting the integrity of the data; authenticity refers to the proof of the source of information. An electronically signed document can be seized by cyber hackers before it reaches its intended destination, impersonating the owner of the document and creating a crime by changing the attachment of the document. Example: Transmitting the document in which the information of a military operation is sent to the unit that will carry out the operation, in the changed form, after the location information to be operated is changed. In an example of a study conducted by local institutions in order to determine the data authenticity and to ensure cyber security by checking the compliance of the relevant data with the integrity principle.

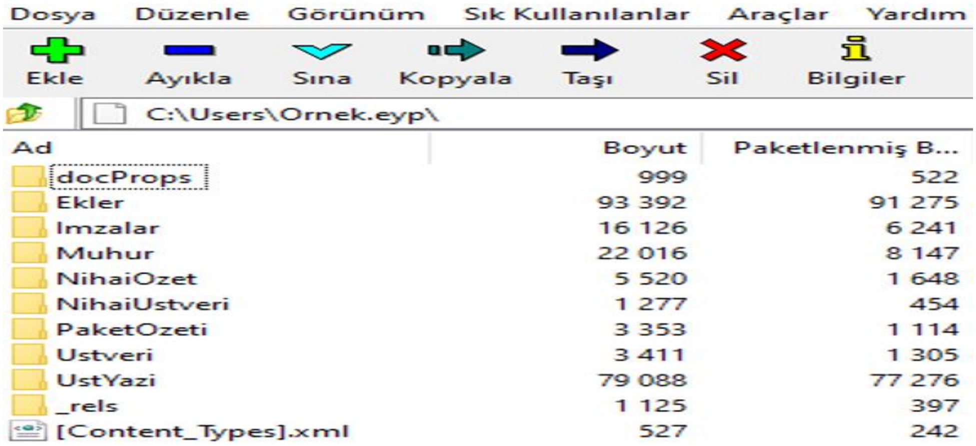
With the electronic signature of the document, the EYP-2.0 (Electronic Correspondence Package) package is created in the system in the background with the format and standards determined by the Presidency Digital Transformation Office (see Figure 1).



| Ek/ İlgi Tipi | Ad | Belge / Doküman Adı | İndir |
|---|---|---|---|
| Nüsha | İmza Nüshası.pdf | İmza Nüshası.pdf | |
| Nüsha | Dosya Nüshası.pdf | Dosya Nüshası.pdf | |
| Ek | Çalıştay (1 Sayfa) | ek_1_.pdf | |
| E-Yazışma Paketi | Eyp_E-65998458-000-1580335_Imza.eyp | Eyp_E-659984! 000-1580335_Imza | |

Figure 1. Presidency Digital Transformation Office

After the EYP-2.0 package, which was seized by unauthorized persons, is captured, the package is opened by the hackers through compression applications (see Figure 2 ).

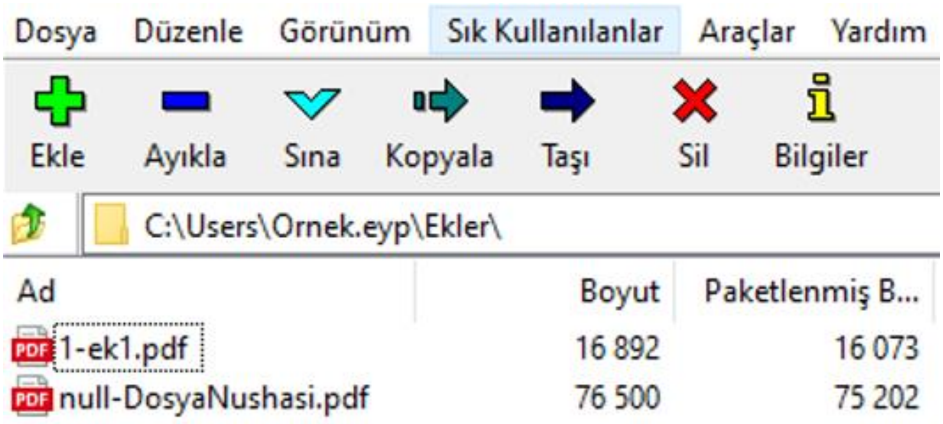


C:\Users\Ornek.eyp\

| Ad | Boyut | Paketlenmiş B... |
|---|---|---|
| docProps | 999 | 522 |
| Ekler | 93 392 | 91 275 |
| Imzalar | 16 126 | 6 241 |
| Muhur | 22 016 | 8 147 |
| NihaiOzet | 5 520 | 1 648 |
| NihaiUstveri | 1 277 | 454 |
| PaketOzeti | 3 353 | 1 114 |
| Ustveri | 3 411 | 1 305 |
| UstYazi | 79 088 | 77 276 |
| _rels | 1 125 | 397 |
| [Content_Types].xml | 527 | 242 |

Figure 2. Compression Applications

The attachments folder in the opened package opens (see Figure 2 ).

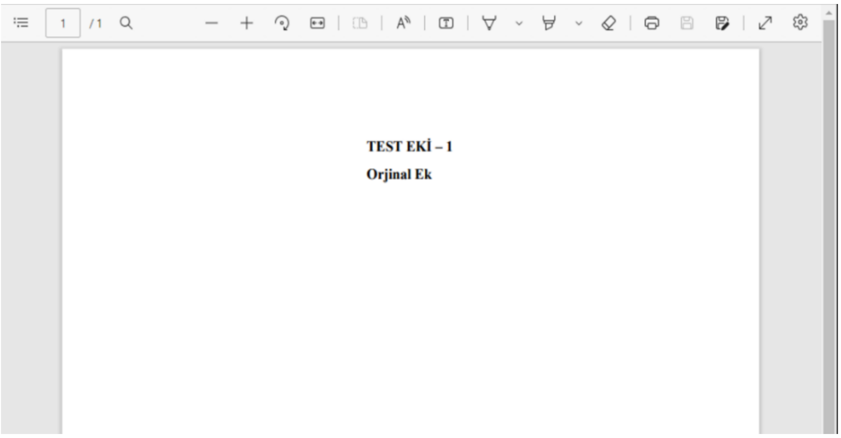


C:\Users\Ornek.eyp\Ekler\

| Ad | Boyut | Paketlenmiş B... |
|---|---|---|
| 1-ek1.pdf | 16 892 | 16 073 |
| null-DosyaNushasi.pdf | 76 500 | 75 202 |

Figure 3. Opened Packge

After unpacking the document named annex 1 in the folder, it is opened by cyber hackers with the appropriate application (see Figure 4).

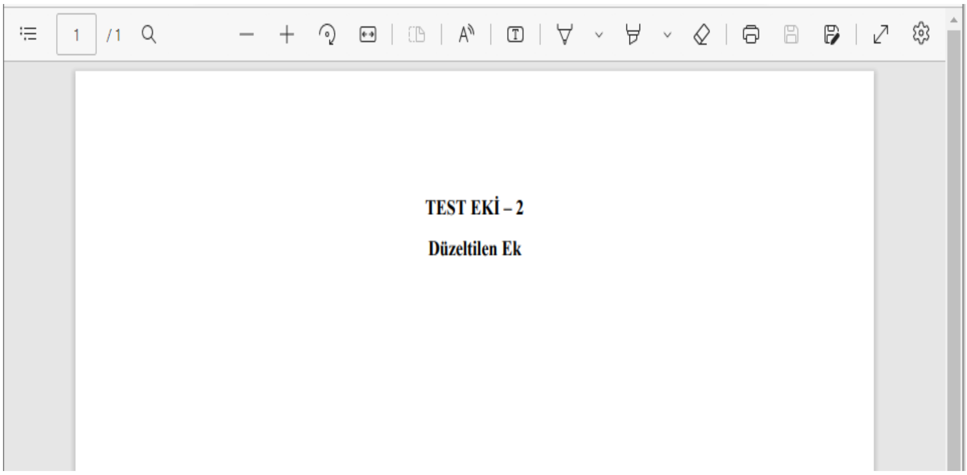


**TEST EKİ – 1**

**Orjinal Ek**

Figure 4. Cyber Hackers with the Appropriate Application

After the original Supplement has been manipulated, it is put back into the package. (see Figure 5)



**TEST EKİ – 2**

**Düzeltilen Ek**

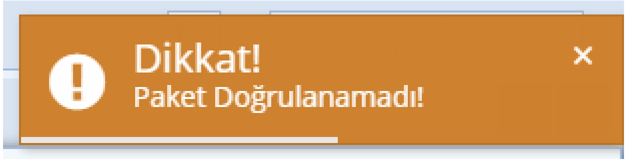
Figure 5. Put Back Into The Package

If the document, whose integrity and originality is damaged by unauthorized and confidential changes, is requested to be forwarded to the recipient as if it were original;

a) When the document is sent to the recipient, when the document is requested to be sent over the PTT's KEP system, since the package is checked through the APIs offered by TÜBİTAK, as a result of this control, it becomes clear that it is different from the original version of the EYP, and therefore the document is not transmitted by the PTT.

b) In the event that the EYP is transmitted in a different way other than the PTT's KEP system; When the forwarded EYP package is tried to be uploaded to any EBYS (Electronic Document Management System) that uses the APIs offered by TÜBİTAK, it is observed that the package is

c) not opened because the EYP cannot be verified. (see Figure 6).



Dikkat!
Paket Doğrulanamadı!

Figure 6. Packed Confirmation

## 5. RESULT and SUGGESTIONS

Cyber security; it is defined as the protection of the security, integrity and confidentiality of our communication, life, integration, tangible or intangible assets, and even our data in electronic environment, that we establish in information systems between people or institutions. In addition, it is a set of activities that include the activation of protection mechanisms against the threats in question and the subsequent restoration of the system in which the attack was targeted to its previous state. Considering that government-level services, business processes, individual transactions are increasingly being transferred to cyberspace; ensuring security in space will be inevitable. Especially in recent years, cyber security has been given importance at the level of states and cyberspace is seen as a new area to be defended. The destruction caused by cyber attacks causes problems at both the state and institutional level. The importance of cyber security is emphasized in state policies all over the world and states are trying to establish cyber armies that can defend their own cyberspaces. Considering that the following years are pregnant with cyber wars, the importance of creating cyber armies with the necessary knowledge and equipment to defend itself is clearly understood.

In the light of all this information, in this study, especially in the corporate field, the methods of activity that threaten cyber security, as well as legal and institutional infrastructures are discussed and the level of current cyber security awareness is tried to be determined. As the application dimension of the research, the format and standards determined by the Presidency Digital Transformation Office in military institutions and EYP-2.0 (Electronic Transformation) in the system in the background Correspondence Package) package examined and a demo of the relevant package program has been created. In this research, corporate cyber security was conceptually discussed within the scope of meta-synthesis research method, quantitative and qualitative findings of the studies carried out within the scope of the related subject were evaluated, and in this context, new inferences were made on the subject. As the application dimension of the research, the format and standards determined by the Presidency Digital Transformation Office in military institutions and EYP-2.0 (Electronic Transformation) in the system in the background Correspondence Package) package examined and a demo of the relevant package program has been created. It is foreseen that the study will contribute to the literature in this context and will be a useful resource for institutions and organizations in terms of gaining the functionality and sustainability of cyber security mechanisms.

Future research on the subject of the research and suggestions for researchers are presented below for corporate cyber security;

- Complex passwords should be used to access servers. Password, 1q2w3e, names, dates of birth, license plate codes should not be used.

- The software on all servers should be updated periodically.

- All ports on the network should be kept closed except for the ports required by the servers such as web, mail, pdks, routine. They can be used for offensive purposes.

- Physical security tests (Penetration) should be applied to the structures in the institution and strengthened if necessary.

- Cyber security, system and network units should actively use the common mail account in order to share information about the attacks, problems and current issues they encounter.

- Cyber incident records should be reported and added to the Cyber Security Folder.

## REFERENCES

Akyazi, U. (2013). International Cyber Security Strategy and Measures Between Doctrines, 6th International Cyber Security and Cryptology Conference, (E.T. 10.12.2022). http://www.iscturkey.org/s/2226/i/2013-paper105.pdf.

Alwan, H. B. (2018). Policy Development and Frameworks for Cyber Security in Corporates and Law Firms. *International Journal of Legal Information, 46*(3). 137 – 162. s. 150. (E.T. 07.12.2022). https://doi.org/10.1017/jli.2018.41.

Bozgeyik, A. (2021). *Corporate Cyber Security Management*. (1 BS). Justice Publishing: Ankara.

Chakraborty, P. (2020). Re-Thinking Corporate Cyber Security: Changing The System To Meet. The Needs Of The Business İs İmportant. Dataquest 38(8). 70-72. (E.T. 12.12.2022). https://www.dqindia.com/re-thinking-corporate-cyber-security-risk-landscape/.

Cakır, H. & Yasar, H. (2015). Corporate cyber security threats and measures. *Düzce University Journal of Science and Technology, 3(*2), 488-507. (E.T. 02.12.2022). https://dergipark.org.tr/tr/pub/dubited/issue/4810/66286.

Chakraborty, A., Biswas, A. & Khan, A., K. (2022). Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation. *Computer Science*, DOI:10.48550/arXiv.2209.13454

Darılıcı, A.B. (2017). *What is cyber space and cyber security*? (1 BS). Dora Publishing House: Bursa.

Demirdögen, S. (2021). *Industry 4.0 and digital supply chain*. (1st bs.) Ankara: Gazi Bookstore.

World Economic Forum (Wef) Global Risks Report 2022, (E.T. 02.12.2022). https://www.tisk.org.tr/dokuman/dunya-ekonomik-forumu-wef-kuresel-riskler-raporu- 2022.pdf.

Gencoğlu, M. T. (2021). Against Digital Extinction: Cyber Peace. *Turkish Journal of Science and Technology, 16*(2), 245-250. (E.T. 12.12.2022). https://dergipark.org.tr/tr/pub/tjst/issue/64916/970262.

Gungor, N. (2021). *Information technologies and cyber security in internal audit*. (1 BS). Gazi Bookstore: Ankara.

Karagun, V. & Aras, M. S. (2022). Globalization and information age. *Dicle Academy Journal, 1* (3), 32- 40. (E.T. 08.12.2022) https://dergipark.org.tr/en/pub/dade/issue/72954/1186215.

Karasoy, A. & Babaoglu, P. (2021). Cyber Security in Turkey: Legal and Institutional Infrastructure. *Legislative Journal,* 123-155. (E.T. 08.12.2022). https://dergipark.org.tr/en/download/article-file/22011183.

Knight, R. & Nurse, Jason R.C. (2020). A Framework For Effective Corporate Communication After Cyber Security İncidents. *Computers & Security. 99.* (E.T. 08.12.2022).

Krishan, R. (2018). Corporate Solutions To Minimize Expenses From Cyber Security Attacks In The United States. *Journal of Internet Law, 21*(11), 16-19. (E.T. 08.12.2022).

Polat, S. & Ay, O. (2016). Meta-Synthesis: A Conceptual Analysis. *Journal of Qualitative Research in Education, 4* (2), 52-64. Retrieved from https://dergipark.org.tr/tr/pub/enad/issue/32040/354541

Yıldız, E., P. & Simsekler, O. (2023). Corporate Cyber Security In Turkey Investigation Of Legal And Corporate Infrastructure : A Meta-Synthesis Study. *13*(1), 46-58.

Richard and Nurse, Jason R. C. (2020) A Framework for Effective Corporate Communication after Cyber Security Incidents. *Computers & Security* . ISSN 0167-4048.

Unver, M. Canbay, C. & Mirzaoğlu, A.G. (2011). Ensuring Cyber Security: Current Situation in Turkey and Measures to be Taken. (1st ed.) Ankara: Information Technologies and Communication Institution.

Whitman, M.E & Mattord, H. J. (2017). Risk Management: Controlling Risk. ME Whitman/ HJ Mattord. Management of Information Security. (E.T. 12.12.2022). https://www.emerald.com/insight/content/doi/10.1108/eb023001/full/html.

Yıldız, B. & Younes Gejam, E. H. (2022). Cyber-Physical Systems and Cyber Security: A Bibliometric Analysis. *OPUS Journal of Society Research, 19* (45), 35-49. (E.T. 12.12.2022). https://dergipark.org.tr/tr/download/article-file/2213779.