MAINTAINING CYBERSECURITY AWARENESS IN LARGE-SCALE ORGANIZATIONS: A PILOT STUDY IN A PUBLIC INSTITUTION

MUHAMMED ASLAN

SEPTEMBER 2022

ÇANKAYA UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

DEPARTMENT OF COMPUTER ENGINEERING

MASTER'S THESIS IN

INFORMATION TECHNOLOGIES

MAINTAINING CYBERSECURITY AWARENESS IN LARGE-SCALE ORGANIZATIONS: A PILOT STUDY IN A PUBLIC INSTITUTION

MUHAMMED ASLAN

SEPTEMBER 2022

ABSTRACT

MAINTAINING CYBERSECURITY AWARENESS IN LARGE-SCALE ORGANIZATIONS: A PILOT STUDY IN A PUBLIC INSTITUTION

ASLAN, Muhammed

Master of Science in Information Technologies

Supervisor: Assoc. Prof. Dr. Özgür Tolga PUSATLI

September 2022, 58 pages

Parallel to the spread of technology, the amount of information stored and processed by workplaces is also increasing. There is a need to ensure the security of the information infrastructures in which this information is processed and stored in addition to the need to protect personal data. The loss of information caused by employee-related security vulnerabilities may cause irreparable damage. In our thesis, research was conducted to increase the awareness of employees with regard to cyber security.In the literature review, it was observed that there were few studies on how effective the measures implemented in organizations were reported. Our research includes data on the results of the phishing drills that a public institution applied to its personnel, the level of participation of said personnel in awareness training, and the reading statistics of regularly published information security bulletins. Our work has been beneficial in determining the methods that can be used to increase the cyber security awareness of personnel in organizations with 1,000 or more personnel. In our study, users were considered as a whole, and not individually evaluated. According to the findings, organizations can increase users' cybersecurity awareness by systematically conducting phishing exercises, providing awareness training, and regularly publishing information security bulletins. The awareness of reading bulletins rapidly increased after phishing exercises and training and decreased in the following

months, an increase was observed in the awareness of reading the bulletin in the long term.

Keywords: Cyber, Security, Phishing, Drill, Awareness, Training, Bulletin

ÖZ

BÜYÜK ÖLÇEKLİ KURUMLARDA SİBER GÜVENLİK FARKINDALIĞININ SAĞLANMASI: BİR KAMU KURUMUNDA UYGULANAN PİLOT ÇALIŞMA

ASLAN, Muhammed

Bilgi Teknolojileri Yüksek Lisans

Danışman: Doç. Dr. Özgür Tolga PUSATLI

Eylül 2022, 58 sayfa

Teknolojinin yaygınlaşmasına paralel olarak iş yerlerinin sakladığı ve işlediği bilgi miktarı da artmaktadır. Bu bilgilerin işlendiği ve saklandığı bilgi altyapılarının güvenliğinin sağlanmasına ve kişisel verilerin korunmasına ihtiyaç vardır. Çalışan kaynaklı güvenlik açıklarından oluşan bilgi kayıpları, telafisi mümkün olmayan zararlara neden olabilir. Tezimizde, çalışanların siber güvenlik konusunda farkındalıklarının artırılmasına yönelik bir araştırma yapılmıştır.

Literatür taramasında, kurumlarda uygulanan önlemlerin ne kadar etkili olduğuna dair az sayıda çalışmanın olduğu ve çok az güvenlik ihlali rapor edildiği gözlemlenmiştir. Araştırmamız, bir kamu kurumunun, personeline uyguladığı oltalama tatbikatlarının sonuçlarına, personelin farkındalık eğitimlerine katılım düzeylerine ve düzenli olarak yayımlanan bilgi güvenliği bültenlerinin okunma istatistiklerine ilişkin verileri içermektedir. Bu çalışmanın faydası, 1000 ve üzeri personeli olan kurumlarda, personelin siber güvenlik farkındalığını artırmak için kullanılabilecek yöntemlerin belirlenmesi yönündedir. Çalışmamızda, kullanıcılar bir bütün olarak ele alınmış ve bireysel değerlendirmeye tabi tutulmamıştır. Bulgulara göre, kurumlar, sistematik olarak oltalama tatbikatları yaparak, farkındalık eğitimleri vererek ve düzenli olarak bilgi güvenliği bültenleri yayımlayarak kullanıcıların siber güvenlik farkındalığını artırabilir. Buna ek olarak, bülten okuma farkındalığı, oltalama

tatbikatları ve eğitimler sonrasında hızlı bir şekilde artıp, ilerleyen aylarda azalsa da bir yılın sonunda bülten okuma farkındalığında da kalıcı bir artış gözlenmiştir.

Anahtar Kelimeler: Siber, Güvenlik, Oltalama, Tatbikat, Farkındalık, Bülten

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my parents for their support and sacrifice to me. Your memories would ever shine in my mind.

Special thanks to my supervisor Assoc. Prof. Dr. Özgür Tolga PUSATLI for the excellent guidance and for providing me with an excellent atmosphere to conduct this research. My special gratitude also goes to the thesis committee for the encouragement and insightful comments.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

HIMS: Hospital Information Management System

IP: Internet Protocol

ISMS: Information Security Management System

ISO: International Organization for Standardization

IT: Information Technology

SSL: Secure Socket Layer

TÜBİTAK BİLGEM: Informatics and Information Security Research Center of TÜBİTAK

CHAPTER I
INTRODUCTION

1.1. PROBLEM AND MOTIVATION

Ensuring information security in corporate organizations is of vital importance. In both public institutions and private sector companies, many precautions are taken to protect information assets like all other assets and not to share them with third parties without permission. Humans, as the weakest link in the security chain, must be investigated for the protection of information.

Cyber security is commonly ensured by implementing hardware and software solutions in information systems infrastructures. However, even though the necessary infrastructure investments have been made, it cannot be said that information assets are completely secure. To achieve real cyber maturity, increasing the cyber security awareness of personnel working in corporate organizations is necessary. Despite all advanced security products, the user cannot be prevented from sharing his/her password with someone else or from opening an e-mail containing fake links. It is obvious that the investments to be made to increase the awareness of users regarding information security are at least as important as infrastructure investments such as hardware and software assets.

From this perspective, we have opted in our thesis to study how to strengthen the human dimension. We reviewed the studies on this subject in the literature and we have observed that similar methods are applied in Türkiye and abroad. To prepare users against a possible threat by conducting phishing drills, to educate them on basic issues by providing information security awareness training, to regularly publish information security bulletins to inform personnel about current cyber events and cyberattacks, to inform users via e-mail and to attract the attention of the personnel through digital screens can all be listed as featured methods.

1.2. AIM OF THE STUDY

Although it is observed that some studies have been carried out to increase information security awareness both in public institutions and in the private sector, we found few studies examining how these activities benefited in terms of increasing user awareness.

We aim to reveal how much phishing exercises, awareness training, and the publishing of bulletin activities in public institutions and private sector businesses with 1,000 or more users work in increasing personnel awareness. Moreover, we aim to determine which of these three methods is most effective and to show how long this effect lasts. As a result of the determinations, we aim to guide public institutions and large-scale enterprises in increasing personnel awareness and ensuring information security.

Within the scope of our study, we investigated the contribution of these three measures to garner information security awareness in an institution with roughly 1,000 personnel. In our study, which focuses on the human factor, technical cyber security measures taken through hardware and software products are excluded or minimized.

The main purpose of our study is to show how phishing exercises, the provision of information security awareness training, and issuing monthly information security bulletins have an impact on personnel within one year.

The research question of the thesis is:

Can conducting phishing drills and awareness training as well as preparing information security bulletins increase the cyber security awareness of personnel in the long term?

1.3. OUTLINE

In Chapter 2, we present information about the studies in the literature and the subjects that form the background of our thesis. We detail reviews on information security, cyber security, phishing attacks, phishing exercises, awareness training, and cyber security bulletins. We have included screenshots of examples of phishing attacks in public sources. We give examples of users being directed to fake websites with similar techniques. We also provide examples and screenshots of what content is mentioned in security bulletins. In addition, we have included a summary of the

methods applied in the public institution as the subject of our study. We have included the information we obtained from articles, theses, and websites that examine the institutions and companies that use the aforementioned awareness-raising methods. We examined the studies on the behavior of employees working in corporate organizations. We examined the studies on the information security awareness of the academic staff working at the university. On the other hand, we present research measuring the cyber awareness of civilians in this section. In the last part of Chapter 2, include our evaluations regarding the deficiencies in the studies in the literature.

In Chapter 3, we briefly described our research method. We obtained this data from an institution that implemented a phishing exercise and information security awareness training program more than once and regularly publishes an information security bulletin for its personnel every month. We also include data on the activities carried out between February 2021 and April 2022.

In Chapter 4, we examine the data related to the activities that form the basis of our thesis, including the results of three different phishing drills. The monitoring rates of two different information security awareness training programs within the institution were also included in this section and we compared the reading rates of eleven different information security bulletins. We had the opportunity to evaluate the effect of these methods on each other.

In Chapter 5, we evaluated the findings based on the information we obtained during our research. We also described the limitations affecting these findings and state how these limitations can be overcome in future studies. In this section, we finally answer our research question.

CHAPTER II
BACKGROUND AND LITERATURE REVIEW

2.1. BACKGROUND

2.1.1. Information as an Asset

As the most fundamental element of our study is information security, first of all, what information means must be fully understood.

Information is defined as a collection of data that can be recorded, understood, and transmitted on paper or through other media, or the real and fictitious products of ideas transmitted, recorded, or published in any form in the mind, formally or informally [1].

Information is an asset that can be an opportunity when one possesses it. However, it can become a threat if it is lost and can be changed without notice if it is stolen. For this reason, the security of an information asset is of great importance to the owner of the information.

2.1.2. Information Security and Cyber Security

As discussed in [2], security of information assets can be defined as providing continuous access to information to protect the confidentiality, integrity, and accessibility of the information source, ensuring end-to-end confidentiality during the transfer of information, and transferring it in integrity without being corrupted or captured by someone else.

As reported in [3], cybersecurity is the collection of security policies, risk management approaches, training, tools and techniques, and best practices with regard to technologies that can be used to protect the cyber environment and assets of organizations and users. On the other hand, the assets are the sum of the information infrastructure, applications, services, and information transmitted and/or stored in the cyber environment. Cyber security endeavors to ensure the security of these assets in

a sustainable manner against security risks in the cyber environment.Information assets that must be kept secure within the scope of our work include personal information such as identity numbers and telephone numbers, credentials such as computer user names and passwords, and commercially confidential information such as price offers.

In the literature, the user is often referred to as the weakest link; examples are found in [4] and [5]. Bulletins, drills, and training sessions are among the popular approaches to increase awareness. Before going into the details, we introduce these approaches for the purpose of familiarization.

2.1.3. Information Security Bulletin

In general, content that is shared online through web pages, in which recent developments in the field of cyber security are compiled, are called information security bulletins. For example, the images of the February 2022 bulletin published by a firm on its website are given in Figure 2.1 [6].

Figure 2.1: An Example of Cyber Security Bulletin [6]

An information security bulletin is regularly published every month in the workplace from where we obtained our dataset. There are generally ten pieces of content in the bulletin, which are sent to all personnel via e-mail. The bulletin is about

corporate cyber security activities and news about global cyber security that may be of interest to the end user.

The bulletin also includes detailed information on what users should do to protect information security while using digital and social media in both their business and private lives. For example, applications that use a user's biometric data for entertainment purposes may violate personal data security. These applications carry the risk of fraudulent access to bank accounts by using the user's biometric data. There is news that the information we provide on our social media accounts may be in the hands of hackers. There are examples in a bulletin from cyber incidents around the world to understand the level reached by the attackers in cyberattacks and hacking. Bulletins also include some information about the legal aspects of information security personnel data protection law [7].

The bulletin includes popular incidents to attract the reader's attention. Warnings about voice imitation, which may lead to personal data breaches and be used for fraudulent purposes, the dangers that await users as a result of the change in the user agreement of the WhatsApp messaging application, and warnings and important information about the major cyber threats that will stand out in the world in the close future can be given as examples of a number of topics in the bulletin.

The aim of publishing a newsletter every month is to keep users aware of information security.

On the other hand, in our study, a phishing drill was carried out with scenarios compatible with the news content in the bulletin. There are reports that personal information and password information can be obtained by redirecting to fake pages. The phishing risk was included in the monthly bulletin before the phishing exercise with the content given in Figure 2.2. In the example, there was news stating that users may receive fake e-mails containing the information that a vaccination campaign had been launched.

Kasım 2021

Aşılama Faaliyetleri için Gelen E-Postalara Dikkat!

Salgın sürecinde aşılama faaliyetlerinin devam etmesi nedeniyle kullanıcılar hackerların hedefi olmaktadır.

3. veya 4. doz aşı randevularının aktif olduğu yönünde ulaşan bir e-posta ile kullanıcıların e-devlete giriş yapmaları istenmektedir.

Uzmanlar gelen mesaj içeriğinde yanlış yönlendirme ile zararlı bir site bağlantısı içerip içermediği hususunda dikkatli olunması gerektiği yönünde uyarılarda bulunarak, e-posta içeriklerinde tıklanacak butonların doğru adrese yönlendirildiği ve 'http' yerine 'https' ile güvenli siteye giriş yapıldığının kontrol edilmesi gerektiği hususuna dikkat çekmektedirler.

Figure 2.2: An example of news in a bulletin

It is aimed to increase the interest of users in the bulletin by sharing news, including the scenario to be used before a phishing drill in the bulletin. We give details of the phishing exercise in Chapter 3.

2.1.4. Phishing

Phishing is described as a skill of impersonating a trusted website aiming to obtain private and secret information such as usernames and passwords and/or social security and credit card numbers [8].

A phishing e-mail specially crafted by an attacker may appear as a genuine e-mail. With the help of the prepared e-mail, computer users are directed to fake screens and they are requested to log in with a password. On the other hand, by running the files attached to these e-mails, the computers of the victims can be controlled by the attacker [9].

Since there is no international authority that controls the content of web pages, it is possible to create fake web pages on the Internet. The phishing attacker designs a fake interface similar to, for instance, a real bitcoin account interface. Then, trap content is prepared for the user to access the link in the e-mail sent to the user and redirect to this fake interface. When the user tries to enter their account information on the fake web interface, this information is captured by hackers. Figure 2.3 shows a screenshot of a phishing e-mail received in the author's e-mail box.

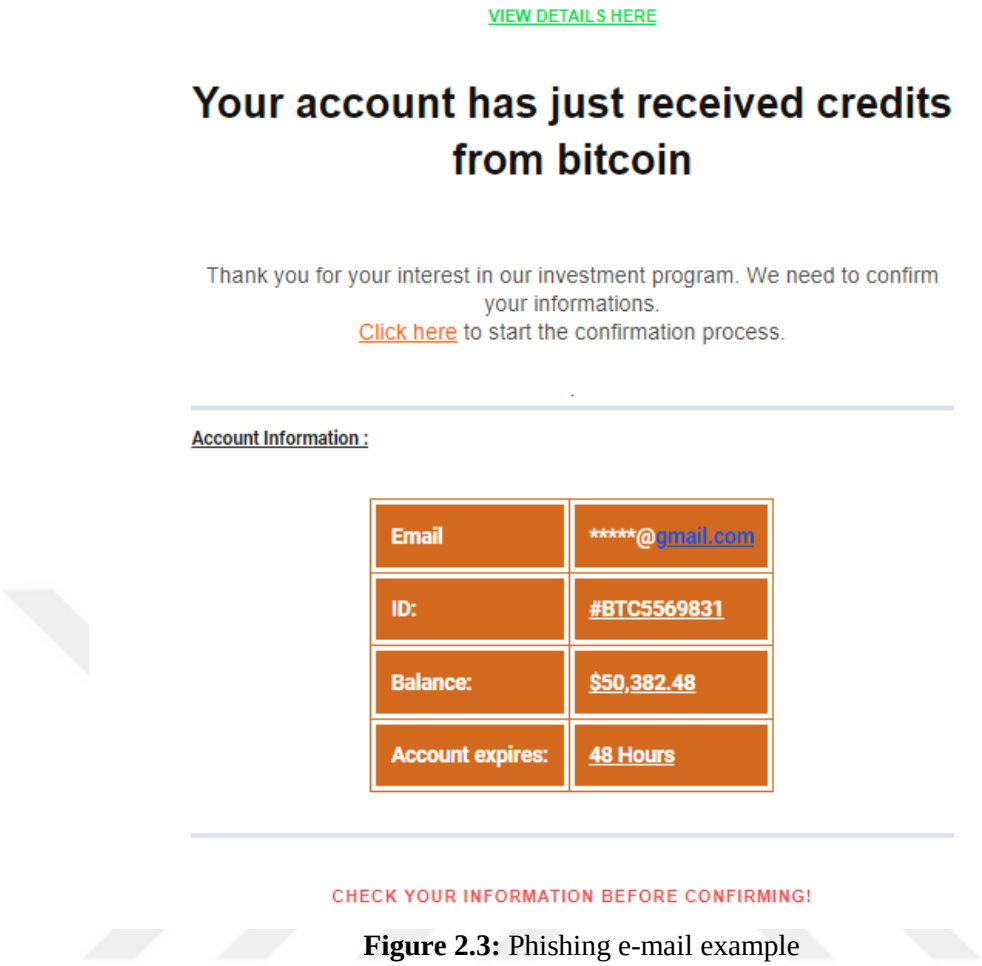

Figure 2.3: Phishing e-mail example

Another example is phishing on Twitter. The real Twitter account of the global payment system platform PayPal is shown in Figure 2.4. A New Year gift announcement with phishing purposes sent on behalf of PayPal is shown in Figure 2.5 [10].

Figure 2.4: Real PayPal tweet

Figure 2.5: Fake PayPal tweet

Press releases made by the CBRT (Central Bank of the Republic of Türkiye), which is the determinant of monetary policies in Türkiye, are closely followed by all citizens. Therefore, attackers impersonate the account belonging to this institution. The real Twitter account of the Central Bank of the Republic of Türkiye (@Merkez_Bankasi) is in Figure 2.6. It can be seen that, in Figure 2.7, a Twitter account was created with a name similar to the Central Bank of the Republic of Türkiye (@cMerkez_Bankasi) and a phishing attack was made through this account [10].

Figure 2.6: Real tweet from the Central Bank of the Republic of Türkiye

Figure 2.7: Fake tweet about the Central Bank of the Republic of Türkiye

During the coronavirus pandemic, which affected the whole world from 2020, many cyberattacks were experienced. One of these was the phishing attack, which deals with the state aids implemented in Türkiye. Due to the pandemic, cash support was offered to citizens by the state. It can be seen in Figure 2.8 that the icon in the browser address line of the web page containing the application link for the aid made by two different ministries is not reliable. This icon tells us that the domain does not use the SSL (secure socket layer) protocol and is not a secure page [11].

Figure 2.8: Fake web page about state aids

As can be seen in the examples, users can be exposed to phishing attacks at any time. Phishing drills should be carried out within the organization to increase users' awareness of phishing attacks.

2.1.5. Phishing Drills and the ISMS

Institutions and organizations must create ISMS (Information Security Management System) policies within the scope of ISO 27001. In line with these policies, corporate information security processes operate. Although cyber security products endeavor to provide security in information infrastructures, it is vital to prepare the weakest link, the human, against possible threats. Phishing drills are accepted as an effective method in both measuring user awareness and increasing awareness [4].

Before phishing attacks are experienced against an organization, phishing drills that are similar to phishing attack scenarios are performed to determine the level of readiness of human resources.

It is thought that the most effective method to prevent information security violations that may occur as a result of personnel mistakes in the institution where we performed our study is to train and inform personnel. Phishing drills are implemented to cover all personnel for this purpose. Practice scenarios similar to current phishing attacks are determined by the IT department. The details of the phishing exercises conducted in our study are discussed in Chapter 3.

Training should be organized to inform users after phishing exercises and awareness is expected be increased against cyber threats such as phishing attacks.

2.1.6. Information Security Awareness Training

The leading risk that threatens information security is the lack of awareness of employees with regard to security. When information security violation incidents experienced by world-famous IT companies in recent years are examined in detail, it is revealed that the problem is mostly caused by the lack of information security awareness of the employees.

Information security awareness training is training that aims to equip employees with the information they need to protect an organization's information assets from loss and damage [12].

In the workplace where we carried out our work, online training was held at certain intervals within the scope of information security activities. When the personnel history was examined, it was observed that there were employees from different disciplines who may have little experience in the field of information technologies. For this reason, many subjects in the training were covered at the basic level.

Examples that all users can easily understand and encounter in daily life were included in the training. In addition, the training content was prepared interactively to make the training more efficient. Immediately after providing information about a certain subject in the training, questions about the subject were asked to the user, and unless the correct answer was received, it was not possible to move on to the next subject.

The access address was sent to the e-mail of the personnel via the training platform. In this way, users were able to complete their training at a time convenient for them. Information on personnel who attended or did not participate in the training were reported. In addition, reminder e-mails were sent periodically to those who did not attend the sessions.

The aim of the awareness training was to increase the information security awareness level of the personnel and keep their information up-to-date on information security issues.

Training contains the definition and details of secure information that is explained in the context of Confidentiality, Integrity, and Accessibility. Details on issues such as disruption of business continuity are also included. Internal and external threats that may endanger information security are explained in detail. Details of technical measures may be insufficient if the user violates security. There is detailed information about prevention, storing the information for which the user is responsible, how mobile devices should be carried, leaving a computer session locked, and not leaving documents in meeting rooms. In addition, how to diagnose a social engineering attack and clues about the manner of defense if an attack is noticed are also examined with sample scenarios. Risks that may arise in wireless networks in open areas are detailed.

A number of basic habits are expected from users at the end of the training. Some of these habits include determining passwords that are sufficiently complex and

with a large number of characters, refraining from clicking on connection addresses that do not have SSL certificates, being careful when sharing personal information such as identity numbers and phone numbers, the avoidance of using corporate e-mail information while joining e-commerce sites, contacting the technical support unit in cases of receiving suspicious e-mails, not connecting to wireless networks serving in open areas, and not leaving confidential information on office desks.

In this chapter, we discussed the fact that information is a valuable asset that needs to be protected and we touched on the training of human resources, which is the weakest link in the context of information protection. In this context, we discussed bulletins, phishing drills, and awareness training. In Section 2.2, we examine the studies in the literature on these issues.

2.2. LITERATURE REVIEW

A literature search through national and international sources was conducted on the studies conducted in the field of cyber security. We took studies that fall within the scope of measuring cyber security awareness after training, drills, and publishing bulletins.

2.2.1. Public and Private Sector Organizations

A study that was carried out in South Korea recently [13] included factors that have an impact on information security awareness. These factors included awareness training, participation of management in security, and physical security. In addition to the impact of the titles on cyber security awareness, there are evaluations of the interaction between each other. In the study, based on the foresight that corporate training will increase information security awareness, the hypothesis of "Information Security Education is positively related to Information Security Awareness" was tested. As the research instrument, a questionnaire was sent to 3,000 people from three different institutions operating in the public sector in South Korea. As a result of the study, it was understood that the participation of employees in awareness training had a positive effect on their focus on information security processes and procedures. When the results of the survey were examined, the hypothesis that says there is a positive relationship between the level of cyber security awareness and awareness training was confirmed.

A study [14] was conducted to measure the cyber security awareness of the employees of a financial institution operating in Thailand. In the financial sector, where monetary transactions occur instantly, it is important to avoid experiencing any problems regarding the services received or to provide a quick solution to the problem. As a result, there is a SLA with its stakeholders. SLA values being applied for both internal and external customers are important in the finance sector. Employees are required to respond quickly and effectively to requests from customers. This study was carried out by following the e-mail phishing drill method with Bank of Thailand employees. There were 20,500 employees and 700 managers within the scope of the study. A cyber scenario was determined for redirecting to a fake address with the URL in the e-mail text content and typing the password information on the page that opens. According to the results of the study, it was observed that 72.9% of the managers rejected the e-mail. 3% of the administrators, that is 21 people, only opened the e-mail. 85 people, corresponding to 12.3%, opened the e-mail and clicked on the link. 81 people, that is 11.72%, opened the e-mail, clicked the link, and completed the password information. 76.77% of other employees did not open the e-mail. 1.32% of them opened the e-mail but did not perform any clicks. 6.96% of them opened the e-mail and clicked the link. 3,063 people, 14.95% of the employees, opened the e-mail, clicked the link, and entered the password on the fake web page. As a result of this study, a prediction was made about the cyber security awareness levels of the company employees. It was determined that some studies should be performed to reduce the risk. This research aimed to measure and increase cyber security awareness by performing a phishing exercise. However, there was no test study on whether the exercise increased the awareness of the employees thereafter.

In a recent study [4], to measure cyber security awareness, a phishing exercise was conducted in a public institution with 33,000 employees and 400 provincial units. The provincial organization and the central organization and the IT personnel of the institution also participated in the study. Fake web pages and fake e-mails were used. This study was carried out in two different phases and for three different personnel types with seven scenarios. The address of the fake website was chosen to be very similar to the name of the institution, just like attacks seen in real life. Users can access the site by sending an e-mail over the domain name used for the exercise. The fake website was designed similarly to the interface of the corporate remote access service.

It can be seen in the browser that the site is not safe. On the landing page, there is a username and password field where user information can be entered. As a result of this comprehensive study, it was concluded that cyber security awareness is quite low. However, there is no study conducted to increase awareness after this exercise, and benefits were not reported.

Another study [15] aimed to determine the information security awareness levels of people working in public institutions based on various criteria. IT department employees and employees from other departments from many different institutions participated in the study. Most of the 501 personnel were undergraduates. One of the criteria in the survey was education. In the statistical evaluation made according to education level, it was observed that university graduate employees have higher information security awareness than participants with high school or below education levels. In the study, there was no data on the examination of the change after giving awareness training to the same people. However, it was revealed that there is a link between the increase in education level and the increase in information security awareness in general. However, it was argued that one time would not be sufficient to increase the awareness of information security and that it should be a constantly renewed process.

In another enterprise-wide study [16], employees in a local hospital were taken as a case. Password habits of physicians using the Hospital Information Management System (HIMS) were examined. Since access to institutional information resources is provided through HIMS, physicians must have a high level of information security awareness and use strong passwords. A questionnaire form was sent to 420 physicians via e-mail. The evaluation was made based on the answers of 203 physicians who responded to the questionnaire. Password meter software developed by TÜBİTAK BİLGEM (Informatics and Information Security Research Center of TÜBİTAK) was used to measure password security levels. Password security levels are collected in five categories. When the results of the study were examined, it was observed that none of the physicians participating in the study used it at the “strong” or “very strong” level. On the other hand, only 9% used “good/medium” passwords. The password security levels of the remaining 91% were determined as “weak” or “very weak.” As a result of the study, it was recommended to increase the inspections for the end users in health institutions and to disseminate information security awareness training as a

necessity. On the other hand, although it was suggested to provide awareness training to increase awareness of information security, it is observed that no research thereafter has been conducted to measure the contribution of this training to awareness.

Another local study was carried out on the information security awareness of the employees of the Erzincan Public Health Directorate [17]. For employees' awareness of information security, an evaluation was made based on factors such as age, gender, education level, title, and experience of using information and communication technologies. Information security awareness training was given and a situation analysis was made before and after the training. The training included information about social engineering attacks, malware types and precautions, password security, and legal responsibilities. A total of 53 personnel, including a doctor, midwife, nurse, dietitian, public servant, technician and manager, participated in the study. A significant difference was found between the information security awareness of the public health personnel participating in the study before and after the training. It was concluded that the majority of the employees did not have enough information about information security before the training and they increased their level of information security after the training. It was concluded that the training given in the research was beneficial and created awareness against cyber and social engineering attacks.

In the literature, another study of the experiences and results obtained during the establishment and development of the information security management system of a Medical Faculty Hospital are discussed [18]. In this 1,200-bed hospital, there is an automation system. All medical procedures and administrative work in the hospital are carried out with this automation system with 2,000 users being able to operate on this system at the same time. During the three-year-long ISMS installation process, six specialist personnel provided regular training to the hospital staff every year. An annual average of 1,217 personnel received an average of 23 hours of training. After the training, regular e-mails and system messages were sent to the employees in order to keep the awareness of the employees high and to keep the issue on the agenda. In addition to these factors, information security warnings were placed at certain points within the institution, and reminders were provided. As a result of the study, thirteen cyber threats at the major level in the previous year before the ISMS integration within the institution interrupted the information systems at an annual rate of 6%. It was

determined that 72% of the threats created before the establishment of the ISMS system were caused by the human factor. After three years of training, the total number of threats to information resources decreased by 95%. The rate of human error decreased to 40%. Within two years after the system was installed, the system outage rate decreased to 1%. At the end of the third year, no major threats to information resources were detected. With these results, it was understood that the training given to the employees gave results and that progress was made in the awareness of information security.

In another study, data from the personnel working in the IT departments, which are responsible for providing cyber security, of universities operating in Türkiye were used [19]. Within the scope of the study, a personal information form, a data security awareness scale, and a personal cyber security provision scale were sent to the e-mail addresses of 1,440 personnel working in 174 of 206 universities. The evaluation was carried out with the information collected from 410 people who responded voluntarily. It was determined that the awareness of the working personnel of providing digital data security and personal cyber security is high, and there is a positive relationship between these two types of awareness.

In recent research on the example of the Kayseri Bar Association [20], it is stated that several practices occurred in order to transfer the services offered by the Kayseri Bar Association to the digital environment on a daily basis so as to minimize the risks that may arise due to this and to increase the awareness of cyber security. With developing technology, various security risks arise in the Internet environment at the individual or public level, and accordingly, public institutions tend to take various measures. The legislative information system, which envisages regulations on information security and cyber security in order to create a security culture in public institutions, constitutes the source of the institutional documents that the study deals with. Although the aim is to raise awareness through training, announcements, briefings and bulletins, there is no evaluation of the extent to which these applications contribute to cyber security awareness.

Another study [21] was performed in 2012 to seek an answer to the question "Is the existing virtual and physical security in the institution sufficient as perceived by the staff working in the Turkish Grand National Assembly?" The research was conducted to determine the general security perceptions of the Turkish Grand National

Assembly personnel, both virtual and physical, in a comparative manner. A questionnaire was administered to 430 personnel in different administrative units. The survey consisted of two parts. In the first part, there were demographic questions about the individual characteristics of the employees. In the second part, some propositions measured the security perception of the personnel. The sources and documents used in this study were deemed to contain correct and true information. It was stated that the sensitivity in the IT unit was not at a sufficient level despite increasing cyber-attacks. Although there is a suggestion for the development of the systems, there is no information about increasing and measuring the sensitivity and awareness of the personnel.

Within the scope of another study, the questionnaire applied to the gendarmerie and police officers in the Provincial Gendarmerie Command and the Provincial Security Directorate in the city center of Siirt was evaluated [22]. 404 personnel, including 207 gendarmerie personnel and 197 police personnel, participated in the study. In the first part of the questionnaire, questions about socio-demographic characteristics were included, and in the second part, a 34-item information security awareness scale set of questions was included. When the results of the study were evaluated, the information security awareness levels were found to be low in general. The reason for this was thought to be insufficient in-house training. Based on the results of the study, it was recommended to provide information security and awareness training and exams together with basic computer training during the orientation training before starting the profession to at least maximize the information security awareness level of the personnel.

Another local study in the literature includes research on information security in information centers [23]. The research, based on the qualitative method, was carried out in a total of 14 university libraries in Ankara. In the process of raising information security awareness, it is one of the predetermined criteria for the participants to be the head or assistant of the library and documentation department, as the managers constitute the primary response group. Within the framework of the research calendar, the fact that the participants work in university libraries in Ankara was also among the predetermined criteria. In this research, the data obtained from the interviewer's notes were coded with predetermined concepts and explained with five themes. The research process was completed with the interpretation of the findings. The themes in question

were information security, necessity and importance of information security, information security practices in libraries, knowledge of information security, personnel audits, and user audits. As a result of the research, seven determinations were made within the scope of information security awareness. In light of these findings, five suggestions were presented. However, we could not reach the implementation of the proposed recommendations and the analysis of their benefits as a follow-up study.

In another study [24], it was stated that it was aimed to provide an effective and efficient combat capability against these threats by increasing awareness. Due to the difficulty of obtaining the desired data and the need for expert opinions, data collection methods such as interview and document analysis were used, and qualitative research methods in which the researcher himself had a key role in data collection were used. In this context, reports submitted by national and international institutions and organizations with competence in the field of cyber security regarding threats to corporate cyber security (within the scope of document analysis), and domestic and foreign studies were examined. Interviews were made with ten personnel working in cyber security-related units with tenures ranging from two to seven years. There was no benefit assessment regarding the precautionary measures to be taken within the scope of the study.

In another study [25], the literature observed that if enough attention is not paid to the issue of cyber security, how much damage can be caused to both public organizations, private sector organizations, individuals, and states, and that the issue of cyber security cannot be only with technological devices, it was pointed out that there are many factors in the cyber security management model. In the study, the theoretical aspects of the cyber security management model, which can be used to cope with the cyber security issue of any organization and ensure the security of their critical infrastructures, are examined for organizations to survive cyberattacks with the least damage with a good policy. Regardless of being in the public or private sector, it was stated that the necessary infrastructure should be created to ensure the cyber resistance of corporate organizations, the awareness of personnel should be increased, and management should make decisions first. Within the scope of the said study, there is no evaluation of the contribution of the activities to be made although the measures recommended within the scope of cyber security management are included.

Within the scope of another study [26], a questionnaire was administered to the information technologies managers of 150 small and medium-sized enterprises selected randomly among 5,000 enterprises registered in the Bursa Chamber of Commerce and Industry operating in the city of Bursa. After the evaluation of the questionnaires were made in line with the information security criteria, it was determined that 65% of the employees in the enterprises do not have sufficient knowledge about cyber security. It has been suggested that awareness studies on cyber security should be carried out in order to increase the awareness and knowledge levels of employees with regard to cyber risks. On the other hand, although the problem point has been determined, concrete suggestions for the solution of the problem and measurements regarding the benefits of the suggestions were not included.

The results of the study conducted in an airline company operating in Türkiye in the recent period were examined [27]. Several activities were carried out within the scope of the ISMS installation at the said airline company. After the documentation, studies started to increase the awareness of information security. Increasing the number of personnel who received information security awareness training above 60% was determined as a target. The change in the number of personnel receiving training over the years was examined. It is stated that 1,000 of the existing 5,000 personnel received training in 2018. After the ISMS studies, 4,000 of the 5,500 personnel received this training in 2019. The participation rate, which was 20%, increased to 72% within one year. Although the rate of receiving awareness training in this business had increased thanks to ISMS studies, there was no analysis of the level of information security awareness in real terms. There was also no information about the change in the level of personnel awareness before and after the training.

In a recent study [28], information security awareness levels of IT companies operating in Ankara were examined. An analysis was carried out based on the survey data made to a manager from 253 different companies. As a result of the survey, answers to five different questions were sought. One of the questions, namely “Does the information security awareness of companies change according to the education level of company managers?” was in the form. The educational status of 253 participants was grouped as high school, associate degree, undergraduate, and graduate. When the findings were evaluated, it was observed that as the education level of the company manager increases, the level of awareness also increases. Within the

scope of the study, the relationship between education status and awareness levels was examined in general; however, there is no data on which graduate level employees should receive information security awareness training. Therefore, no connection was established between mindfulness training and awareness level.

Another study [29] aimed to measure the information security awareness of the personnel working at Bahçeşehir University, where 111 academic staff and 58 administrative staff participated. An information security awareness scale was sent to 169 employees who were asked to answer 34 questions. The feedback received from the employees was analyzed according to variables such as demographic characteristics, title, working time, and gender. In line with the findings of the study, it was concluded that training should be organized and visual materials should be used in order to increase the information security awareness of the employees. Within the scope of the research, the level of information security awareness was examined, but there was no evaluation of how much it would contribute to levels of awareness if the training recommended to be organized to increase information security awareness were implemented.

In a study conducted in Ankara in 2021 [30], the cyber security awareness levels of secondary school teachers were examined. Personal information forms and some other questions were used in the research. Responses from 455 teachers were analyzed according to demographic characteristics, branch, etc. and evaluated according to the criteria. It was observed that the level of providing personal cyber security to teachers in the branch of information technologies is significantly higher than for teachers in other branches, regardless of the branches, courses, etc. for information and communication technologies. It was observed that the level of providing cyber security to trainees was higher. According to the results of the research, it was observed that the awareness of teachers who received training in information and communication technologies and cyber security was higher. From this perspective, it was evaluated that training should be given to all personnel in the school, especially teachers, in order to increase cyber security awareness.

2.2.2. Other Research

In another study [31], information about the cyber security awareness study conducted with 153 students studying at a university in Taiwan was given. Within the

scope of the study, 153 students were divided into three different groups consisting of 51 people. In the study, the effects of three different educational environments on cyber security awareness were compared. The first of these was the hypermedia environment with intense visual content, the second the multimedia environment with medium visual content, and the third was the hypertext environment, which was mostly text-based, with a low amount of visual content. The same topics were covered in all classes conducting the phishing drills training and as many comparable sessions were held as possible. While determining the content of the training organized, thirty different topics were evaluated. People frequently would show weakness in the e-mail management topic that was selected among the other topics. A twenty-question multiple-choice test was conducted to measure the students' awareness levels. When the results of the study were examined, it was observed that education in the hypermedia environment was the most effective way to increase the security awareness level of the students. This was followed by the multimedia environment and the hypertext environment, respectively. A hypermedia environment contains both textual content such as a hypertext environment and visual content such as a multimedia environment.

An examination was made on the effectiveness of cyber security awareness in Thailand. Thirty-three students of the Faculty of Information and Communication Technology participated in the study [32]. The participants were divided into two different groups. The training given to those in the first group had been designed to include written, video and game content. Those in the second group also received classroom-based education. In order to measure the effectiveness of the training, phishing e-mails were sent to the employees before and after the training. In the evaluations, it was seen that awareness training did not increase the false positive rate, but was effective in reducing the false negative rate.

In another study conducted in Istanbul, the behavior of people in cyber environments was examined [5]. The main population of the study was determined as individuals aged 18 and over living in Istanbul. Convenience sampling, one of the non-random sampling methods, was used as the sampling method in the study. It was studied at a 95% confidence interval. A questionnaire form was prepared for data collection, and 335 forms were collected from the respondents with an online questionnaire. The study concludes that employees at private sector companies have

higher cyber security awareness than the employees in public institutions; however, suggestions that will contribute to raising awareness and their effects were not evaluated.

A study was prepared based on the results of the survey conducted with 48 employees of a call center operating in Antalya [33]. The survey study consisted of sixteen questions in total. According to the results of the research, it was observed that the level of awareness about cyberattack-threat technologies was higher among trained employees. It was emphasized that training is necessary to cope with cyberattacks and cyber threats. On the other hand, awareness training was applied to the employees participating in the survey, and the change in the awareness level was not examined afterward.

In a study, the results of the survey conducted among the students of the Vocational School of Health at a foundation university operating in Ankara are included [34]. In the research, 153 students who took the "Information and Communication Technologies" course contributed to the study by completing a questionnaire which comprised two parts and 48 questions. The questions were on the topic of malware blocking, computer user account security, online shopping, wireless networks, social networks, password security, and legal issues. In the study, an answer was sought for the question "Does the information security awareness of users show a significant difference according to their previous information security training?" In the mentioned study, two separate questionnaires were not administered to the same students before and after taking the Information and Communication Technologies course. It was not measured in which areas the awareness of the same students increased after taking a course for some time. However, a comparison was made between student groups with similar qualifications in terms of information security awareness. It was observed that the information security awareness of the students who had taken the information and communication technologies course was higher than the students who had recently started university. It was understood that education is effective in increasing awareness of information security.

Research on information security awareness was conducted with the participation of 88 students studying at a private university operating in Türkiye [35]. A questionnaire was administered to the students, some questions were asked and an evaluation was made based on the answers received. The age range of the study group

was 18-29 years, with an average age of 20.33 of the students studying in six different departments. The twenty-four items about cyber security and eighteen items on information security awareness were used in the questionnaire. As a result of the research, when all of the students were evaluated, it was observed that the awareness of information security was at a high level. On the other hand, it was observed that the information security awareness of the students studying at the education faculty was lower than the students studying at the engineering faculty. Although a detailed study was required, it was claimed that the students studying at the engineering faculty would take more courses in the field of informatics, which is effective in obtaining this result. In addition, a moderately significant relationship was found between taking precautions and awareness of information security. It has been claimed that students who were more conscious of Internet security were more conscious about taking precautions in the process of providing personal cyber security.

In a study conducted in Ankara, the importance of information security awareness was examined [36]. To measure the importance of awareness within the scope of the study, a 43-question questionnaire was prepared. While conducting the research, the same questionnaire was sent to three different groups and the responses received were evaluated. The first group included 100 civil servants who worked in different departments of the same institution. The second group comprised 113 university students from different engineering departments. In the third group consisted of 100 students studying at the high school level. The participants were asked whether they had knowledge about phishing in the survey. 54 people out of 100 civil servants in the first group stated that they knew what phishing means. 12 out of 113 engineering faculty students in the second group stated that they knew the meaning of phishing. 21 out of 100 high school students in the third group stated that they knew what phishing means. According to the results of the research, it was evaluated that training, posters, and briefings should be prepared in order to increase the level of information security awareness. On the other hand, no study has been conducted on the level of contribution of awareness training, posters, and briefing preparations to cyber security awareness thereafter.

2.3. DISCUSSION

The literature we have reviewed so far shows a considerable amount of work on preventing phishing attacks.

Examples include [4], [14] and [15]. When we go into more detail, we observe that these tests were conducted in large organizations, similar to our case.

However, they did not concentrate on measuring the preventions; hence, solid results on how the tests were beneficial for the organizations are missing from our knowledge. Most mention that the test was beneficial However, such claims would remain vague and cloudy because they missed rigorous measurements to highlight positive changes.

As we have seen in the literature review, the effect of information security awareness training on increasing the cyber security awareness of people in samples has been examined in many studies. Examples of these studies are [13], [16], [17], [34] and [35]. When the details of these studies are examined, as in our study, the positive contribution of awareness training to the level of awareness can be observed.

On the other hand, the extent to which the training contributed to the level of cyber security awareness could not be determined concretely in these studies.

Among the studies examined within the scope of our study, it was observed that there are a limited number of subjects about the effects of digital bulletin publishing activities on cyber security awareness. [15] and [20] can be cited as examples of studies that include evaluations in this area. When we look at the details of these studies, the effect of publishing digital bulletins with current news and announcements on cyber security awareness has been examined, similar to our study.

On the other hand, in the above-mentioned studies, the extent to which the publication of a digital bulletin contributes to the level of cyber security awareness could not be determined with quantitative data.

In the studies we have examined within the scope of the literature review, it is clear that the solution predictions for increasing the cyber security awareness of the users in corporate organizations remain as suggestions and incentives.

Studies were carried out in the literature on the methods and benefits to be applied to increase cyber security awareness.

In the articles examined, there is information that the training to be given to the employees in order to ensure corporate cyber security would be beneficial.

Awareness training is diversified with developing technology.

A few examples of awareness training methods include:

- collective training in the form of video conferences;
- organizing surveys;
- sending digital bulletins to all personnel;
- Sharing on information screens in the workplace;
- organizing in-class training;
- conducting phishing drills; and
- providing interactive training by preparing computer games.

On the other hand, although the importance of awareness training in the field of information security is emphasized in the studies, it can be observed that the studies on measuring the level of benefits of the training in question are limited.

From this point of view, in this study, the benefits of some of the methods applied to increase cyber security awareness are discussed. The changes in the awareness level were attempted to be measured as a result of the awareness-raising activities carried out regularly and the phishing exercises carried out afterward.

Considering our discussion of the works we have studied, we have opted to concentrate on changes in the awareness of employees after the drills and tests.

The next chapter reports our approach to understanding what and how such tests can change awareness in an organization.

CHAPTER III
METHODOLOGY

3.1. ANALYSIS OF AWARENESS METHODS

When the studies in the literature are examined, it is emphasized that the level of cyber security awareness of employees in organizational structures should be increased. It is foreseen that information security awareness training will contribute to this goal in general.

A number of methods may be applied to increase cyber security awareness. Some of these include:

- Phishing drills,
- Awareness training,
- Digital bulletins,
- Information screens,
- Survey studies.

Within the scope of our study, the contribution of phishing exercises, information security awareness training, and digital bulletins in increasing the awareness level of employees was examined.

In this study, data obtained from repetitive and regular studies were used to measure and increase their awareness levels with regard to the cyber security awareness of the employees in an organization with roughly 1,000 employees. The organization requested that their names be anonymous in the study. In this chapter, we explain how the institution had collected the data.

Our measurement method for increasing the cyber security awareness of the employees was in accordance with the following criteria:

1- Increase in participation rate in awareness trainings to be implemented after the phishing exercises

2-Increase in the rate of reading bulletins after the phishing exercise and awareness training practices

3- Decrease in the number of personnel clicking malicious links in fake e-mail content in the phishing exercises after the trainings and bulletins

4- The effects of activities in changing awareness and bulletin reading rates in the long term.

Phishing exercises were carried out with fake e-mails sent to the employees. Information security bulletins were sent regularly every month and an information security awareness training was provided. Afterwards, a re-phishing exercise was carried out and the awareness levels of the users were measured.

The first phishing exercise was that of a discount agreement having been made with a fuel company. Employees were expected not to click on the button that redirects to an unsafe address in the e-mail.

After the phishing exercise was terminated and announced to all the employees, the online training video was shared with all the employees to raise awareness of information security. With regular reminder notifications, more employees became able to complete this training.

A monthly digital cyber security bulletin was sent to every employee via e-mail. The newsletter contained informative content on current cyber events, phishing attacks, and information security. In addition to the awareness training, users were expected to be vigilant against phishing attacks, thanks to the digital bulletins.

After a certain period, the phishing practice was renewed. The scenario of the second exercise was that of a vaccination campaign that was started against the COVID-19 epidemic with the thought of being a current issue. With the "Vaccination Appointment" button in the fake e-mail, users were directed to a fake "e-government" page and they were asked to enter their citizenship Identity Number and password information.

After the second phishing exercise, information security awareness training was sent to users. Users were reminded for approximately two months and they were informed to complete the training.

Along with awareness training, digital bulletins continued to be published. Details of the phishing exercise carried out were as follows:

- Issues of what users should be aware;
- How to detect whether a redirect to a fake page has been made;
- Security differences between http and https protocols; and
- Some statistical information.

These criteria were shared with users in the monthly bulletin.

After the phishing drills and other awareness-raising activities, a third phishing exercise was conducted. The scenario of this exercise was determined as a discount agreement with a chain of stores selling electronic products and a draw among the participants. In the e-mail that was sent, a button to be clicked to benefit from the discount and participate in the lottery campaign was presented. It was analyzed whether the users noticed that the relevant button was redirecting to a fake web page.

CHAPTER IV
RESULTS

4.1. PHISHING DRILLS

4.1.1. Contracted Gas Station Campaign Scenario

The data regarding the phishing exercise carried out with the contracted fuel station campaign scenario are given in Table 4.1. E-mails were sent to 100 personnel. The number of personnel reading the e-mail was 334. The number of personnel who clicked on the link that led to downloading the malicious file contained in the e-mail to the computer was 94. In addition, 47 of the 94 personnel activated the application file in the ".exe", executable format which they had downloaded to the computer. While the rate of those who clicked on the malicious link among the personnel who read the e-mail was 28.14%, the rate of the personnel who ran the malicious file among those who clicked on the link was 50%.

Table 4.1: Results of First Phishing Drill

Number of personnel who were sent e-mail	1,010
Number of personnel reading the e-mail	334
Number of personnel clicking on the link	94
Number of personnel running the malicious file	47
Percentage of personnel clicking on the link among readers (%)	28.14
Percentage of personnel who run the malicious file among those who clicked on the link (%)	50

4.1.2. Vaccination Appointment Scenario

The data regarding the phishing exercise with the scenario of starting a vaccination campaign due to the COVID-19 epidemic are given in Table 4.2.

Table 4.2: Results of Second Phishing Drill

Number of personnel who were sent e-mail	1,019
Number of personnel reading the e-mail	822
Number of personnel clicking on the link	237
Number of personnel entering information	132
Percentage of personnel clicking on the link among readers (%)	28.83
Percentage of personnel entering information among those clicking on the link (%)	55.70
Percentage of personnel who entered information among those who read the e-mail (%)	16.06

An e-mail was sent to 1,019 personnel for phishing purposes. 822 personnel read the e-mail. 237 personnel clicked on the link in the e-mail. The number of personnel who entered the information requested for the appointment on the page that opened was 132. Among those who read the e-mail, the rate of those who clicked on the harmful link was 28.83%. The rate of personnel entering information among those who clicked on the link is 55.70%. The rate of personnel who entered the information among those who read the e-mail was 16.06%.

4.1.3. Electronics Store Discount and Lottery Campaign Scenario

The data regarding the discount and lottery agreement campaign scenario with the chain of stores that sell electronic products and the phishing exercise are given in Table 4.3.

Table 4.3: Results of Third Phishing Drill

Number of personnel who were sent e-mail	1,034
Number of personnel reading the e-mail	639
Number of personnel clicking on the link	55
Percentage of personnel clicking on the link among readers (%)	8.61

The number of personnel to whom the e-mail was sent is 1,034. The number of personnel who read the e-mail was 639 and the number of personnel who clicked on the malicious link was 55. The rate of those who clicked on the harmful link among the personnel who read the e-mail was 8.61%.

4.2. CYBER SECURITY AWARENESS TRAINING

4.2.1. Awareness Training 1

The data regarding the information security awareness training held shortly after the Contracted Fuel Station Campaign Phishing exercise are listed in Table 4.4**.**

Table 4.4: Results of First Awareness Training

Number of personnel who were sent e-mail	1,015
Number of personnel reading the e-mail	921
Number of personnel completing training	525
Percentage of personnel who completed education (%)	57.00

The number of personnel sent e-mails is 1,015. The number of personnel reading the e-mail is 921. The number of personnel who completed the awareness training reached 525. The rate of those who completed the training among those who read the e-mail is 57%.

4.2.2. Awareness Training-2

The data regarding the information security awareness training carried out after the phishing exercise with the vaccination appointment scenario are given in Table 4.5.

Table 4.5: Results of Second Awareness Training

Number of personnel who were sent e-mail	1,024
Number of personnel reading the e-mail	925
Number of personnel completing training	650
Percentage of personnel who completed education (%)	70.27

The number of personnel sent e-mail is 1,024. The number of personnel reading the e-mail is 925. The number of personnel who completed the training is 650. The rate of those who completed the training sessions among those who read the e-mail is 70.27%.

4.3. READING LEVELS OF DIGITAL BULLETINS

Prior to the phishing exercises and awareness training, information security bulletins containing news about current cyber threats were shared with the personnel. Statistics about the reading rate of digital bulletins are listed in Table 4.6.

Table 4.6: Statistics about Digital Bulletins

Bulletin	**Number of personnel who were sent e-mail**	**Number of personnel reading the e-mail**	**Number of personnel reading the bulletin**	**Percentage of personnel bulletin readers among reading the e-mail (%)**
1	990	500	27	5.40
2	1,015	550	47	8.55
3	1,029	603	51	8.46
4	1,029	667	121	18.14
5	1,023	622	51	8.20
6	1,027	616	72	11.69
7	1,027	636	71	11.16
8	1,023	688	52	7.56
9	1,021	728	246	33.79
10	1,030	704	87	12.36
11	1,033	724	112	15.47

The first information security bulletin reached 990 people. Out of 990 people, 500 opened the e-mail they received. The number of personnel who clicked on the link in the e-mail to access and read the newsletter was 27. The rate of those who read the e-mail and access the newsletter was 5.40%.

After the first phishing exercise and awareness training, the reading rate of another bulletin shared with the staff was 8.55%. The reading rates of subsequent bulletins were 8.46%, 18.14%, 8.20%, 11.69%, 11.16% and 7.56%, respectively. After eight information security bulletins were published, the second phishing exercise was performed, and then the second information security awareness training was shared online with all personnel. The reading rate of the ninth information security bulletin,

which was prepared after these activities, was 33.79%. The reading rates of the other two bulletins that followed were 12.36% and 15.47%.

4.4. COMPARISON OF RESULTS

The chronological order and results of the methods applied in accordance with the methodology specified in Chapter 3 are listed in Table 4.7.

Table 4.7: Comparison of Results

Results of Methods	Bulletin Reading Rate (%)	Phishing Drills Rate (%)	Awareness Trainings Rate (%)	Date
Bulletin 1	5.4			January 2021
Phishing Drill 1		28.14		February 2021
Awareness Training 1			57.00	April 2021
Bulletin 2	8.55			June 2021
Bulletin 3	8.46			July 2021
Bulletin 4	18.14			August 2021
Bulletin 5	8.20			September 2021
Bulletin 6	11.69			October 2021
Bulletin 7	11.16			November 2021
Bulletin 8	7.56			December 2021
Phishing Drill 2		28.83		January 2022
Awareness Training 2			**70.27**	February 2022
Bulletin 9	**33.79**			January 2022
Bulletin 10	12.36			February 2022
Bulletin 11	15.47			March 2022
Phishing Drill 3		**8.61**		March 2022

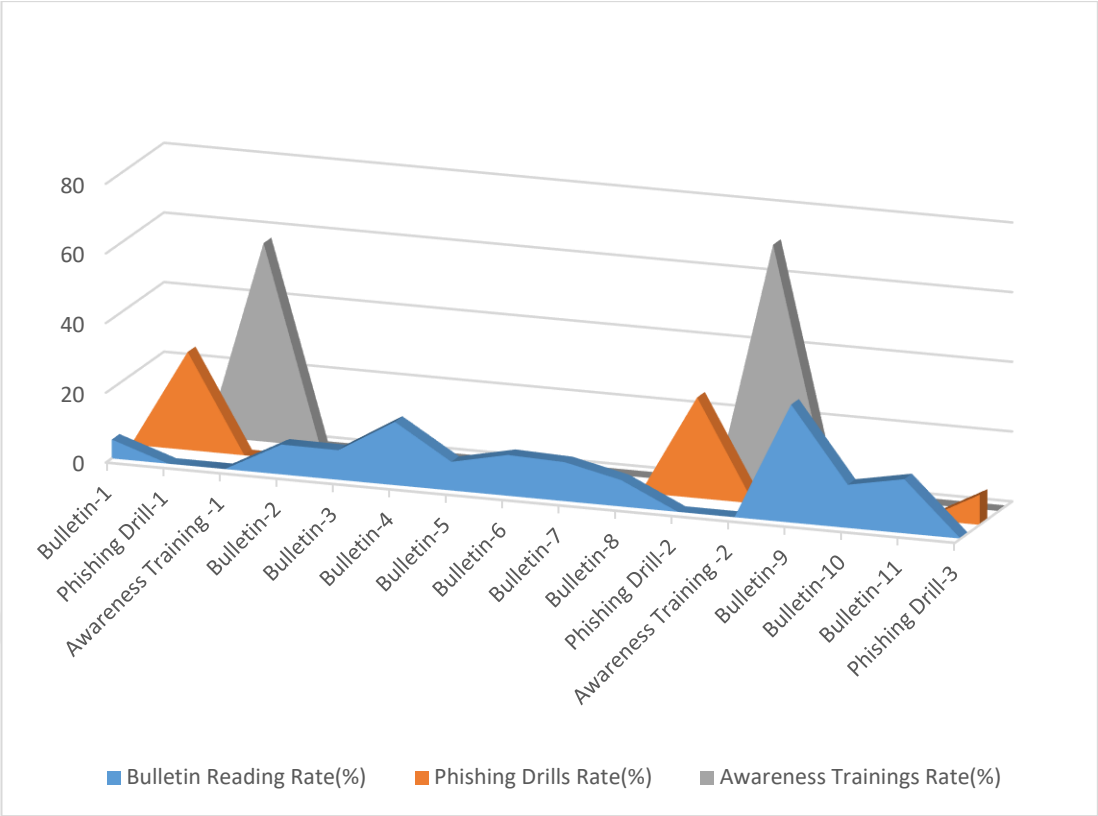

Figure 4.1: Activity results

Figure 4.1 shows bulletin reading rates (colored blue), malicious link click rates in phishing exercises (colored orange), and participation rates in awareness trainings (colored gray). It can be observed that the rate of reading the bulletins and participation in trainings increases over time. Due to the increase in awareness, a decrease was observed in the rate of personnel who clicked on fake links in the phishing attack in the long term.

On the other hand, the reading rate of the fourth bulletin increased significantly compared to the rate of the previous bulletin. Although no awareness-raising work was carried out, this change has been observed. The reason for this change could not be determined.

CHAPTER V
CONCLUSION

Survey studies conducted on different groups, such as employees from the private and public sectors, students, academicians and teachers, form the basis of the theses in the literature.

Based on the information received as a result of the surveys, the aim was to determine the level of cyber security awareness in organizations. Suggestions on which methods should be followed to increase awareness and keep awareness at a high level are also included in these studies.

We studied a dataset from a public institution with more than 1,000 personnel. Three methods had been determined to increase the awareness level of the institution's personnel. For phishing exercises, the aim was that users be aware of cyberattacks, while keeping personal and corporate information safe thanks to information security awareness training, and having information about current cyber events with information security bulletins. In addition, as a result of these studies, the change in the level of information security awareness was examined.

In this chapter, we first present our findings followed by discussions that emerged as a result of the study in the items. Then, we include the limitations of our study at the point of revealing the findings. How the limitations can be overcome and research that can be done in future studies are included in the "Future Works", Section 5.3. Finally, we recall our research question and give an answer in light of these findings.

5.1. FINDINGS

Finding 1: Organizations disclose cybersecurity breaches to the public.

Since the examples are explained in detail in Section 2.2, it is understood that the level of information security awareness of employees not only in Türkiye but also abroad is at a low level. However, when we consider public institutions and private sector organizations all over the world, it is observed that the reported information security violations are limited. It is known that many DDoS attacks are made instantly

and there are many ransomware attacks. Valuable information on which vulnerabilities have emerged against which attack is not shared by organizations. Moreover, it is not reported whether this vulnerability is caused by the user, and if in fact caused by the user, how to take precautions and train the user.

Finding 2: The research on the benefits of suggestions presented for increasing information security awareness is limited in the literature.

Studies in the literature generally include questionnaires. Survey questions focused on user habits and the importance of information security. In many studies, survey questions were sent to users by e-mail and their answers were requested via e-mail. According to the results of the survey, the information security awareness levels of users were determined. Moreover, similar to the studies carried out in Türkiye, it is observed that phishing exercises and training are organized in order to measure and improve the level of awareness in the studies carried out abroad; these are included in Section 2.2. The methods we used in our study are global. As discussed in Section 2.3, it is generally suggested that phishing drills and information security awareness training will be beneficial in increasing information security awareness. These methods have been implemented within the scope of information security management system policies. However, a second survey was mostly not applied to confirm these recommendations.

Finding 3: As a result of phishing exercises and information security awareness training, the rate of reading information security bulletins has increased in the long term.

Although written information is more reliable and more permanent, it is understood that the practices regarding the publication of digital bulletins, as in Section 2.3, are seen as a supporting element rather than the main activity. On the other hand, in the statistical data detailed in Section 4.3, it was observed that the digital bulletin first achieved a low average reading rate. In the institution where we conducted the case study, the reading rate of the last bulletin sent to the users before the phishing exercise and awareness training was slightly higher. After the phishing exercise and training activities, it was understood that the rate of reading the bulletin had increased by a factor of 1.5 in the long term. This change is an indication that phishing drills and awareness training increase users' information security awareness and interest in the bulletin.

Finding 4: As a result of information security awareness training and information security bulletins, fewer employees believe in phishing emails.

As explained in Section 4.1, the rate of personnel in the organization who clicked on the malicious link in a fake e-mail in the first phishing exercise was 28%. Furthermore, 50% of the people downloaded the malicious file after being redirected to the fake website. On the other hand, similar results were obtained in the second phishing exercise, which was carried out after awareness training and a few bulletins. After two phishing exercises, two awareness training sessions and the publication of eight different monthly bulletins, a third phishing exercise was held. As a result of the last exercise, the rate of those who clicked on the harmful link decreased to 8%. It is understood that regular activities on information security increase users' awareness of phishing attacks.

Finding 5: As a result of phishing drills and reading information security bulletins, more employees have attended the information security awareness training.

As explained in Section 4.2, the participation rate in the first information security awareness training was 57%. Afterward, bulletins were published; these bulletins contained the consequences of current cyber dangers and also news about the importance of information security. In addition, a phishing exercise was performed. After the aforementioned activities, the completion rate of the training, which was open to the online participation of the users, exceeded 70%, indicating an increase in the users' interest and need for training in information security.

Finding 6: Findings depend on the literature review and the dataset we had obtained.

In many countries, including Türkiye, information security violations in public institutions must be reported to a competent authority. On the other hand, cyberattacks between countries can be tracked by regulatory agencies and service providers over Internet traffic. However, due to institutional sensitivities, this information is not shared in open sources. For this reason, it was observed that the number of studies in this field in the articles and theses in the literature is limited. In addition, no interviews were conducted with the people who performed phishing exercises or the personnel who were exposed to phishing in the institution where our study was made. Nevertheless, partially personal experiences are included.

5.2. LIMITATIONS

Limitation 1: Verification of users and individual assessments

Phishing drills, awareness training content, and digital bulletins within the scope of the study were sent to the e-mail addresses of the users. Users opened their e-mail clients and logged in with a username and password information. Methods such as camera use and static IP address tracking were not followed to verify the personnel. All evaluations were carried out by considering the participants as a homogeneous cluster. This limitation relates to Findings 3, 4, 5 and 6.

Limitation 2: Sociological effects

While making comparisons between repetitive activities within the scope of the study, sociological changes for users were ignored. There may have been one or more factors in their respective social lives that would have positively or negatively affected the awareness level of users. This limitation relates to Findings 3, 4, 5 and 6.

5.3. FUTURE WORK

Future Work 1: Make user-specific evaluations

Within the scope of our study, all employees were handled homogeneously and an overall evaluation was made. The interactions of the personnel regarding phishing, training, and bulletins may be detected following a method involving a user name and IP address. In this way, changes in the level of information security awareness in organizations could be examined individually. Such research may be a solution to Limitation 1.

Future Work 2: Effects of social events

While evaluating the results of our study, the experiences of the users in their social lives were not included. There may have been changes in awareness levels due to different social events. In future studies, external factors as well as activities within the organization could be included in the evaluation. In addition, studies on the level of cyber security awareness may be carried out in the field of social sciences. For this reason, research could be conducted in the field of social sciences to compare with the studies that include information security analyses on the social lives of personnel. Such research may address Limitation 2.

Future Work 3: Other methods of research

Information security breaches are seldom reported. Face-to-face meetings can be held with officials from many different organizations. The responsibilities of the researcher regarding the use of data shared by companies can be determined. In this

way, a number of organizations could also share their data on cyber security incidents. Thus, more data resources pertaining to the awareness of the users can be accessed. In addition, face-to-face interviews may be conducted with the people who organize information security activities, training, and phishing exercises within the organization. Users affected by phishing may also be interviewed. The method of rewarding users with high awareness can also be determined as the fourth method in addition to our study. Such research may be a solution to Limitations 1 and 2.

5.4. CONCLUSION

The thesis concludes that it is a useful set of practices that can be applied to increase the cyber security awareness of personnel, providing information about current cyber events by preparing information security bulletins in public and private sector organizations, having users experience real attacks by performing phishing drills, and learning basic information through training.

Returning to the research question:

Can conducting phishing drills, doing awareness training, and preparing information security bulletins increase the cyber security awareness of personnel in the long term?

We can present a sound answer; through the light of the findings in Section 5.1 and by considering the limitations in Section 5.2, organizations can systematically conduct phishing drills, provide awareness training and regularly prepare information security bulletins to increase the cyber security awareness of users.

REFERENCES

[1] OK Kerem (2013), *Bilgi ve Bilgi Yönetimine Giriş*, Edition 1, DaisyScience International Publishing House, İstanbul.

[2] YILMAZ Hasan (2014), *"*TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi*"*, *Journal of Denetişim*, Volume 15, Page 45-47

[3] ITU (2009), Series X: Data Networks, Open System Communications and Security Telecommunication Security, 2009, Genova, https://www.itu.int/rec/T-REC-X.1205-200804-I, Date of access: 30.05.2022

[4] ARSLAN Yenal (2021), "Oltalama Saldırıları Farkındalık Tatbikatı Örneği*"*, *Düzce University Journal of Science and Technology*, Volume 9, Issue 3, Page 348-358

[5] ÜNAL Naci A. and ERGEN Ahu (2018), "Siber Uzayda Yeterince Güvenli Davranıyor Muyuz? İstanbul İlinde Yürütülen Nicel Bir Araştırma", *Manisa Celal Bayar University Journal of Social Sciences*, Volume 16, Issue 2, Page 191-216.

[6] HAVELSAN Siber Güvenlik Direktörlüğü (2022), Siber Güvenlik Bülteni Feb. 2022, Ankara, https://www.havelsan.com.tr/kurumsal/basin-yayin/havelsan-dijital/bultenler/siber-guvenlik-bultenleri#7721, Date of access: 16.05.2022

[7] KARABATAK Murat, MUSTAFA Twana (2018), "Performance Comparison of Classifiers on Reduced Phishing Website Dataset", 6th International Symposium on Digital Forensic and Security (ISDFS), page 1-5, Antalya

[8] BGA Security (2019), "What is a phishing attack?", Ankara, https://www.bgasecurity.com/2019/09/phishing-oltalama-saldirisi-nedir, Date of access: 01.05.2022

[9] Sparta IT Services (2019), **"**What is a phishing attack?", Ankara, https://sparta.com.tr/makaleler/oltalama-saldirisi-nedir, Date of access: 20.05.2022

[10] BURAK Ayşenur (2021), "How To Defend Against Malware, Piping Attacks And Scams During The Covid-19 Crisis?", https://arkakapidergi.com/covid-19-krizinde-kotu-amacli-yazilimlara-oltalama-saldirilarina-ve-dolandiriciliga-karsi-nasil-savunulur, Date of access: 01.06.2022

[11] BGA Security (2021), "Free Information Security Awareness Training", Ankara, https://www.bgasecurity.com/2021/11/ucretsiz-bilgi-guvenligi-farkindalik-egitimi, Date of access: 10.05.2022

[12] HWANG Inho, WAKEFIELD Robin, KIM Sanghyun and KIM Taeha (2021), "Security Awareness: The First Step in Information Security Compliance Behavior", *Journal of Computer Information Systems*, Volume 61, Issue 4, Page 345-356

[13] CHATCHALERMPUN Surachai, WUTTİDİTTACHOTTİ Pongpisit and Daengsi Therdpong (2020), "Cybersecurity Drill Test Using Phishing Attack: A Pilot Study of a Large Financial Services Firm in Thailand", IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE), Page 283-286, Malaysia

[14] ÖZDEMİR Ayşe and ULUYOL Çelebi (2021), "Kamu Kurum ve Kuruluşlarında Bilgi Güvenliği Farkındalığı", *Turkish Journal of Social Research*, Volume 25, Issue 3, Page 649-666

[15] İLERİ Yusuf Yalçın (2018), "Kurumsal Bilgi Kaynaklarına Erişimde Güvenlik: Hekimlerin Şifre Yönetimine Yönelik Bir Araştırma", *International Journal of Health Management and Strategies Research*, Volume 4, Issue 1, Page 15-25

[16] ÖZDEMİR Durmuş and ASLAY Fulya (2016), "Bilgi Güvenliği Farkındalık Eğitiminin Erzincan Halk Sağlığı Müdürlüğü Personeli Üzerindeki Etkilerinin İncelenmesi", International Symposium of Erzincan, Erzincan

[17] İLERİ Yusuf Yalçın (2017), "Örgütlerde Bilgi Güvenliği Yönetimi, Kurumsal Entegrasyon Süreci ve Örnek Bir Uygulama", *Anadolu University Journal of Social Sciences*, Volume 17, Issue 4, Page 55-72

[18] GÜNDÜZALP Cengiz (2021), "Üniversite Çalışanlarının Dijital Veri Ve Kişisel Siber Güvenlik Farkındalıkları (Bilgi Işlem Daire Başkanlıkları Örneği)", *Journal of Computer and Education Research*, Volume 9, Issue 18, Page 598-625

[19] MÜRSÜL Damla and KAYA Ali (2019), "Ulusal Bilgi Güvenliği Politikaları Açısından Kamu Kurumlarının İncelenmesi: Kayseri Barosu Örneği", *ASSAM International Refereed Journal*, Page 331-343

[20] YILDIRIM Hakan (2012), *Fiziksel ve Sanal Güvenlik Algısının TBMM Çalışanları Açısından Analizi*, Police Academy Institute of Security Sciences, Ankara

[21] TANER Emre and KILIÇ İbrahim (2019), "Güvenlik Güçlerinin Bilgi Güvenliği Farkındalığını Belirlemeye Yönelik Bir Araştırma", *Journal of Security Sciences*, Volume 8, Issue 2, Page 253-269.

[22] ÖZTEMİZ Semanur and YILMAZ Bülent (2013), "Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı: Ankara'daki Üniversite Kütüphaneleri Örneği*", Journal of Information World*, Volume 14, Issue 1, Page 87-100,

[23] ÇAKIR Hüseyin and YAŞAR Hakan (2015), *"*Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri"*, Düzce University Journal of Science and Technology*, Volume 3, Issue 2, Page 488-507

[24] ASLAY FULYA (2017), *"Siber Attack Methods and Current Situation Analysis of Turkey's Ciber Safety", International Journal of Multidisciplinary Studies and Innovative Technologies*, Volume 1, Issue 1, Page 24 - 28

[25] YILDIRIM YENİMAN Ebru (2018), "Bilişim Sistemlerine Yönelik Siber Saldırılar ve Siber Güvenliğin Sağlanması", *Journal of Vocational Science*, Volume 7, ıssue 2, Page 24-33

[26] ERDOĞAN Seyda Emir (2020), *Building an Information Security Management System, Implementation of IEC / ISO 27001 Standard In A Civil Aviation Organization*, İstanbul Kültür University Institute of Graduate Studies, İstanbul

[27] AKAL Mert (2022), *Bilişim Firmalarında Bilgi Güvenliği Farkındalığı*, Ufuk University Institute of Social Sciences, Ankara

[28] GÜLHAN Beril (2021), *Awareness of Information Security in Higher Education Institutions: The Case of Bahçeşehir University*, Bahcesehir University Graduate School of Education, İstanbul

[29] ALTINER İmren (2021), *Evaluation of Teachers' Personal Cyber Security Awareness Levels According To Different Variables*, Ankara University Graduate School of Educational Sciences, Ankara

[30] SHAW Ruey Shiang. CHEN Charlie C. HARRIS Albert L. HUANG Hui-Jou (2009), "The Impact Of Information Richness On Information Security Awareness Training Effectiveness", *Journal of Computers & Education*, Volume 52, Issue 1, Pages 92-100

[31] TSCHAKERT Kai F. NGAMSURİYAROJ Sudsanguan (2019), "Effectiveness Of And User Preferences For Security Awareness Training Methodologies", *Journal of Heliyon*, Volume 5, Issue 6

[32] ACAR Sami, ZETTER Selin A. and BAŞPINAR Nuran Ö (2018), "Çağrı Merkezi Çalışanlarının Çağrı Merkezi Teknolojileri ve Siber Saldırı-Tehdit Farkındalıkları", *International Journal of Social Sciences in Turkish Cultural Geography*, Volume 3, Issue 1, Page 1-15

[33] AKYOL Elif and UZUN Yıldız (2021), "Bilgi ve İletişim Teknolojisi Dersi Alan Sağlık Meslek Yüksekokul Öğrencilerinin Bilişim Güvenliği Farkındalığı", *Ufuk University Journal of Social Sciences Institute*, Volume 10, Issue 19, Page 69-83,

[34] AVCI Ümmühan and ORUÇ Orçun (2020), "Investigation of the Students' Personal Cyber Security Behaviour and Information Security Awareness", *Inonu University Journal of the Faculty of Education*, Volume 21, Issue 1, Page 284-303.

[35] MOĞOL Şehnaz Hilal (2016), *Importance of Information Security Awareness*, Yıldırım Beyazıt University Graduate School of Natural and Applied Sciences, Ankara