Teknik Bilimler Dergisi
Cilt 13, Sayı 2, S. 50-56, Temmuz 2023

Araştırma Makalesi

TECHNICAL SCIENCES
e-ISSN:2146-2119

Journal of Technical Science
Volume 13, No. 2, pp. 50-56, July 2023

Research Article

Examining Social Engineering Attack Vector in Line of Data Breach

Ahmet Ali SÜZEN[1*]

[1*] Isparta University of Applied Sciences, Faculty of Technology, Department of Computer Engineering, Isparta,Türkiye, (ORCID: 0000-0002-5871-1652), ahmetsuzen@isparta.edu.tr

(İlk Geliş Tarihi 05.05.2023 ve Kabul Tarihi 13.07.2023)

(**DOI:** 10.35354/tbed.1310185)

ATIF/REFERENCE: Süzen, A. A., (2023). Examining Social Engineering Attack Vector in Line of Data Breach. *Teknik Bilimler Dergisi*, 13 (2), 50-56.

Abstract

The versatile use of information and communication technologies also diversifies data sources. The data produced by data sources must reach the relevant target source within the framework of confidentiality, integrity and accessibility. These data sources are protected by technical methods within the scope of information security. The increase in data sources creates information security problems by making protection with only technical methods insufficient. Malicious attackers target the security measures of users or organizations using advanced techniques and methods. One of the most effective methods of these attacks is social engineering attacks. Social engineering is an attack vector that attackers use to force or persuade people to obtain the requested information. The human vulnerabilities that arise in the success of social engineering attacks are fear, desire to help, carelessness and comfort zone. In this study, the contribution of data breaches to social engineering attacks and the contribution of social engineering to data breaches are investigated by analyzing current data breaches from both sides (breach source and data target). At the same time, security approaches are proposed within the scope of the implementation and damage effects of social engineering attacks.

Keywords: Attack Vectors, Data Breaches, Phishing Social engineering.

Veri Sızıntıları Kapsamında Sosyal Mühendislik Saldırı Vektörünün İncelenmesi

Öz

Bilgi ve iletişim teknolojilerinin çok yönlü kullanımı veri kaynaklarını da çeşitlendirmektedir. Veri kaynakları üretilen veriler gizlilik, bütünlük ve erişebilirlik çerçevesinde ilgili hedef kaynağa ulaşmak zorundadır. Bu veri kaynakları bilgi güvenliği kapsamında teknik yöntemler ile korunmaktadır. Veri kaynaklarının artması sadece teknik yöntemler ile korumayı yetersiz hale getirerek bilgi güvenliği sorunlarını oluşturmaktadır. Kötü niyetli saldırganlar gelişmiş teknikler ve yöntemler kullanarak kullanıcıların veya kurumların güvenlik önlemlerini hedef almaktadır. Bu saldırıların en etkili yöntemlerinden biri de sosyal mühendislik saldırılarıdır. Sosyal mühendislik, saldırganların insanları zorla veya ikna ederek isteği bilgiyi elde etmek için kullandığı bir saldırı vektörüdür. Sosyal mühendislik saldırılarının başarıya ulaşmasında ortaya çıkan insan zafiyetleri korku, yardım etme isteği, dikkatsizlik ve konfor alanı olduğu görülmektedir. Bu çalışmada güncel veri sızıntıları çift yönlü (sızıntı kaynağı ve veri hedefi) incelenerek veri sızıntılarının sosyal mühendislik saldırılarına katkısı ve sosyal mühendisliğin veri sızıntılarına katkısı araştırılmıştır. Aynı zamanda sosyal mühendislik saldırılarının uygulanış biçimi ve zarar etkileri kapsamında güvenlik yaklaşımları önerilmiştir.

Anahtar Kelimeler: Sosyal mühendislik, Oltalama, Saldırı Vektörleri.

[*] Sorumlu Yazar: ahmetsuzen@isparta.edu.tr

1. Introduction

In this century, which has been called the age of technology, the widespread use of information and communication technologies has led to significant changes in both the lives of users and the business models of businesses. While ICTs are a source of many benefits for both, they also provide new opportunities to violate personal privacy. At the same time, they make it possible for personal information to be used indifferently [1].

Although the processing of data in many different data sources is based on basic operations such as storing, transmitting, and sharing data, potential security threats have also emerged, such as data being easily altered, deleted, transmitted, and falling into the wrong hands [2]. Storing corporate and personal data in electronic databases poses more threats than manual methods [3]. Especially the interconnection of corporate data sources with the spread of cloud and network technologies increases the security threat even more. Recently, artificial intelligence-based security methods have been developed to ensure data security, privacy, and accessibility. However, the increase in data breaches indicates the emergence of end-user vulnerabilities [4]. The most effective attack method against end users is social engineering attacks. Social engineering is the creation of a vulnerability in corporate or personal data sources by attackers using different methods [3-4]. Social engineering attacks and data breaches have become major problems with the security vulnerabilities brought about by the digital age. These attacks target not only individual users but also organizations. They jeopardize the security of both individuals and organizations with consequences such as theft of sensitive information, fraudulent activities, and loss of reputation.

In this study, social engineering attacks, which are the main source of recent data breaches and frequently encountered by end users, are analyzed. Social engineering attacks are based on two main factors. These are the use of the human factor as a vulnerability in accessing data sources and the realization of more effective social engineering attacks with data breaches. In the first stage, the types of social engineering attacks were evaluated through application methods. In addition, the impact of recent data breaches on social engineering attacks was analyzed. Within the scope of the social engineering attack types and vectors obtained, the precautions that the end user should take are deduced.

2. Requirements of Social Engineering Attacks

Social engineering attacks are an effective attack surface where attackers try to target people's vulnerabilities to achieve results. Social engineering attacks have certain procedures in the way they are implemented. In order to evaluate these attacks and their effects, it is necessary to first examine these topics.

2.1. Information Gathering

The main goal of social engineering attacks is to access the victim's information or information that can persuade them. Attackers try to access private information by misleading or persuading target users [5]. This information includes sensitive information such as personal information, account information, financial information, or corporate data. Information gathering processes are commonly carried out through sources such as search engines, social media accounts, corporate web pages and data breaches. Especially recently, data breaches in corporate databases, e-commerce applications and user computers have made information collection processes more effective.

2.2. Building Trust and Persuasion

One of the most effective strategies of social engineering attacks is to build trust. The more information about the victim in the form of sensitive data is transferred in the connection established by using different communication channels, the more the sense of trust increases. Likewise, the higher the degree of credibility of the corporate identity of the attacker, the higher the rate of persuasion of the victim [6]. For example, in communication tools, attackers try to create a trustworthy image by using corporate designs, logos or fake identities. Again, in attacks via calls, the sound of ambulance and radio in the background are factors that increase the degree of trust. In an attack scenario, the persuasion phase comes right after the increase in trust. Now, by predicting people's natural behaviors and reactions, attackers can have an effect on victims. For example, an attacker can scare or alarm the victim through a phone call and make the victim make sudden decisions.

2.3. Targeting Weaknesses

In social engineering attacks, attackers identify the victim's weak points and force them to be manipulated more easily. People often act with emotional and fear reactions, and this creates an opportunity for attackers [6-7]. During and after the pandemic, the news in the press sources increased people's sense of fear and curiosity, making them the target of attackers. Immediately after social events, social media and other communication tools are used to develop attacks by manipulating those events.

2.4. Timing and Urgency

In social engineering attacks, attackers often exert urgency or time pressure on their victims. In an attack scenario, the attacker pressures the victim to react quickly or to perform the desired behavior immediately. The sense of urgency and time constraints can cause the victim to perform the desired action without thinking and without checking [8].

2.5. Collective Attacks

Some organized social engineering attacks are often carried out by communities of attackers. An attacker can collaborate with other potential attackers and work together to create more impact on the victim [9]. These collective attacks provide more resources and skills and can more easily gain the trust of the victim. For example, in a certain period of time, a group of attackers can spread the claim that credit cards have been stolen and then create collective attacks with the "check if your credit card has been stolen" method.

3. Examining Social Engineering Attack Vectors

Social engineering is a discipline that uses social psychology, communication, and manipulation techniques to influence or control people’s behavior [10]. Social engineering attacks are generally based on persuasion. As a result of data breaches, personal data such as a user’s ID number, mother’s name, father’s name, phone numbers, and relatives’ information are used by

attackers. There are different types and examples of social engineering attacks. In this context, commonly used attack sources, their contents and effects are given in Table 1. Social engineering is used both as a source that feeds data breaches and as a means of persuasion to the victim.

The methods used as social engineering attacks are known as attack vectors and we can examine them under the following headings when grouped according to technique, method and target audience.

Table 1. Types Of Social Engineering Attacks and Their Effects

Attack Source	Attack context	Impact
Social Media	Join in X Bank 4 car and 2 phone lotteries	Bank account details
Social Media	Get Your Credit Card Fees Back	Credit Card details
Social Media	You have violated copyright.	Account details
Short Message	If you want to take part in TV series or movies.	Credit or debit card details
Short Message	Congratulations 100 TL coupon has been loaded to your account!	Credit or debit card details
Short Message	Your account has been frozen due to suspicious transactions!	Cryptocurrency wallet account information
E-mail	Your corporate mail quota is full!	Corporate e-mail login information
E-mail	Can you offer the attached products	Ransomware, malware, ransomware
E-mail	Your phone bill is attached.	Ransomware, malware
Calling	Enter the code sent to you so that your Whatsapp account is not closed.	Personal and Corporate Correspondence
Calling	Make high profits in the short term.	Crypto assets or bank account details
Calling	Account identified in money traffic related to terrorist acts	Bank account or credit card details

3.1. Phishing

Phishing is one of the most common and well-known types of social engineering attacks. In this method, attackers try to deceive their targets through communication such as emails, websites or messages [11]. For example, an attacker sends a fake email to the target and redirects the target to a fake website in order to obtain banking information. This website is designed in the same way as a real bank's website. These pages have no action after the target enters the username, password and authentication information.

3.2. Pretexting

Attackers create a false scenario or pretext to gain the target's trust. In this method, an attacker can pretend to be a technical support staff and request help to gain remote access to the victim's computer. After gaining remote access to an information resource, they can carry out all kinds of malicious activities at that access point [12].

3.3. Baiting

In baiting, attackers use the target's curiosity to set traps. For example, an attacker may leave a device that looks like a USB stick and contains malware in the target's path. When the victim curiously connects this device to their computer or IT assets, the malware can be exposed. It is especially preferred for public targets such as banking and public transactions [11].

3.4. Quid Pro Quo

Attackers try to gain information or access by offering a service or benefit to their victims [3]. For example, an attacker may offer a target a free WIFI connection or a gift card in exchange for the target's login credentials or other sensitive information.

3.5. Dumpster Diving

Attackers try to obtain information through documents or materials discarded by the target [4]. For example, an attacker can gain access to important information through documents removed from an organization's garbage container. The widespread use of information and communication technologies has reduced the effectiveness of this method. However, it is known as a preferred attack vector in targets where the end-user age level and technology usage is low.

3.6. Vishing

Social engineering attacks can be carried out not only in digital environments but also through one-to-one communication sources. Attackers use various tactics to manipulate the end user through phone calls to obtain information [11]. Recent personal data breaches have significantly increased the use of phone fraud. This attack method, which targets users who use technology only at the phone level, is successful for monetary targets. In this method, an attacker calls the end user by phone and convinces them that they are part of a terrorist act or a suspicious event. Thus, he tries to transfer the victim's valuable assets such as money and gold to himself.

3.7. Social Media Manipulation

Social media platforms have become an important part of people's daily lives and attackers are using them for social engineering attacks [12-13]. Social media manipulation involves trying to gain the trust of targets by creating fake profiles. Attackers can spoof victims' social media accounts or create fake content to manipulate users to gather information and fulfill their malicious intentions. They can also hack victims' social media accounts with other social engineering attack methods to launch an attack on the victim's friends list.

3.8. Tailoring

Attackers try to build trust and interest by providing targets with customized messages and content [11]. For example, an attacker may try to build trust by sending a personalized message based on the target's social media profile or past interactions.

3.9. Physical Social Engineering

Social engineering attacks can be carried out not only in digital environments but also in physical environments. Physical social engineering involves attackers convincing their targets using face-to-face interactions and social skills. With this method, an attacker gains trust by pretending to be an employee of an organization and tries to gain the target's help or information to bypass the security system [2].

3.10. Authority

Attackers try to get victims to obey by presenting themselves as authority figures. With this method, an attacker can introduce himself as a policeman, bank manager or senior executive and demand that victims perform certain actions or share information. This method is also used in combination with telephone attacks [12].

3.11. Scareware

Attackers use tactics aimed at creating fear, anxiety or panic in their victims. For example, an attacker may send a frightening message to a victim that malware has been detected on their computer or phone, or that their account has been compromised, prompting an immediate response. As a result, the victim enters personal account information or sensitive information into the attacker's decoy system [13].

3.12. Impersonation

Attackers try to build trust with victims by impersonating another person or organization [9]. For example, an attacker can pretend to be a senior manager or colleague of the victim and request information or access. It is especially used in combination with the Authority attack vector.

3.13. Influence Campaigns

Attackers try to influence communities, groups or audiences using long-term and complex manipulation strategies. For example, an attacker can manipulate public opinion or create a perception by creating fake accounts or content on social media platforms [13].

4. Assessment of Up-To-Date In Social Engineering Attacks In The Scope of Data Breaches

Data sources that produce, process and store information experience data breaches as a result of cyber-attacks in certain periods. In addition to corporate data breaches, phishing websites and end-user data breaches are also experienced. When the Darkweb and hacker forums sharing data breaches are examined, it is thought that the data groups given in Table 2 are in the hands of attackers [14]. The fact that more and more of these data groups will be in the hands of attackers in the future shows that social engineering attacks will increase linearly. When evaluated over the data groups shown in Figure 1, it is seen that the end user can easily access the most vulnerable aspects of the end user such as fear, desire to help, carelessness and comfort zone.

Figure 1. Data Groups Found by Attackers Because of Data Beaches

In order to evaluate social engineering attacks worldwide on the basis of the last 3 years, the reports of the Anti-Phishing Working Group (APWG), which conducts studies in the field of Phishing, were analyzed [15].

Looking at the number of phishing attacks in 2022 given in Table 2, the number of attacks in the first quarter of 2022 was 1,025,968 and reached 1,432,431 in the last quarter of 2022. In total, a record was broken in phishing attacks with 4.5 million attacks in 2022.

Table 2. Distribution of Phishing Attacks in 2022 by Quartiles

Year- quarter	Phishing Attacks
2022-1	1,025,968
2022-2	1,097,811
2022-3	1,270,883
2022-4	1,432,431

Figure 2 shows the graph of social engineering attacks worldwide between 2019 and 2022. It is seen that the number of attacks continues to increase in direct proportion to the increase in data breaches, especially in the last three years. The linear increase in attacks from 2019 to 2022 shows that the success effect of these attacks has also increased [15].

Figure 2. Number of Phishing Attacks Between 2019-2022

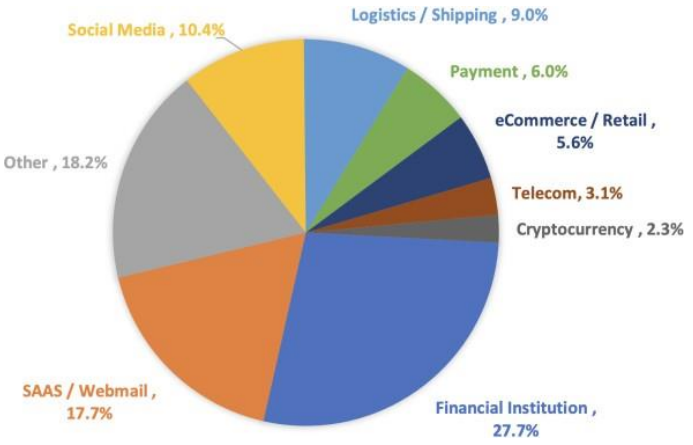

Figure 3. Distribution of Phishing Attacks in 2022 by Sectors

Figure 3 shows the distribution of phishing attacks by sectors in 2022 according to APWG reports. According to these results, it is seen that the attacks are intensely directed towards sectors involving finance and money [15].

5. Protection Methods Against Social Engineering Attacks

It is known that social engineering attack vectors are used as thirteen types on average. Both at the corporate and end- user level, social engineering attacks are at the top of cyber-attacks. Developing firewalls, intrusion detection and prevention systems are not very successful where the human factor is present. In general, the results that will occur with the success of a social engineering attack vector can be listed as follows.

- Unauthorized access,
- Theft of services,
- Loss of reputation and trust,
- Distributed service blocking,
- Access to sensitive information and data loss,
- Facing legal sanctions.

Therefore, end-user-oriented measures are being developed to counter social engineering attacks. In general, the framework of measures to be taken against social engineering attack vectors is described as follows.

5.1. End User Level Training and Awareness

Although artificial intelligence-supported behavioral prevention systems have been developed to protect corporate and personal data sources, data breaches have been increasing recently. When the main causes of data breaches are analyzed, it is seen that the human factor ranks high. The fact that human vulnerability is the main factor in corporate and personal data breaches shows that cyber security awareness is lacking.

Reducing the impact of the human factor in preventing social engineering attacks is to know where, how and by whom the attack occurs. In an organization, attack vectors should be known not only by IT personnel but also by all personnel. It is seen that corporate security, clean desk policy, information security, password security should also be evaluated within the scope of awareness trainings. At the same time, it should be aimed to raise awareness of users on these issues by pointing out that attacks can sometimes be initiated by physical activities. In this context, staff should be made aware of two different topics.

- Corporate data sources and potential phishing attacks to access them.
- Types of social media or communication-based attacks against end-users and how to detect them.

Training for end-users will have a significant impact on reducing potential threats by increasing the user's level of awareness. It is imperative that end users know which technical measures should be taken in their personal information assets. Users should implement the measures under the following headings in order to use their personal assets safely.

- Security software for internet and computer security should be installed and up-to-date on computers.
- Crack software should not be preferred.
- If the password is stored in browsers, the password should be changed in certain periods (about 6 months).
- Check which application has access to which feature of the phone (Gallery, Location, Contacts, Search, Nearby Contacts, Microphone, camera, etc.) from application permissions on mobile phones.
- At least one of the password/patterns/biometric security measures should be activated for access to information assets.
- Virtual cards should be used for internet shopping and limits should be proportional to the amount of shopping.
- Personal data should be regularly backed up to a backup device other than IT assets.

5.2. Security Policies and Technical Procedures

All organizations using information and communication technologies must establish security policies regarding the use of information resources and user responsibility. These policies include measures that the end user should know about information resources and take against their responsibilities. Organizations should establish strong security policies and procedures. These policies should include security measures such as password complexity requirements, user permissions and access control. Policies also determine the level of information security awareness of organizations. Not only determining policies but also implementing and auditing these policies are important for preventing attacks.

In order to reduce social engineering attacks and their effects, IT units should draw attention to the use of certain techniques within their organizations. It is also a mandatory requirement to carry out studies to technically reduce cyber-attack vectors. Accordingly, the technical measures to be controlled can be evaluated as follows.

Two-Factor Authentication (2FA): multi-factor authentication is a security measure that requires users to use multiple authentication methods to gain access to their accounts [16]. 2FA requires a username and password, as well as additional verification steps such as SMS verification code, key software's, biometric data or security questions. Active use of 2FA will help prevent unauthorized access to accounts by attackers.

Technological and Administrative Measures: Corporate and individual users should take technological measures to protect their data sources. Ransomware viruses, especially those

transmitted through social engineering, render data unusable. At this point, personal and corporate data should be backed up regularly and periodically to a different data source (cloud, external disk, in-network backup device, etc.). The fact that users use unlicensed software and do not follow the updates (operating system, antivirus software, database management systems, package programs, etc.) regularly gives attackers an opportunity.

Recognizing and Reporting Suspicious Content: IT staff recognizing and reporting suspicious emails, links or other potential threats is an important scenario for staff awareness for the organization. In particular, organizations using firewalls should integrate resources that share URLs for social engineering purposes. At the same time, they should periodically create social engineering attack vectors and share them with the organization's personnel.

Employee Authorization Audit: Especially in organizations with multiple departments, each department's work activities and data sources differ. Within the organization, departments such as IT or management can access the data sources of other departments. In some internal organizations, there is no restriction on access to data sources, so every employee can access every data source. In such scenarios, it is seen that all data belonging to the organization is at risk in a possible social engineering attack. One of the most important measures against social engineering attacks is the creation and control of an internal authorization matrix. Each organization must define which personnel will be authorized to access which data source and must be audited periodically. At the same time, authorization and auditing should be applied within the physical security mechanism of this audit. These include the use of ID cards, security cameras and access control [17].

Penetration Tests: Organizations that use information and communication resources generally either have IT personnel or outsource support. Many software and hardware resources have vulnerabilities at certain periods. In some cases, vulnerabilities arise due to incorrect or incomplete configuration. If there are in-house software technologies (web page, mobile application, management software, etc.), vulnerabilities may also arise. All these vulnerabilities cannot be discovered by in-house IT personnel. Therefore, penetration tests of information assets should be performed periodically to analyze the current situation [18]. Necessary measures and precautions should be taken within the scope of the penetration test report.

6. Conclusion

In these years of intense use of the Internet and social media, social engineering attacks are heavily favored by two different groups of attackers. The first group includes attackers targeting financial fraud, and these attackers aim to cause financial damage to users by using data breaches. The second group of attackers uses social engineering attacks as the vector of a cyber-attack. This group of attackers tries to get a door from the inside by using the human factor in case there is no technical vulnerability in a system or security measures are high. In this study, social engineering methods are analyzed through attack vectors. The impact of recent personal data breaches on social engineering attacks has been evaluated and measures against these attack types have been evaluated.

References

[1] Acılar, A., & Baştuğ, A. (2016). Social Engineering: An Information Security Threat in Enterprises. Global Business Research Congress (GİAK-2016), Işık University, Şile, 26-27.

[2] Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89.

[3] Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. Computers & Security, 73, 102-113.

[4] Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. IEEE Access, 9, 11895-11910.

[5] M. Z. Gündüz and R. Daş, (2016). Social Engineering: Common Attacks and Security Measures, 9th International Conference on Information Security and Cryptology, 2016.

[6] Anıl Keskin, D. & Gözenman, S. (2019). Social Engineering in terms of Cheating Risk. TIDE AcademIA Research, 1 (2) , 281-306

[7] Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. Computers & Security, 73, 102-113.

[8] Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. IEEE Access, 8, 85094-85115.

[9] Breda, F., Barbosa, H., & Morais, T. (2017). Social engineering and cyber security. In INTED2017 Proceedings (pp. 4204-4211). IATED.

[10] Yathiraju, N., Jakka, G., Parisa, S. K., & Oni, O. (2022). Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security: A Survey of Social Engineering Attacks and Steps for Mitigation of These Attacks. In Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security (pp. 110-132). IGI global.

[11] Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. Comput. Syst. Sci. Eng., 40(3), 1153-1166.

[12] Alkayem, N. F., Cao, M., Shen, L., Fu, R., & Šumarac, D. (2022). The combined social engineering particle swarm optimization for real-world engineering problems: A case study of model-based structural health monitoring. Applied Soft Computing, 123, 108919.

[13] Ferreira, A., & Lenzini, G. (2015, July). An analysis of social engineering principles in effective phishing. In 2015 Workshop on Socio-Technical Aspects in Security and Trust (pp. 9-16). IEEE.

[14] Deguara, N., Paracha, A., Arshad, J., & Azad, M. A. (2023, February). Threat Miner-A Text Analysis Engine for Threat

Identification Using Dark Web Data. In 2022 IEEE International Conference on Big Data. IEEE.

[15] Anti-Phishing Working Group, 2023, Access Date: 30.04.2023, Access Link: https://apwg.org/trendsreports/

[16] Petsas, T., Tsirantonakis, G., Athanasopoulos, E., & Ioannidis, S. (2015, April). Two-factor authentication: is the world ready? Quantifying 2FA adoption. In Proceedings of the eighth european workshop on system security (pp. 1-7).

[17] Brenner, J. (2007). ISO 27001 risk management and compliance. Risk management, 54(1), 24-29.

[18] Bacudio, A. G., Yuan, X., Chu, B. T. B., & Jones, M. (2011). An overview of penetration testing. International Journal of Network Security & Its Applications, 3(6), 19.