MYKOLAS ROMERIS UNIVERSITY
FACULTY OF PUBLIC GOVERNANCE AND BUSINESS

SEYMA TOPALOGLU

CYBERSECURITY MANAGEMENT

MODELING OF PUBLIC RELATIONS (PR) STRATEGIES FOR CYBER THREAT AWARENESS

Master thesis

Supervisor -

assoc. prof. dr. Tadas Limba

Vilnius 2023

LIST OF TABLES

LIST OF FIGURES

CONTENT

INTRODUCTION

Novelty and relevance of the topic. Parallel to technical advancements, cyberattacks have increased in frequency, speed, sophistication, and harm. Cyber threats and crimes include stealing personal data, fraud, and fraudulent activities, violations of privacy, threats, and blackmail, cyberbullying, violations of moral rules, smuggling, terrorist activities, and stealing, selling, and publishing strategic and confidential documents of companies and states. On the other hand, considering cyberspace's breadth, the threat's source can be unlimited.

Organizations may encounter some unexpected threats as a result of the current fierce competition environment. The threat of cyber-attack is one of them. It is critical for organizations to develop a strategic model for these challenges in order to anticipate risks and build corporate defences against them.

This study investigates public relations studies for cyber threat awareness and strategic models that can be created against cyber threats. The findings of this study are based on a thorough review of the literature, chronological order, consideration of current developments, exemplification, and comparison.

Scientific issue. A successful cyberattack can have significant consequences for an organization's operations, impacting its revenue and damaging its reputation and consumer confidence. Assessing public awareness of cyberattacks is crucial. Leclair and Keeley (2015) emphasize the importance of raising awareness in areas that directly influence the future of security. By establishing a metric for awareness, the public's understanding of cyberattacks can be measured for training purposes and to meet the objectives of the training.

Cyber security is bolstered by hardware and software investments in IT infrastructures. Yet, cyber security is still out of reach, even with these investments. Genuine cyber maturity requires amplified awareness of cyber security among the public. Despite cutting-edge security products, a user can still accidentally reveal their password or open a malicious email. Investing in information security awareness is, thus, just as essential as investing in hardware and software.

The object of the research. Public relations activities for cyber-security awareness will be used to design a conceptual framework.

The purpose of the study. Cyber-defence is now a crucial task globally and locally due to the rise of cyber threats. "Security" refers to the state of being protected from various dangers such as physical, psychological, financial, and emotional hazards. It impacts communities, nations, and businesses and has a crucial impact on individual safety. "Security" is becoming a vital factor for the success of both public and private sector corporations and enterprises. (Robert Fischer, Halibozek,E & Walters,D, 2012).

The goal is also to prevent the theft of private information through exploitation and security breaches, which are common forms of cybercrime. Various proactive policies, laws, and standards regulate these issues and protect our data and privacy. (Smith, H.Dinev, T& Xu.H, 2011). However, laws cannot completely prevent cyber threats as the public is not sufficiently informed about cyber threats.

In the field of cyber threat awareness, on the one hand, increasing user awareness and education levels come to the fore as a national priority. On the other hand, there is a need for the training of professionals who manage and operate institutions and people who use these technologies. Non-formal and formal education projects to create a cyber security culture, as well as in-service training activities, are implemented through detailed action plans in many country strategies.

Cyber-Threats are constantly changing and changing with the changing technology.

It has become a necessity for private and public institutions to raise public awareness by determining public relations strategies in this field. The aim of this thesis is to compare the cyber threat awareness levels of the public. In addition to this main purpose, society's awareness of cyber threats; The differentiation status according to variables such as age, gender, educational status, rural and urban living spaces, and social media usage was examined.

Research Question and Hypotheses. Research question: To what extent is the public aware of the cyber threats and how to protect themselves, and what can be done to increase public awareness and education?

H1. “The general public's awareness of cyber threats appears to be limited, and they may not proactively seek information on this subject.”

H2. "Age and level of education are significant factors in determining the level of public awareness of cyber threats and protective measures."

H3. “Public service announcements raising public awareness of cyber threats or posts on digital platforms informing the public about cyber threats effectively to reach target audiences.”

H4. "The training and events organized by public institutions and the private sector to raise awareness about cyber security are insufficient."

H5. "Cyber-attacks can damage a business's reputation and erode the trust its customers have in it."

Research design The research will be divided into four main sections. The first section will cover the definition and practice of public relations. The second section will delve into the concepts of cyber security and cyber threats, emphasizing the importance of cyber security awareness. The third section will analyze the results of the Cyber Security Awareness Survey. Finally, the fourth section will present a model designed to implement public relations strategies aimed at increasing awareness of cyber threats. The research will conclude with recommendations for improving the implementation of public relations strategies, and a visual structure of the thesis is presented in Figure 1.

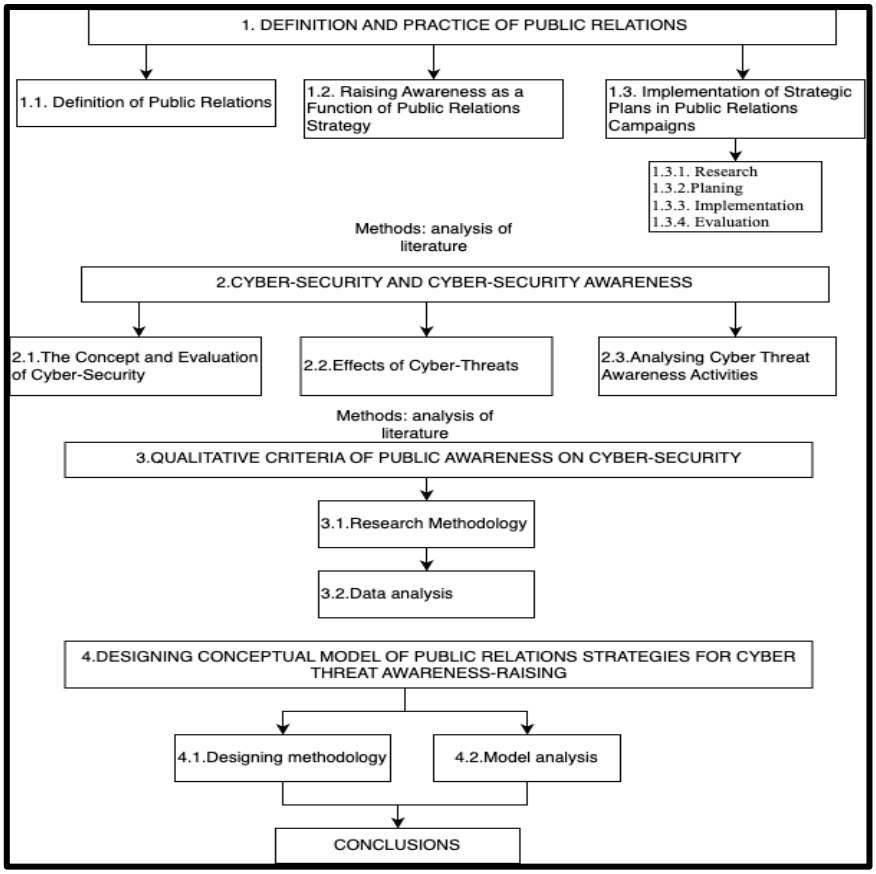


Figure 1. The visual structure of the thesis

1. DEFINITION AND PRACTICE OF PUBLIC RELATIONS

1.1. Definition of Public Relations

Public Relations, commonly abbreviated as PR, is a term used across a wide range of industries and is associated with a diverse set of skills and competencies among experts to some extent. As a result, there is no universally accepted definition of what Public Relations actually means. (L'Etang, 2008).

The field of Public Relations can be valuable in our pluralistic society, aiding in the effective attainment of objectives and decisions by promoting shared empathy between institutions and groups and harmonizing public and private policies. It serves a diverse range of organizations, including the business community, trade unions, government agencies, educational institutions, foundations, hospitals, religious groups, voluntary associations, and the tourism sector (Harlow,

1976). To achieve their goals, these organizations need to establish real relationships with various targeted audiences or the public, including customers, local communities, employees, members, shareholders, society in general, and other organizations (Harris, 1997).

To achieve corporate objectives, it is crucial for managerial staff in institutions to understand the values and attitudes of their target audience. Often, external government policies shape these objectives. Public Relations practitioners play a crucial role in translating specific objectives into policies and actions that are publicly acceptable by advising and mediating management (Agee, 1998). According to Wilcox (1992), the concept of public relations includes a management function, comprehensive objectives, and activities, two-way interactive communication, and the understanding that public corporations are plural, not singular (i.e., consumers). Public relations emphasizes long-term relationships rather than short-term goals.

Up-to-date descriptions of public relations definition emphasize the construction of jointly helpful ties among various publics and organizations. However, Professor Glen Cameron at the University of Missouri School of Journalism has offered an ambitious approach. Public relations is demarcated as deliberate competition management and dispute for the advantage of the corporation and, where feasible, for the joint advantage of the several peoples or stakeholders and the organization at large" (Reber, 2015). However, memorizing any definition of public relations it is not necessary. It is more important to know the keywords that are used in most explanations framing the current up-to-date public relations keywords (Reber, 2015);

■ Deliberate; Public relations endeavor is deliberate and is a scheme to understand, persuade, receive feedback from the affected ones, and provide information.

■ Planned; Public relations is a recognized activity of as organized one. When the activities take place after a while, resolutions to difficulties are exposed and coordination is considered. It is systematic and requires a strategic way of thinking and research.

■ Performance; Actual policies and performance are the evaluation were of Public Relations effectiveness. If the organization's policies are weak and do not respond to public problems, public relations is not expected to generate any goodwill and support.

■ Public interest; Tasks of public relations ought to provide communal profit for the community and the organization; the personal concerns of the organization are aligned with the welfare and concerns of the public.

■ Two-way communication; The operation of Public relations is not just mean to spread information, but also the art of speaking and listening to various public opinions.

■ Management function; The activities of Public relations are effective when the integral part of decision-making and the top management is strategic. The practice of public relations includes consulting, conflict management, competition, and problem-solving.

1.2. Raising Awareness as a Function of Public Relations Strategy

In the context of public administration, public relations aims to achieve a balance between the policies of the administration and the expectations of the target audience. The goal is to create a consensus within the framework of the concept of public interest. Public relations in public administration serves two main purposes: promoting services to the target audience and ensuring their support for policies. (Sen, F., 2012).

From the literature, we can infer that public relations engage in public relations activities to achieve various objectives, including promoting the public interest, meeting social expectations, establishing two-way communication and interaction, facilitating governance, raising awareness of social issues, keeping up with trends, gaining social support, managing positive image and reputation, and responding to crises. Although there are various purposes in government public relations, the role of public relations in developing social consciousness and awareness of social problems will be emphasized here. In this framework, we will try to clarify the conceptual framework of our thesis by giving definitions of developing social consciousness and awareness of social problems.

The term "awareness" refers to having knowledge and understanding of the existence or occurrence of something (Awareness, 2023). As awareness is more outwardly-focused than consciousness, it can have a greater impact on behavior. In the context of public relations, increasing awareness among the target audience is crucial for influencing behavior because

individuals can only respond to situations of which they are aware. The process of raising awareness involves providing information to the target audience about a potential problem and ensuring their comprehension of the issue. Government public relations practices can play a role in informing the target audience about issues that may pose a social problem and making them aware of these concerns. Individuals have the right to access information produced by the state, and it is essential that this right is legally protected. The right to information should be available to all members of society, regardless of their education, income, gender, or occupation. (Canoz, 2008).

1.3. Implementation of Strategic Plans in Public Relations Campaigns

Effective public relations campaigns require the persuasion of target audiences and the development of communication, which must be based on solid foundations. (Sezgin, 2007) A process management approach is necessary for carrying out successful public relations campaigns within a system. To achieve this, it is advisable to conduct such campaigns in four distinct steps, which are: Bicakci (2006)

-research,

-planning

- implementation

-evaluation.

1.3.1. Research

The initial phase of any public relations campaign is the research stage. This involves the systematic and well-organized collection of data to identify and address issues that arise, along with the analysis and interpretation of the data. In order to establish effective communication, it is essential to understand the target audience in public relations practices, just as individuals need to understand the people they encounter. Conducting research is a reliable way to achieve this (Özer, 2009). Therefore, the information gathered through research will become the cornerstone of any successful public relations campaign (Başok, Coşkun, 2008).

The research process involves a set of sequential steps that need to be followed, which include problem identification, analysis, and data collection.

Problem Identification: Questions related to the problem are to be solved at this stage and hypotheses are developed. (Özer, 2009).

Analysis: In the analysis phase, the target is determined. Based on the data, target groups are examined in detail and communication opportunities with target groups are identified (Özer, 2009).

Data Collection: The collecting data phase is important for the success of public relations practices. The collected pieces of information constitute the content of the public relations campaign. In order to collect information in public relations practices are:

-surveys,

-observations,

-methods. (Okay, Okay, 2014).

1.3.2. Planing

Planning is crucial in public relations and requires answering questions such as what needs to be accomplished, how it should be achieved, when it should be executed, who the target audience is, and who will carry out the plan. By providing answers to these questions in advance, a comprehensive and effective plan can be developed. (Karadeniz, 2010).

Planning a Strategy: A strategy is a general approach to be created for the project in the project process. A strategy should be determined after research (Başok and Coşkun, 2008).

Planning Budget: To ensure the success of a public relations campaign, it is imperative to prepare a budget in advance. This budget should outline the tools and methods to be employed, the duration of the campaign, the total cost of the campaign, and whether the budget is being used efficiently.

By preparing a comprehensive budget for a public relations campaign, the likelihood of achieving desired outcomes can be increased.

Planing Media: In public relations practices, media planning involves identifying the most effective media channels to reach the target audience with appropriate messages. (Okay, Okay, 2014).

1.3.3. Implementation

The implementation phase is often considered the most challenging stage in public relations campaigns. This stage involves executing the plans and decisions developed by public relations experts, based on the information gathered. Common tools used in the implementation process include campaign plans, programs, and calendars. (Karadeniz, 2010).

1.3.4. Evaluation

The final stage of public relations campaigns is the evaluation phase, which involves assessing the results of the campaign according to a predetermined plan. During this phase, practitioners seek to answer important questions such as whether the plans were developed correctly, whether the desired objectives were achieved, whether effective communication was established with the target audience and whether the program costs were in line with expectations. The evaluation phase is critical for measuring the success of the campaign and identifying areas for improvement in future campaigns. (Bicakci, 2006).

2. CYBER-SECURITY AND CYBER-SECURITY AWARENESS

2.1. The Concept and Evaluation of Cyber-Security

Cyber-Security: Cybersecurity is essential for the success of organizations, nations, and industries. System management professionals have the responsibility to ensure the protection of business activities with security policies and protection strategies. This is essential for the sustainability of economic and business activities.

Cyber security is the practice of protecting digital assets from unauthorized access, damage, and disruption. (Ryder & Madhavan, 2019). Cyber security systems protect digital and physical assets

from cyber-attacks, vulnerabilities, and damages. The goal of cyber security is to inhibit cyber-attacks, minimize vulnerabilities and damages, and optimize recovery time, as outlined in the United States Cyber Space Strategy. (Westby, 2004).

The European Union's cybersecurity authority, ENISA, defines cybersecurity as; *"all of the activities necessary to protect cyberspace, its users, and those affected by cyber threats"*. (ENISA, 2009)

In its 2017 cybersecurity terminology booklet, ENISA identifies nine core principles: confidentiality, integrity, availability, reliability, sustainability, resilience, flexibility, accountability, and authenticity. (EU Commission Decision, 2000) ENISA divides security areas necessary for a successful cybersecurity plan into layers based on Maslow's Pyramid of Needs.

Source: ENISA, 2017, p. 4

Figure 2. Layers of cybersecurity protection

The content of concepts and measures can be defined as follows:

-*Basic Security Protection*: This security layer allows users to take an active role in protecting themselves from cyber threats. As it is the foundation of cybersecurity, users must be trained in

recognizing and reacting to risks. To further increase users' knowledge, formal training, and awareness-raising activities are recommended.

-*Critical Infrastructures Protection*: This layer aims to protect public service networks and digital services. In order to achieve this, it is stated that critical infrastructure sectors and security requirements should be determined by using legal regulations.

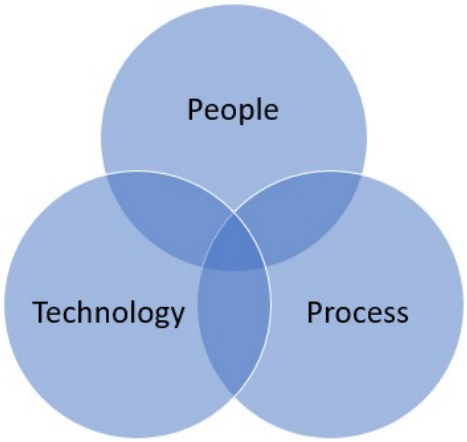
-*Digital Single Market Protection*: Cyber developments bring advantages to capital and consumers yet make them vulnerable to cyber interference. Cybercrime sabotages, and espionage can target organizations and individuals, leading to economic harm.

Global Stability Protection: War and espionage have been used throughout history and now occur in cyberspace too. International actors are working to foster global stability by creating cyber norms and diplomacy through cooperation.

Democracy and Human Rights Protection: Rapid technological advances in the lives of individuals bring with them problems related to human rights and democracy. Therefore, it is necessary to protect these concepts and EU values also in the internet environment. In this context, appropriate measures should be taken to safeguard these values in cyberspace.

Cybersecurity under the framework of basic security goals involves the protection of a structure composed of three intermingling elements: process, people, and technology. (EU Commission 2001)

The three pillars of cyber-security are described below:



Source: Mjdsystems 2020,

Figure 3. Three pillars of cyber-security

People: According to the Human Factor report, a study conducted in 2019, attackers mostly target people instead of working systems in order to install malware, steal confidential information or defraud. Attackers focus on the human factor in 99% of breaches, using social engineering to attack targets in email, social media, and cloud applications. Forging emails, compromising credentials or uploading malicious attachments to cloud applications is easier and more advantageous than a costly, time-consuming attack with a high probability of failure. It is noted that a significant proportion of attacks depend on human interaction, such as clicking on a link in a phishing email or opening a malicious file. Security experts have noted that social engineering plays an important role in these attacks and that these attacks will continue no matter how advanced security technologies become. The fact that one out of every four phishing emails in 2018 was related to Microsoft products is also one of the important details highlighted in the research.(Korucu, O. 2021)

Process: To effectively combat cyber-attacks, organizations must establish specific units dedicated to this task. Developing and implementing information security strategies, policies, processes, procedures, and instructions that align with the organizational structure is crucial. Although it is impossible to cover all aspects of these policies and processes here, a process-specific approach is necessary to ensure cyber security. This means examining how situations should be handled and by whom. Furthermore, processes should be continuously improved. Defined processes are

essential for efficiently managing corporate operations. They must be carried out in an organized, effective, and consistent manner to guide people on how to perform their tasks. The list below outlines some of the processes that organizations must have in place to engage in cybersecurity activities: (Clarke, R. A., & Knake, R. K, 2010)

· Continuous Security Monitoring

· Cyber Incident Management and Response

· Identity and Access Management

· Log Management

· Call Management

· Change Management

· Cyber Threat and Intelligence Management

· Vulnerability Management

· Risk Management

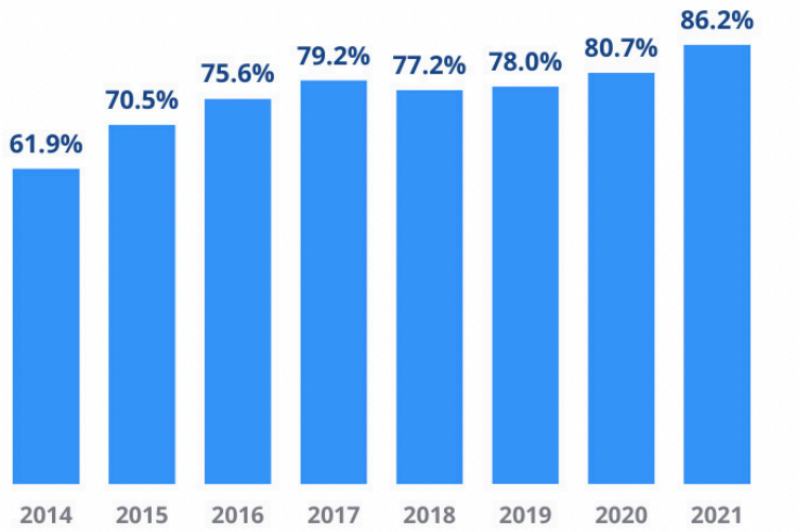
Technology: The protection of organizational systems against cyber-attacks is dependent on technology. It has become crucial to provide various technologies that ensure cyber security. Cybersecurity experts should be trained to manage these technologies effectively. After developing processes, organizations must implement the latest technological advancements. Assets that need protection can be classified into three categories: personal endpoint devices, networks, and clouds. Several technologies such as firewalls, DNS filters, anti-malware, antivirus solutions, and email security are commonly used to protect these assets. (Quinn Kiser, 2020)

Cyber Threat: Cyber threats can have a range of adverse impacts on businesses, both tangible (data warehouses, computing devices, industrial control systems) and intangible (profits). Scholars have difficulty precisely classifying cyber threats, but they typically fall into two categories: basic technical errors (e.g., system defects) which may have unintentional operational impacts, and

malicious acts (e.g., finance, marketing, production impacts) that affect all levels of an organization. (Progrebna & Skilton, 2019).

Cyber threat categorization provides enterprises with the benefit of reduced costs and improved focus on their main targets. Visuals, maps, and schedules help to paint a better picture of cyber security constraints for management. Cyber threats can be classified based on their descriptions and severity, which can determine the assets they target. For example, hacktivist activity is a severe threat with the aim of creating political tension in countries, regions, or companies. (Tari Schreider, et.al, 2017). Vulnerability is a measure of an object's, system's, or organization's weak points. In cyberspace, vulnerability can be evaluated based on its probability of resulting in a threat. Cyber vulnerability indicates potential gaps in a digital system, leading to risk when exposed to cyber threats. To calculate the vulnerability level of an organization to cyber threats, one must analyze the possible ways of accessing data, an object, or an asset. However, this is often hard to predict due to the unpredictable nature of human behavior and cyberspace circumstances. Thus, the encounter of a vulnerability and cyber threat is often hard to foresee. (Progrebna & Skilton, 2019).

Critical assets are essential to an organization, as their destruction can cause large costs and losses. Risk profiles for organizations are determined by their operating sectors, and cyber security precautions are developed with the IT department to help protect them. (Lopez, Setola, & Wolthusen, 2012).



Source: Cyber-Edge 2021 p.7,

Figure 4. Statistics of cyber-attacks from 2014-2021 per organization have increased.

Cybercrime: Cyber risks based on cyber threats and organizational weaknesses can cause tangible and intangible harm to enterprises, leading to unexpected costs. Cybercrimes are intentional attacks meant to damage physical and intellectual values, such as viruses, worms, trojans, spamming, denial service assaults, ransomware, identity forging, and data theft. Cyber security governance rules conduct, and ethics are continually changing to address cybercrime concerns worldwide. (Jain, 2005). Terrorists exploit cyberspace to implement numerous forms of attacks. These include spreading propaganda, radicalizing societies, and raising funds under the guise of a legal organization. Their intent is to undermine public and private businesses by degrading their strategic infrastructure and vital assets, thus damaging their reputations and market value (Trim & Yang-Im, 2014).

Xingan Li divides the history of cybercrime into four stages: "germination" (1940-1960), "rapid development" (1970-1990), "broad expansion" (the 1990s), and "routinization" (2020s). (Li, J. X., 2017) The first prosecuted financial cybercrime in history occurred during the "germination" stage and it took eight years (1958-1966) to prosecute. It was revealed that an employee had used a company's computer to embezzle money from long terms accounts. (Parker, D. B 1989) This time period shows that in the absence of a comprehensive legal structure, the criminal justice system is unable to work efficiently.

Malware such as Trojans, viruses, worms, and logic bombs surged in the 1980s. As the number of PC users increased with the introduction of the World Wide Web, cybercrimes became an international problem. However, convictions dropped significantly from the previous stage. (Li, J. X. 2017).

Cybercrime is the use of the internet or internet-enabled devices to commit unlawful acts. (Koziarski, J., & Lee, J. R. 2020). Cybercrime is generally defined as any illegal activity committed via an internet-connected device. It takes advantage of the specific aspects of cyberspace and would not be possible without technology. Examples of cybercrime include both computers and the internet. (Furnell, S. 2002).

Cybercrimes include data interference, system interference, illegally obtaining and distributing data, preventing the functioning of a system, altering, deleting, or corrupting data,

and misuse of devices. Offenses such as child exploitation, sexual harassment, threats, blackmail, xenophobia, racism, extremism, drug trafficking, money laundering, and terrorism are regarded as cybercrimes when a suspect uses computer-related technology to break rules or laws. Thus, cybercrime is determined by what a suspect is capable of doing with their computer.

It is impossible to tackle cybercrime and provide adequate cybersecurity with only one agency or organization. Working together is essential to protect internet users. Therefore, to prevent cybercrimes, find the culprits, make reparations, and punish them, cooperation between parties is necessary, as well as proper management of public relations regarding cyber threats.

2.2. Effects of Cyber-Threats

The interconnected information technology objects that rely on the internet and communication infrastructure are essential for meeting the needs of individuals, institutions, and communities. Public services, including communication, education, energy, transportation, water, health, security, and finance, increasingly rely on critical systems and infrastructure. However, this growth also poses significant security challenges that must be addressed to safeguard against cyber threats, which can exploit vulnerabilities in any network-connected object. To mitigate these risks, it is crucial to raise awareness of cybersecurity not only through technical defenses but also by instilling a culture of security across society. This section will explore the effects of cyber threats.

The negative impact of cyber-security threats on firm performance is a significant concern, although the extent of the impact may vary depending on the circumstances and the company involved. When a breach occurs, the firm's control over its business operations is temporarily lost, leading to disruptions in sales and revenues (Hovav, A. & Gnizy, I., 2017). To maintain a consistent level of performance, businesses must ensure that their operations remain uninterrupted, but cyber threats make it difficult to achieve this goal. These illegal activities hinder the ability of businesses to meet customer needs and retain them over time (Juma'h, A. H., & Alnsour, Y. 2020). The presence of numerous substitutes in the market means that even a single incident can result in customer loss. Furthermore, the loss of control over the delivery of goods and services due to a breach can lead to a decline in firm performance. In some cases, firms can recover from breaches,

while in others, permanent damage may occur. Regardless, it is clear that cyber-security threats are a major obstacle preventing firms from achieving optimal performance levels (Hovav, A. & Gnizy, I., 2017). While this problem is well-known, it is crucial for businesses to continuously work towards mitigating risks and adopting techniques that can ensure the security of their systems in the long term.

In the current business environment, customer loyalty is crucial for companies as it is challenging to not only attract new customers but also retain them. Customer loyalty is imperative as it drives customers to repeatedly choose a particular brand (Biga et al., 2016). The increasing availability of substitutes and evolving customer behavior and requirements are among the main factors that contribute to decreased brand loyalty. Cybersecurity threats have emerged as a significant cause of poor customer loyalty, as customers lose trust in companies that experience data breaches. This occurs because customers are concerned about the exposure of their personal information and financial security (Jeong et al., 2019). In online businesses, customers are often asked to provide their banking information or other financial details for transactions, which can lead to disloyalty. If a company is associated with a cybersecurity breach, it becomes difficult to regain customer trust and attract new customers (Bhardwaj, A. & Goundar, S., 2019). Customers today are well-informed and consider the potential risks, seeking to minimize the risk of financial loss by making informed choices.

Online businesses face significant challenges due to the heightened risk of privacy breaches. Companies must address this issue, and while initiatives such as artificial intelligence and improved IT strategies have shown some improvement, there is still much work to be done. Furthermore, customer requirements are constantly changing, resulting in a general decrease in brand loyalty (Biga et al., 2016).

To address the challenge of decreasing brand loyalty, companies are introducing new products and marketing strategies aimed at regaining customer loyalty. However, if a cybersecurity breach occurs, customers are likely to switch to a brand with better protection and fewer risks of information breaches (Ettredge et al., 2018). The issue of trust is a crucial aspect affected by cyber-security threats, which has led to changes in consumer behavior regarding brand selection. The rising number of threats and breaches in online businesses has made individuals more cautious

about online activities, resulting in a loss of trust in organizations (Yeboah-Boateng, E. O., 2018). Fraudulent activities have made customers doubtful about sharing personal data, as they face an equal threat along with the company. These incidents have had an adverse impact on the sales and profitability of businesses (Ettredge et al., 2018). Hackers have played a significant role in eroding trust, as increasing breaches have contributed to a loss of trust between consumers and companies. Once a breach occurs, consumers related to the specific brand may permanently lose trust, making it challenging for firms to retain such customers (Whitler, K.A. & Farris, P.W. 2017). Safety is a critical factor for consumers in any transaction with an organization. Businesses that prioritize safety can achieve loyalty, enhance trust, and build better relationships with their customers (Juma'h, A. H., & Alnsour, Y. 2020).

The impact of cyber-security threats on businesses is multifaceted, with one of the most critical effects being lower sales. Breaches in online security have made consumers wary of providing their personal information and conducting transactions online, leading to decreased sales and lower trust in businesses (Daud et al., 2018). This issue is particularly pronounced for newly established businesses that lack a solid brand image and reputation, as they find it difficult to attract customers and reassure them about the safety of their personal information (Whitler, K.A. & Farris, P.W. 2017). Even established businesses that have not experienced security breaches have been impacted by the loss of trust in online businesses overall. Despite these risks, many consumers still rely on online businesses, and those that have established a strong reputation in the industry continue to maintain significant sales and revenues (Biga et al., 2016).

To overcome the challenges posed by cyber-security threats, businesses must continue to improve their systems and processes to mitigate risks. Multinational companies have been actively engaged in developing strategies to ensure that cyber-security threats do not negatively impact their sales and business effectiveness. While these strategies have yielded varied results, it is essential for all companies to make a constant effort to retain their position in the industry and build trust with their customers (Juma'h, A. H., & Alnsour, Y. 2020).

2.3. Analysing Cyber Threat Awareness Activities

According to a report by the UK's Government Code and Cypher School, the majority of successful cyber-attacks, around 80%, are a result of users of the attacked system failing to meet basic security

requirements, indicating that errors or neglect on the part of the user are responsible for most cyber-attack methods. (ENISA, 2016)

In this context, with the approach that everyone who is part of cyberspace is responsible for cybersecurity, cyber awareness activities are carried out worldwide, primarily by institutions and organizations, to encourage internet users to take the relevant measures. (Ankara University 2018). Referring to this situation, the EU (2019/881) emphasizes that not only public authorities but also the behavior of civilian users in cyberspace is important in ensuring cybersecurity. (ENISA 2019)

The EU (ENISA Overview of Cybersecurity and Related Terminology) stresses the importance of individuals, businesses, and organizations taking regular measures to reduce cybersecurity risks, which are referred to as "cyber hygiene."

Thus, the measures of cyber hygiene typically include conducting anti-virus scans to examine all files and emails entering the system (to prevent phishing attacks), creating strong and updated passwords for accounts, regularly backing up data, conducting network security audits, and keeping up with software and hardware updates. (ENISA, "Review of Cyber Hygiene Practices")

The European Network and Information Security Agency (ENISA) has published a poster outlining 7 golden rules for online safety. These rules include:

"-Think very carefully about what you write online, it can be read by people after 10 years!

-Do not chat with strangers, and never arrange a meeting with someone you do not know!

-Computer viruses can be transmitted online as easily as in the real world! Always use a firewall and updated antivirus software!

-Never share your name or password with anybody!

-Never share personal information (address, phone, school name, sports club).

-Be polite and treat others the way you would like to be treated!

-If someone threatens you online, immediately inform your teachers and parents!"

The EU designates October of each year as Cybersecurity Month and conducts cybersecurity awareness studies in member states during this time to promote cyber hygiene among citizens. ENISA has placed cyber hygiene and cyber awareness as the foundational step in ensuring cybersecurity, at the base of its pyramid of layers of protection of cyberspace, to ensure active user participation in this regard.

Source: Enisa, 2022

Figure 5. The deployment report of the European Cybersecurity Month (ECSM) for 2021

A literature search through 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:

- A study investigated the information security awareness levels of employees in public institutions. Over 501 undergraduates, including IT department employees and other departments' employees, participated. Education was a major factor and stats showed that university graduates were more aware than those with high school or below education. However, no data were collected on the efficacy of awareness training. Nonetheless, a link was found between increased education and increased security awareness overall. (Ileri Yusuf Yalcin, 2018),

- A study was conducted to measure the cyber security awareness of employees of a financial institution in Thailand. To ensure fast monetary transactions and maintain service quality, an SLA with stakeholders is essential. Hence, employees need to respond quickly and effectively to

customer requests. The study was done through an e-mail phishing exercise with 20,500 employees and 700 managers. The scenario was a fake URL in the e-mail content and a password-protected page. 72.9% of managers rejected the e-mail, and 3% (21) opened it. 85 clicked the link, while 81 opened and entered the password on the phishing page. 76.77% of other employees didn't open it, 1.32% opened it but didn't click, and 6.96% opened and clicked. 14.95% (3063) opened, clicked, and entered the password. The study predicted employee awareness levels, but no testing took place after. Its aim was to measure and increase awareness through phishing. (Ayse Ozdemir & Celebi Uluyol, 2021).

-A study conducted in South Korea showed that factors such as awareness training, management participation in security, and physical security can influence information security awareness. Additionally, the mutual impact of these factors was evaluated. The hypothesis, “Information Security Education is positively related to Information Security Awareness," was tested using a questionnaire sent to 3,000 people from three public institutions in South Korea. The results affirmed the hypothesis, demonstrating that employee participation in awareness training had a significant positive effect on their consideration of security processes and procedures.: The survey results confirmed the hypothesis that cyber security awareness and awareness training are positively correlated. (Chatchalermpun S., 2020)

- A study conducted in Istanbul examined people's behavior on the internet [4]. The population included individuals aged 18 or over who lived in Istanbul and were sampled using convenience sampling. Data were collected from 335 respondents via an online questionnaire with a 95% confidence interval. The study showed that employees at private sector companies have higher cyber security awareness than those in public institutions. (Unal Naci A. & Ergen A., 2018)

-Another study of 153 students at a Taiwanese university evaluated the effects of three different educational environments (hypermedia with intense visual content, multimedia with medium visual content, and hypertext with low visual content) on cyber security awareness. Thirty subtopics, including e-mail management, were covered in all classes, and a 20-question multiple-choice test was conducted to measure students’ awareness levels. Results showed the hypermedia environment was the most effective in raising security awareness, followed by multimedia and

hypertext, respectively. Hypermedia combines both textual and visual content unlike hypertext and multimedia environments. (Kai Florian Tschakert , 2019).

- Another study of the experiences and outcomes of installing an information security management system at a 1,200-bed Medical Faculty Hospital with an automation system for medical and administrative procedures, capable of 2,000 simultaneous users. During a three-year ISMS installation period, six specialists provided annual training to an average of 1,217 personnel, totaling 23 hours per person. Maintaining employee awareness and keeping the issue on the agenda was ensured with regular e-mails and system messages and security warnings and reminders placed in key locations within the hospital. In the year prior to the ISMS integration, 13 major cyber threats disrupted the institution's info systems at an annual rate of 6%. 72% of these threats originated from human error. After 3 years of training, the total number of threats to information resources decreased by 95%; the human error rate dropped to 40%. In the 2 years following the ISMS installation, the system outage rate declined to 1%. After 3 years, no significant threats to information resources were detected. It was determined that employee training was effective in increasing cybersecurity awareness**.** (Gunduzalp C., 2021).

Kritzinger and von Solms (2010) explored a new approach to protecting individual users: cyber security awareness. The study's findings showed that those who do not create awareness of cyber security leave themselves open to the risk of multiple cybercrimes.

Yu, W., Xu, G., Chen, Z. ve Moulema, P. (2013) investigated a cloud computing architecture for cyber security awareness. Their research suggested storing and processing sizeable, monitored data in order to generate cyber security awareness. Consequently, they proposed a cloud computing-based architecture for achieving this goal.

Korpela (2015) used data analytics to examine the advantages and disadvantages of introducing awareness and training programs for cyber security. He noted that such measures are an effective way of preventing cybercrime.

Articles studied demonstrate that providing employees and students with cyber security training would be beneficial, emphasizing the importance of awareness training. Technology advances have diversified awareness training.

Examples of awareness training methods include:

- Organize group training.
- Creating surveys for data collection.
- Emailing bulletins to all staff or students.
- Displaying shared information on workplace screens can be beneficial for workflows.
- Running cyber-attack simulations.

3. QUALITATIVE CRITERIA OF PUBLIC AWARENESS ON CYBER-SECURITY

3.1. Research Methodology

Issue of the research. The imperative for the public to be cognizant of cyber threats is crucial. Despite multiple studies conducted by both public and private sectors on this issue, the extent of their impact remains uncertain.

The object of the research. measuring cyber security awareness

The goal of the research. In order to assess the impact of cyber security awareness campaigns, conducting a comprehensive evaluation that includes the measurement of individuals' cyber security awareness levels.

The qualitative research method. In the study, a questionnaire was used as a data collection method. The questionnaire is a specially prepared tool to reveal important information to be used in the analysis. It is also a method for collecting data from the community (Babbie, E. 2007).

The questionnaire was prepared by the researcher in research of the literature described in the previous chapters and the overall aim of the thesis. Carefully crafted questionnaires provide the same type of data from all different respondents. The questionnaire used basically consists of 4 sections. In the first part of the questionnaire, closed-ended questions (gender, age, marital status, education level) were asked to determine the socio-demographic and some other personal characteristics of the respondents. In the second part, Social Media Usage and Cyber Security Information were included, and in the third part of the questionnaire, the effects of cyber threat

awareness campaigns developed by the researcher by reviewing the literature, and in the fourth part, the personal cyber security awareness scale in end users consisting of 25 items were included to determine the level of personal cyber security awareness (Annex- 1). Each item on the scale was subjected to a 5-point Likert-type rating and was determined as 1= Strongly disagree, 2= Disagree, 3= Neither agree nor disagree, 4= Agree and 5= Strongly agree. The data were analyzed with IBM SPSS Statistics 26.0 software and the socio-demographic and some other individual characteristics of the public employees were shown with frequency and percentage distribution. On the other hand, each item in the scale was described with frequency and percentage distribution as well as arithmetic mean and standard deviation values.

3.2. Data analysis

Table 1: Descriptive Statistics and Reliability Analysis Results of Personal Cyber Security Scale Scores

	Min.	**Max.**	**Centre.**	**ss.**	**Skewness**	**kurtosis**	**Cronbach Alpha**
Protecting Personal Privacy	10	50	36,24	8,53	-0,973	1,285	0,869
Avoiding Untrusted Sources	4	20	12,45	4,58	0,118	-0,847	0,813
Taking Preventive Measures	5	25	14,47	5,18	0,346	-0,967	0,827
Protecting Payment Information	2	10	6,70	2,70	-0,453	-1,197	0,910
Managing Digital Footprint	4	20	11,83	4,27	0,277	-1,068	0,824
Ensuring Personal Cyber Security	25	116	81,68	14,99	-0,478	2,146	0,837

The kurtosis and skewness values of the scores calculated according to the scale information between +3 and -3 are considered sufficient for normal distribution (Hopkins & Weeks, 1990). Accordingly, it is determined that the scores of Ensuring Personal Cyber Security ensured normality (Skewness / Kurtosis: -3:+3).

It is appropriate to use parametric methods in the analysis. Reliability levels of the Ensuring Personal Cyber Security scale were calculated.

It is stated that Cronbach's alpha coefficient varies between 0-1, and according to the evaluation criteria, "if 0.00-0.40, the scale is not reliable, if 0.40-0.60, the scale is of low reliability if 0.60-0.80, the scale is reliable and if 0.80-1.00, the scale is highly reliable" (Nunnaly, 1967, 257-258). As a result, the reliability of the Ensuring Personal Cyber Security scale is very high (Cronbach Alpha>0.800).

Statistical Tests:

Data were analyzed with SPSS 26.0 program and 95% confidence level was used. Frequency (n) and percentage (%) statistics were given for categorical (qualitative) variables, and mean, standard deviation (mean±ss), minimum, and maximum statistics were given for quantitative variables.

In the study, independent groups t and one-way ANOVA tests were used to compare the scores of Ensuring Personal Cyber Security according to the groups, and Chi-square test was used in the relationships between grouped variables.

Independent samples t is a test technique used to compare two independent groups in terms of a quantitative variable.

One-way ANOVA is a test technique used to compare more than two independent groups (k=group>2) in terms of a quantitative variable. Chi-square test is a test technique used to determine the relationships between grouped variables.

FINDINGS

Table 2: Distribution of Demographic Characteristics:

		n	**%**
Gender	Male	108	43,0
	Female	143	57,0
Age (18-67 Mean=37)	20 and under	21	8,4
	21-30	100	39,8
	31-40	51	20,3
	41-60	56	22,3
	Over 60	23	9,2
Education status	Below High School	5	2,0
	High School	64	25,5
	University	156	62,2
	Master's and Doctorate	26	10,4
Employment status	Employee	131	52,2
	Unemployed	58	23,1
	Retired/Pensioner	39	15,5
	Student	23	9,2
Place of residence	Large urban	171	68,1
	District or town	64	25,5
	Rural area	16	6,4

Of the respondents, 57.0% were female, 39.8% were 21-30 years old, 62.2% were university graduates, 52.2% were employed, and 68.1% lived in Large urban areas.

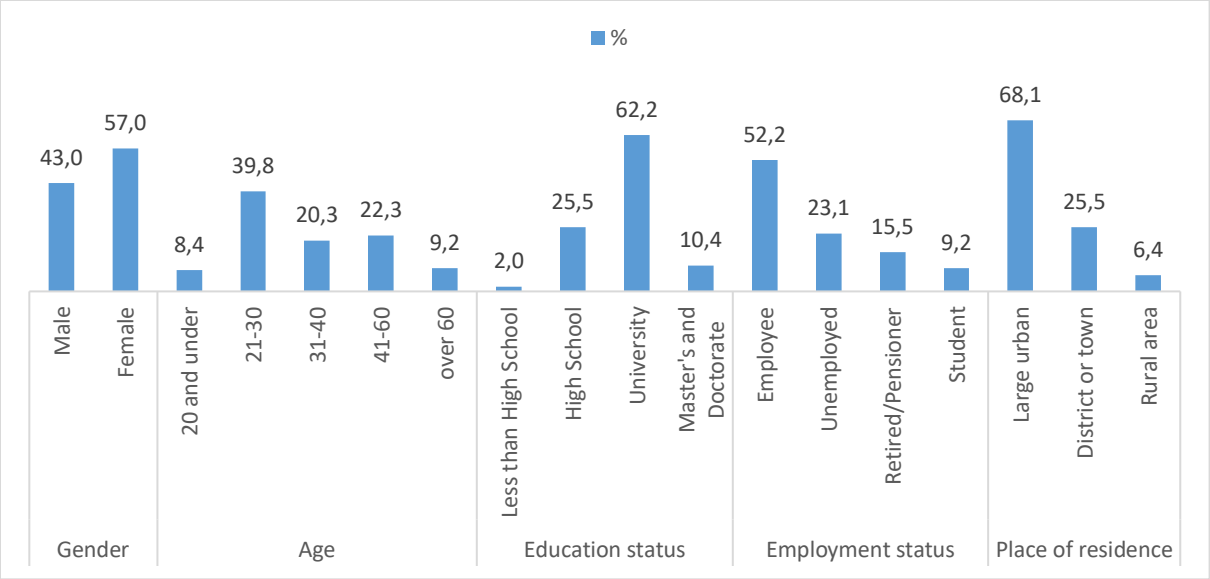


Figure 6. Distribution of Demographic Characteristics

Table 3. Distribution of Social Media, Cyber Crime Information

		n	%
Time spent on social media per day	Never	66	26,3
	Less than 1 hour	102	40,6
	1-2 hours	60	23,9
	3-4 hours	23	9,2
	More than 4 hours	0	0,0
Social Media Networks**	Facebook	86	34,3
	Instagram	173	68,9
	Twitter	120	47,8
	Youtube	170	67,7
	TikTok	40	15,9
	WhatsApp	164	65,3
	Other	16	6,4
Being victim of cybercrime on the internet, social media	Yes	60	23,9
	No.	191	76,1
Type of cybercrime encountered**	Identity theft	56	22,3
	Stolen Bank Card information	40	15,9
	SMS/Telephone fraud	55	21,9
	Online Shopping scams	50	19,9
Using mobile banking applications	Yes	214	85,3
	No.	37	14,7
Using the e-government application	Yes	208	82,9
	No.	43	17,1

***More than one elective*

40.6% of respondents spend less than 1 hour on social media daily, 68.9% spend time on Instagram, 67.7% on Youtube, and 65.3% on WhatsApp.

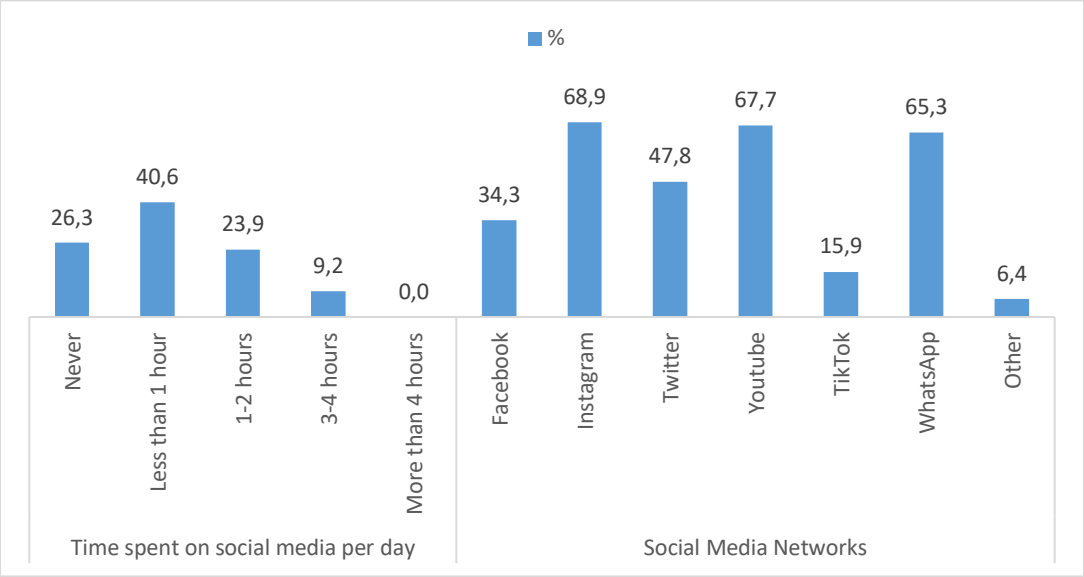


Figure 7. Distribution of Social Media,

23.9% of the respondents were exposed to cybercrime on the internet and social media, 22.3% experienced Identity theft and 21.9% experienced SMS/phone fraud. Of those who responded to the survey, 85.3% use mobile banking applications and 82.9% use the e-government application.

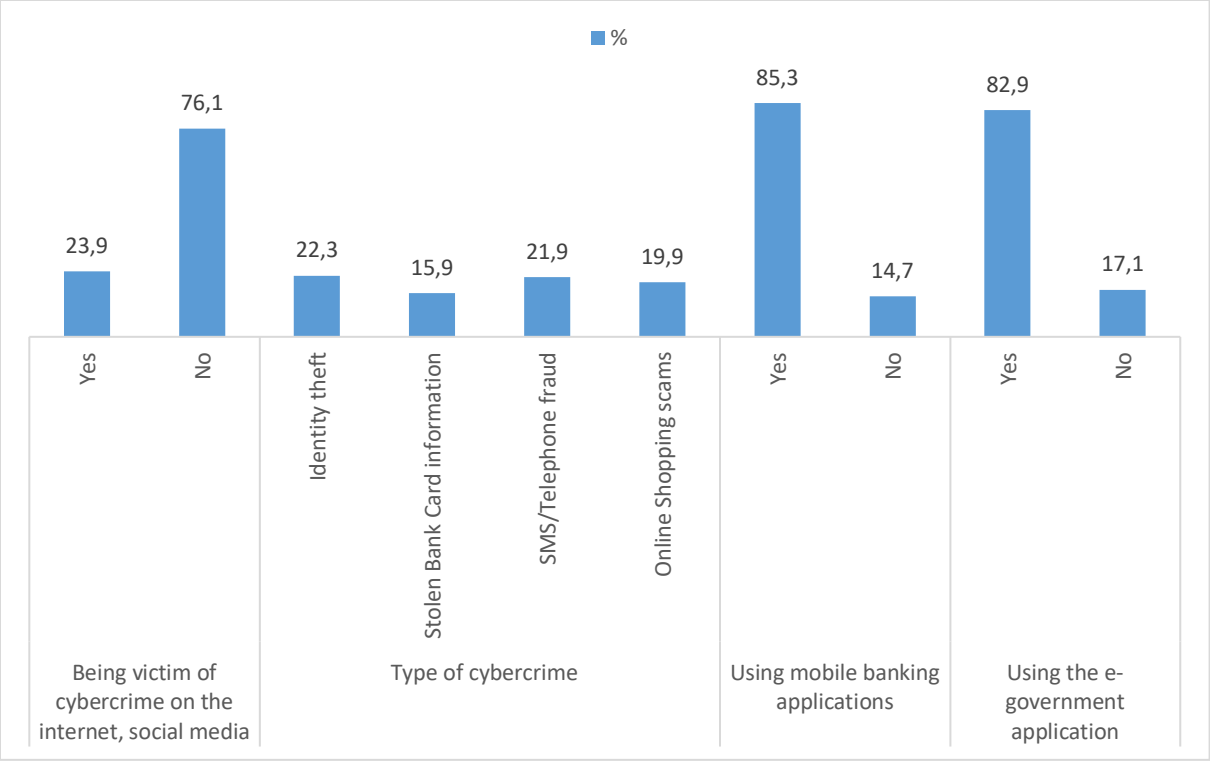


Figure 8. Cyber Crime Information

Table 4: Distribution of Cyber Threats Awareness Information

	Yes		No.	
	n	**%**	**n**	**%**
Have you seen a public service announcement raising public awareness of cyber threats?	138	55,0	113	45,0
Have you seen any posts on digital platforms informing the public about cyber threats?	151	60,2	100	39,8
Have you ever attended any cyber-awareness training at school?	61	24,3	190	75,7
Are you aware of the laws and rights of information security?	87	34,7	164	65,3
Do you have any information about the policies taken by the government to ensure cyber security nationally and internationally?	84	33,5	167	66,5
Have you heard of the European Union Agency for Network and Information Security (ENISA)?	108	43,0	143	57,0
Would you be a customer of a company that has experienced a cyber security crisis before?	74	29,5	177	70,5
Do you search about cyber security on the internet?	89	35,5	162	64,5
Have you received information or joined training on cyber security at work?	56	22,3	195	77,7

55.0% of the respondents have seen a public service announcement on the subject, 60.2% have seen informative posts on digital platforms, 24.3% have received cyber awareness training at school. 34.7% of the respondents have information about the laws set by the state, 33.5% have information about the cyber security policies. 43.0% of the respondents have heard of the ENISA

organization. 29.5% of the respondents stated that they would prefer a company that has experienced a cyber security crisis before. 35.5% of respondents searching about cyber security, 22.3% of respondents stated that information and training on cyber security are provided in the workplace.

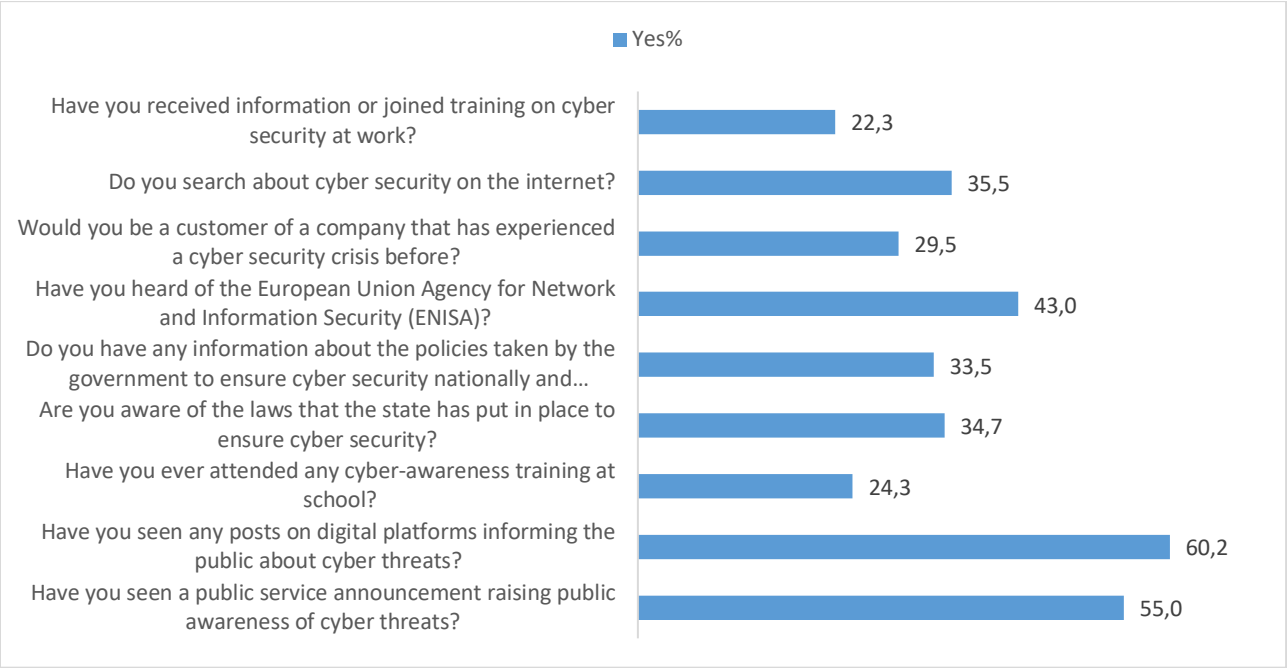


Figure 9. Distribution of Cyber Threats Awareness Information

Table 5: Levels of Agreement Regarding the Scale Statements of Ensuring Personal Cyber Security:

	1		2		3		4		5		Centre
	n	%	n	%	n	%	n	%	n	%	
I purchase products on social media ads	46	18,3	69	27,5	59	23,5	59	23,5	18	7,2	2,74
I open e-mail attachments from people I do not know	114	45,4	59	23,5	43	17,1	17	6,8	18	7,2	2,07
I respond to emails from banks and online shopping website	80	31,9	103	41,0	24	9,6	30	12,0	14	5,6	2,18
I share my personal information on the internet when necessary (ID No, date of birth, etc.)	62	24,7	70	27,9	35	13,9	55	21,9	29	11,6	2,68
I share my personal information on social media	64	25,5	105	41,8	30	12,0	39	15,5	13	5,2	2,33
I make video or voice calls with people I don't know	103	41,0	70	27,9	38	15,1	20	8,0	20	8,0	2,14
I create passwords easy to remember ("123", birthday, etc...)	102	40,6	72	28,7	19	7,6	31	12,4	27	10,8	2,24
I often share my location on the internet	83	33,1	59	23,5	61	24,3	28	11,2	20	8,0	2,37
I reply to authentication messages received by e-mail	82	32,7	82	32,7	48	19,1	25	10,0	14	5,6	2,23
I use same password for all my internet accounts	50	19,9	77	30,7	36	14,3	54	21,5	34	13,5	2,78
I don't sign up for websites that I don't trust.	35	13,9	55	21,9	49	19,5	37	14,7	75	29,9	3,25
I don't accept unusual payment requests	47	18,7	47	18,7	33	13,1	47	18,7	77	30,7	3,24

I don’t accept friend requests that I don't know on social media	34	13,5	55	21,9	37	14,7	58	23,1	67	26,7	3,27
I download files from insecure websites	62	24,7	56	22,3	71	28,3	23	9,2	39	15,5	2,69
I update the software I use	25	10,0	64	25,5	44	17,5	74	29,5	44	17,5	3,19
I have antivirus software on my computers	48	19,1	69	27,5	33	13,1	37	14,7	64	25,5	3,00
I check an SSL certificate on any website	66	26,3	66	26,3	47	18,7	37	14,7	35	13,9	2,64
I avoid using simple strings when setting my passwords	37	14,7	61	24,3	65	25,9	34	13,5	54	21,5	3,03
I change the security settings of my web browser	49	19,5	84	33,5	59	23,5	34	13,5	25	10,0	2,61
I do online shopping from my personal device	31	12,4	44	17,5	37	14,7	87	34,7	52	20,7	3,34
I do internet banking transactions from my personal device	49	19,5	30	12,0	28	11,2	69	27,5	75	29,9	3,36
I change the passwords regularly (email, social networks etc..)	51	20,3	103	41,0	51	20,3	28	11,2	18	7,2	2,44
I clear my browsing data	34	13,5	63	25,1	55	21,9	50	19,9	49	19,5	3,07
I log out of my internet accounts	36	14,3	84	33,5	43	17,1	30	12,0	58	23,1	2,96
I make sure no personal data is left on other devices	25	10,0	57	22,7	50	19,9	40	15,9	79	31,5	3,36

1:Strongly disagree,...,5:Strongly agree

The level of participation of the respondents to the scale statements of Ensuring Personal Cyber-Security is given. The statements with the highest level of agreement are as follows:

- I make sure no personal data is left on other devices
- I do Internet banking transactions from my personal device
- I do online shopping from my personal device
- I don’t accept friend requests that I don't know on social media
- I don’t sign up for websites that I don’t trust.
- I don’t accept unusual payment requests
- I update the software I use

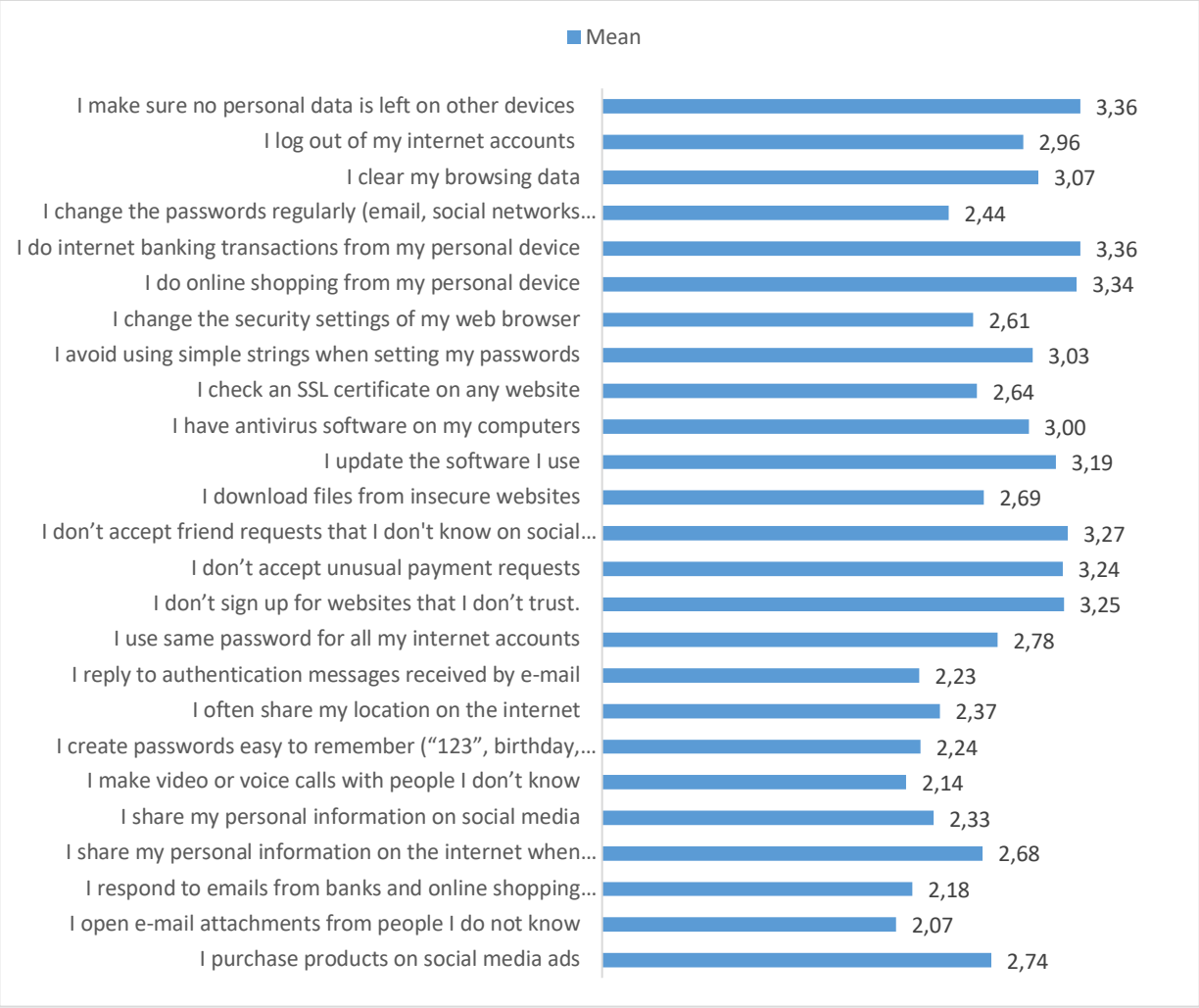


Figure 10. Levels of Agreement Regarding the Scale Statements of Ensuring Personal Cyber Security

Table 6: Comparison of Personal Cyber Security Scale Scores by Gender:

		n	Centre	ss	t	p
Protecting Personal Privacy	Male	108	38,97	6,81	4,769	**0,000***
	Female	143	34,17	9,12		
Avoiding Untrusted Sources	Male	108	11,94	5,15	-1,491	**0,138**
	Female	143	12,83	4,08		
Taking Preventive Measures	Male	108	14,32	5,14	-0,377	**0,706**
	Female	143	14,57	5,23		
Protecting Payment Information	Male	108	6,80	2,77	0,483	**0,629**
	Female	143	6,63	2,66		
Managing Digital Footprint	Male	108	12,42	4,04	1,906	**0,058**
	Female	143	11,38	4,40		
	Male	108	84,44	15,25	2,548	**0,011***

Ensuring Personal Cyber Security	Female	143	79,59	14,49		

**p<0,05 significant difference, p>0,05 no significant difference; t test*

There is a statistically significant difference between men and women in terms of Protecting Personal Privacy and Ensuring Personal Cyber Security scores (p<0.05). Men have higher levels of Protecting Personal Privacy (38.97) and Ensuring Personal Cyber Security (84.44). There is no significant difference in terms of other scale scores (p>0.05).

Table 7: Comparison of Personal Cyber Security Scale Scores by Age

		n	Centre	ss	F	p
Protecting Personal Privacy	20 and below	21	30,19	10,57	8,577	**0,000***
	21-30	100	34,12	8,15		
	31-40	51	39,51	7,87		
	41-60	56	37,73	8,29		
	Over 60	23	40,09	3,62		
Avoiding Untrusted Sources	20 and below	21	12,10	4,31	6,495	**0,000***
	21-30	100	13,87	4,21		
	31-40	51	12,59	4,78		
	41-60	56	10,20	4,22		
	Over 60	23	11,74	4,76		
Taking Preventive Measures	20 and below	21	14,81	6,03	3,749	**0,006***
	21-30	100	15,69	5,29		
	31-40	51	14,55	4,86		
	41-60	56	12,95	5,06		
	Over 60	23	12,35	3,17		
Protecting Payment Information	20 and below	21	5,90	2,55	12,693	**0,000***
	21-30	100	7,21	2,57		
	31-40	51	8,16	1,87		
	41-60	56	5,63	2,93		
	Over 60	23	4,61	1,97		
Managing Digital Footprint	20 and below	21	11,95	4,15	2,641	**0,034***
	21-30	100	12,46	4,24		
	31-40	51	12,24	3,66		
	41-60	56	11,21	4,97		
	Over 60	23	9,57	3,12		
Ensuring Personal Cyber Security	20 and below	21	74,95	13,38	4,501	**0,002***
	21-30	100	83,35	15,82		
	31-40	51	87,04	16,10		
	41-60	56	77,71	12,77		
	Over 60	23	78,35	9,63		

**p<0,05 significant difference, p>0,05 no significant difference; ANOVA test*

There is a statistically significant difference between those of different ages in terms of Protecting Personal Privacy, Avoiding Untrusted Sources, Taking Precautions, Protecting Payment Information, Managing Digital Footprint, and Ensuring Personal Cyber Security scores (p<0.05).

Those over 60 years of age have a higher perception level of Protecting Personal Privacy (40.09), those aged 21-30 have a higher perception level of Avoiding Unreliability (13.87), Taking Preventive Measures (15.69), Managing Digital Footprint (12.46), and those aged 31-40 have a higher perception level of Protecting Payment Information (8.16) and Ensuring Personal Cyber Security (87.04).

Table 8: Comparison of Personal Cyber Security Scale Scores by Education Level:

		n	Centre.	ss.	F	p
Protecting Personal Privacy	High school and less	69	33,33	10,91	6,596	**0,002***
	University	156	37,67	6,66		
	Master's and doctorate	26	35,38	9,62		
Avoiding Untrusted Sources	High school and less	69	10,80	4,01	6,958	**0,001***
	University	156	12,94	4,55		
	Master's and doctorate	26	13,88	5,15		
Taking Preventive Measures	High school and less	69	12,61	5,73	8,321	**0,000***
	University	156	14,88	4,74		
	Master's and doctorate	26	16,92	4,74		
Protecting Payment Information	High school and less	69	5,29	2,57	14,874	**0,000***
	University	156	7,16	2,68		
	Master's and doctorate	26	7,69	1,64		
Managing Digital Footprint	High school and less	69	10,55	4,29	16,180	**0,000***
	University	156	11,73	3,93		
	Master's and doctorate	26	15,81	3,92		
Ensuring Personal Cyber Security	High school and less	69	72,58	15,67	22,154	**0,000***
	University	156	84,37	12,80		
	Master's and doctorate	26	89,69	14,89		

**p<0,05 significant difference, p>0,05 no significant difference; ANOVA test*

There is a statistically significant difference between those with different educational backgrounds in terms of Protecting Personal Privacy, Avoiding Untrusted Sources, Taking Precautions, Protecting Payment Information, Managing Digital Footprint, and Ensuring Personal Cyber Security scores ($p<0.05$). The perception levels of master's and doctorate graduates on Avoiding Unreliability (13.88), Taking Preventive Measures (16.92), Managing Digital Footprint (15.81), Protecting Payment Information (7.69), Ensuring Personal Cyber Security (89.69), and the perceived level of university graduates on Protecting Personal Privacy (37.67) are higher.

Table 9: Comparison of Personal Cyber Security Scale Scores according to Employment Status:

		n	Centre.	ss	F	p
Protecting Personal Privacy	Employee	131	37,24	6,95	1,609	**0,188**
	Unemployed	58	34,34	9,17		
	Retired/Pensioner	39	35,79	11,05		

	Student	23	36,04	9,86		
Avoiding Untrusted Sources	Employee	131	12,52	4,69	0,610	**0,609**
	Unemployed	58	12,86	4,71		
	Retired/Pensioner	39	12,21	4,37		
	Student	23	11,39	4,05		
Taking Preventive Measures	Employee	131	14,62	4,92	0,403	**0,751**
	Unemployed	58	14,47	5,26		
	Retired/Pensioner	39	14,62	5,72		
	Student	23	13,35	5,62		
Protecting Payment Information	Employee	131	7,34	2,67	6,423	**0,000***
	Unemployed	58	6,41	2,50		
	Retired/Pensioner	39	5,59	2,63		
	Student	23	5,65	2,62		
Managing Digital Footprint	Employee	131	12,42	3,74	2,271	**0,081**
	Unemployed	58	11,12	4,87		
	Retired/Pensioner	39	10,74	4,89		
	Student	23	12,09	4,01		
Ensuring Personal Cyber Security	Employee	131	84,15	14,86	2,525	**0,058**
	Unemployed	58	79,21	19,59		
	Retired/Pensioner	39	78,95	8,20		
	Student	23	78,52	7,87		

**p<0.05 significant difference, p>0.05 no significant difference; ANOVA test*

There is a statistically significant difference between those with different employment statuses in terms of the Protection of Payment Information score (p<0.05). Employees have a higher perception level of Protecting Payment Information (7.34). The difference is not significant in other scores (p>0.05).

Table 10: Comparison of Personal Cyber Security Scale Scores according to Place of Residence:

		n	**Centre.**	**ss**	**F**	**p**
Protecting Personal Privacy	Large urban	171	36,49	8,56	2,696	**0,069**
	District or town	64	36,77	7,56		
	Rural area	16	31,50	10,88		
Avoiding Untrusted Sources	Large urban	171	13,18	4,69	7,283	**0,001***
	District or town	64	10,94	3,65		
	Rural area	16	10,63	5,02		
Taking Preventive Measures	Large urban	171	15,50	5,48	15,437	**0,000***
	District or town	64	12,97	3,35		
	Rural area	16	9,38	3,18		
Protecting Payment Information	Large urban	171	7,25	2,55	11,811	**0,000***
	District or town	64	5,53	2,79		
	Rural area	16	5,56	2,16		
Managing Digital Footprint	Large urban	171	12,59	4,43	15,047	**0,000***
	District or town	64	10,95	3,13		
	Rural area	16	7,19	2,69		
Ensuring Personal Cyber Security	Large urban	171	85,01	13,45	20,782	**0,000***
	District or town	64	77,16	13,69		
	Rural area	16	64,25	19,23		

**p<0.05 significant difference, p>0.05 no significant difference; ANOVA test*

There is a statistically significant difference between those who live in different places in terms of Avoiding Untrusted Sources, Taking Precautions, Protecting Payment Information, Managing Digital Footprint, and Ensuring Personal Cyber Security scores (p<0.05). Those living in Large urban areas have higher perception levels of Avoiding Untrusted Sources (13.18), Taking Preventive Measures(15.50), Managing Digital Footprint (12.59), Protecting Payment Information (7.25), and Ensuring Personal Cyber Security (85.01). The difference is not significant for the Protecting Personal Privacy score (p>0.05).

Table 11: Comparison of Personal Cyber Security Scale Scores according to Time Spent on Social Media:

		n	**Centre.**	**ss**	**F**	**p**
Protecting Personal Privacy	Never	66	39,89	5,83	7,600	**0,000***
	Less than 1 hour	102	36,13	9,40		
	1-2 hours	60	33,77	6,59		
	3-4 hours	23	32,70	11,64		
Avoiding Untrusted Sources	Never	66	13,67	4,72	7,932	**0,000***
	Less than 1 hour	102	12,52	4,96		
	1-2 hours	60	12,50	3,27		
	3-4 hours	23	8,48	3,19		
Taking Preventive Measures	Never	66	14,91	3,99	7,403	**0,000***
	Less than 1 hour	102	14,37	5,81		
	1-2 hours	60	15,80	5,15		
	3-4 hours	23	10,13	2,55		
Protecting Payment Information	Never	66	6,23	2,52	7,158	**0,000***
	Less than 1 hour	102	7,37	2,32		
	1-2 hours	60	6,82	2,78		
	3-4 hours	23	4,78	3,49		
Managing Digital Footprint	Never	66	11,17	4,07	4,470	**0,004***
	Less than 1 hour	102	12,22	4,46		
	1-2 hours	60	12,82	3,92		
	3-4 hours	23	9,43	3,85		
Ensuring Personal Cyber Security	Never	66	85,86	14,87	12,199	**0,000***
	Less than 1 hour	102	82,61	13,49		
	1-2 hours	60	81,70	10,25		
	3-4 hours	23	65,52	21,26		

**p<0.05 significant difference, p>0.05 no significant difference; ANOVA test*

There is a statistically significant difference (p<0.05) in the scores for Protecting Personal Privacy, Avoiding Untrusted Sources, Taking Precautions, Protecting Payment Information, Managing Digital Footprint, and Ensuring Personal Cyber Security among those who have different duration of social media use. Those who never use social media have higher levels of Protecting Personal

Privacy (39.89), Avoiding Untrusted Sources (13.67), and Ensuring Personal Cyber Security (85.86), those who use social media for 1-2 hours have higher levels of Taking Preventive Measures (15.80), Managing Digital Footprint (12.82), and those who use social media for less than 1 hour have higher levels of Protecting Payment Information (7.37).

Table 12: Relationship between Cyber Security Awareness Effectiveness and Gender:

		Gender				X^2	p
		Male		Female			
		n	%	n	%		
Have you seen a public service announcement raising public awareness of cyber threats?	Yes	79	73,1	59	41,3	25,280	**0,000***
	No.	29	26,9	84	58,7		
Have you seen any posts on digital platforms informing the public about cyber threats?	Yes	83	76,9	68	47,6	22,038	**0,000***
	No.	25	23,1	75	52,4		
Have you ever attended any cyber-awareness training at school?	Yes	33	30,6	28	19,6	4,029	**0,045***
	No.	75	69,4	115	80,4		
Are you aware of the laws and rights of information security	Yes	47	43,5	40	28,0	6,567	**0,010***
	No.	61	56,5	103	72,0		
Do you have any information about the policies taken by the government to ensure cyber security nationally and internationally?	Yes	53	49,1	31	21,7	20,740	**0,000***
	No.	55	50,9	112	78,3		
Have you heard of the European Union Agency for Network and Information Security (ENISA)?	Yes	58	53,7	50	35,0	8,814	**0,003***
	No.	50	46,3	93	65,0		
Would you prefer a company that has experienced a cyber security crisis before?	Yes	51	47,2	23	16,1	28,696	**0,000***
	No.	57	52,8	120	83,9		
Do you search about cyber security on the internet?	Yes	40	37,0	49	34,3	0,206	**0,650**
	No.	68	63,0	94	65,7		
Have you received information or joined training on cyber security at work?	Yes	45	41,7	11	7,7	39,038	**0,000***
	No.	63	58,3	132	92,3		

**p<0.05 significant relationship, p>0.05 no significant relationship; Chi-square test*

There is a statistically significant relationship between gender and seeing a public service announcement, seeing informative posts on digital platforms, receiving cyber awareness training at school, having information about the laws imposed by the state, having information about the measures taken by the state, hearing about the ENISA organization, stating that they would prefer a company that has experienced a cyber security crisis before, conducting research on the subject, providing information and training on cyber security at work ($p<0.05$).

For men, seeing a public service announcement (73.1%), seeing informative posts on digital platforms (76.9%), receiving cyber awareness training at school (30.6%), having information about the laws set by the state (43.5%), having information about the measures taken by the state (49%), 1%), hearing about the ENISA organization (53.7%), stating that they would prefer a

company that has experienced a cyber security crisis before (47.2%), and receiving information and training about cyber security at the workplace (41.7%).

The relationship is not significant for conducting research on cyber-security (p>0.05).

Table 13: Relationship between Cyber Security Awareness Effectiveness and Age:

		Age										X^2	p
		20 and below		21-30		31-40		41-60		Over 60			
		n	%	n	%	n	%	n	%	n	%		
Have you seen a public service announcement raising public awareness of cyber threats?	Yes	9	42,9	50	50,0	24	47,1	37	66,1	18	78,3	11,802	**0,019***
	No.	12	57,1	50	50,0	27	52,9	19	33,9	5	21,7		
Have you seen any posts on digital platforms informing the public about cyber threats?	Yes	13	61,9	47	47,0	27	52,9	50	89,3	14	60,9	31,896	**0,000***
	No.	8	38,1	53	53,0	24	47,1	6	10,7	9	39,1		
Have you ever attended any cyber-awareness training at school?	Yes	7	33,3	22	22,0	7	13,7	15	26,8	10	43,5	8,894	**0,064**
	No.	14	66,7	78	78,0	44	86,3	41	73,2	13	56,5		
Are you aware of the laws and rights of information security	Yes	13	61,9	28	28,0	24	47,1	17	30,4	5	21,7	14,091	**0,007***
	No.	8	38,1	72	72,0	27	52,9	39	69,6	18	78,3		
Do you have any information about the policies taken by the government to ensure cyber security nationally and internationally?	Yes	2	9,5	34	34,0	12	23,5	28	50,0	8	34,8	15,571	**0,004***
	No.	19	90,5	66	66,0	39	76,5	28	50,0	15	65,2		
Have you heard of the European Union Agency for Network and Information Security (ENISA)?	Yes	13	61,9	33	33,0	19	37,3	30	53,6	13	56,5	12,128	**0,016***
	No.	8	38,1	67	67,0	32	62,7	26	46,4	10	43,5		
Would you prefer a company that has experienced a cyber security crisis before?	Yes	8	38,1	22	22,0	18	35,3	12	21,4	14	60,9	15,922	**0,003***
	No.	13	61,9	78	78,0	33	64,7	44	78,6	9	39,1		
Do you search about cyber security on the internet?	Yes	10	47,6	23	23,0	22	43,1	25	44,6	9	39,1	11,984	**0,017***
	No.	11	52,4	77	77,0	29	56,9	31	55,4	14	60,9		
Have you received information or joined training on cyber security at work?	Yes	4	19,0	24	24,0	13	25,5	11	19,6	4	17,4	1,026	**0,920**
	No.	17	81,0	76	76,0	38	74,5	45	80,4	19	82,6		

**p<0.05 significant relationship, p>0.05 no significant relationship; Chi-square test*

There is a statistically significant relationship between age and seeing a public service announcement on the subject, seeing informative posts on digital platforms, having information about the laws imposed by the state, having information about the measures taken by the state, hearing about the ENISA organization, and searching about cyber security (p<0.05). Those over 60 years of age have higher rates of seeing a public service announcement on the subject (78.3%), stating that they would prefer a company that has experienced a cyber security crisis before (60.9%), 41-60 years of age have higher rates of seeing informative posts on digital platforms

(89.3%), having information about the measures taken by the state (50.0%), 20 years of age and younger have higher rates of having information about the laws set by the state (61.9%), hearing about the ENISA organization (61.9%) and searching about cyber security(47.6%). The relationship is not significant for other awareness characteristics (p>0.05).

Table 14: Relationship between Cyber Security Awareness Effectiveness and Education Level:

		Education status						X^2	p
		High school and less		University		Master's and doctorate			
		n	%	n	%	n	%		
Have you seen a public service announcement raising public awareness of cyber threats?	Yes	31	44,9	90	57,7	17	65,4	4,426	**0,109**
	No.	38	55,1	66	42,3	9	34,6		
Have you seen any posts on digital platforms informing the public about cyber threats?	Yes	34	49,3	100	64,1	17	65,4	4,662	**0,097**
	No.	35	50,7	56	35,9	9	34,6		
Have you ever attended any cyber-awareness training at school?	Yes	18	26,1	30	19,2	13	50,0	10,391	**0,006***
	No.	51	73,9	126	80,8	13	50,0		
Are you aware of the laws and rights of information security	Yes	22	31,9	64	41,0	1	3,8	17,880	**0,000***
	No.	47	68,1	92	59,0	25	96,2		
Do you have any information about the policies taken by the government to ensure cyber security nationally and internationally?	Yes	17	24,6	52	33,3	15	57,7	8,924	**0,012***
	No.	52	75,4	104	66,7	11	42,3		
Have you heard of the European Union Agency for Network and Information Security (ENISA)?	Yes	30	43,5	66	42,3	12	46,2	0,142	**0,932**
	No.	39	56,5	90	57,7	14	53,8		
Would you prefer a company that has experienced a cyber security crisis before?	Yes	15	21,7	47	30,1	12	46,2	5,347	**0,069**
	No.	54	78,3	109	69,9	14	53,8		
Do you search about cyber security on the internet?	Yes	26	37,7	54	34,6	9	34,6	0,204	**0,903**
	No.	43	62,3	102	65,4	17	65,4		
Have you received information or joined training on cyber security at work?	Yes	13	18,8	43	27,6	0	0,0	15,987	**0,000***
	No.	56	81,2	113	72,4	26	100,0		

**p<0.05 significant relationship, p>0.05 no significant relationship; Chi-square test*

There is a statistically significant relationship between educational level and receiving cyber awareness training at school, having knowledge about the laws set by the state, having knowledge about the measures taken by the state, and being informed and trained about cyber security in the workplace (p<0.05). Master's and doctorate graduates have higher rates of receiving cyber awareness training at school (50.0%) and having information about the measures taken by the state (57.7%), while university graduates have higher rates of having information about the laws

imposed by the state (41.0%) and being informed and trained about cyber security at work (27.6%). The relationship is not significant in other awareness characteristics (p>0.05).

Table 15: Relationship between Cyber Security Awareness Effectiveness and Employment Status:

		Employment status								X^2	p
		Employee		Unemployed		Retired/Pensioner		Student			
		n	%	n	%	n	%	n	%		
Have you seen a public service announcement raising public awareness of cyber threats?	Yes	71	54,2	31	53,4	25	64,1	11	47,8	1,895	**0,594**
	No.	60	45,8	27	46,6	14	35,9	12	52,2		
Have you seen any posts on digital platforms informing the public about cyber threats?	Yes	91	69,5	23	39,7	31	79,5	6	26,1	32,424	**0,000***
	No.	40	30,5	35	60,3	8	20,5	17	73,9		
Have you ever attended any cyber-awareness training at school?	Yes	25	19,1	16	27,6	13	33,3	7	30,4	4,433	**0,218**
	No.	106	80,9	42	72,4	26	66,7	16	69,6		
Are you aware of the laws and rights of information security	Yes	57	43,5	3	5,2	16	41,0	11	47,8	36,304	**0,000***
	No.	74	56,5	55	94,8	23	59,0	12	52,2		
Do you have any information about the policies taken by the government to ensure cyber security nationally and internationally?	Yes	59	45,0	11	19,0	8	20,5	6	26,1	17,352	**0,001***
	No.	72	55,0	47	81,0	31	79,5	17	73,9		
Have you heard of the European Union Agency for Network and Information Security (ENISA)?	Yes	59	45,0	6	10,3	27	69,2	16	69,6	47,758	**0,000***
	No.	72	55,0	52	89,7	12	30,8	7	30,4		
Would you prefer a company that has experienced a cyber security crisis before?	Yes	34	26,0	16	27,6	15	38,5	9	39,1	3,320	**0,345**
	No.	97	74,0	42	72,4	24	61,5	14	60,9		
Do you search about cyber security on the internet?	Yes	45	34,4	13	22,4	22	56,4	9	39,1	11,930	**0,008***
	No.	86	65,6	45	77,6	17	43,6	14	60,9		
Have you received information or joined training on cyber security at work?	Yes	33	25,2	3	5,2	11	28,2	9	39,1	17,787	**0,000***
	No.	98	74,8	55	94,8	28	71,8	14	60,9		

**p<0.05 significant relationship, p>0.05 no significant relationship; Chi-square test*

There is a statistically significant relationship between employment status and seeing informative posts on digital platforms, having information about the laws set by the state, having information about the measures taken by the state, hearing about the ENISA organization, searching about cyber-security, providing information and training on cyber security in the workplace (p<0.05). The rates of seeing informative posts on digital platforms (79.5%) and searching about cyber security(56.4%) are the highest among retirees, the rates of having information about the measures

taken by the government (47.8%), hearing about the ENISA organization (69.6%), being informed and trained about cyber security at work (39.1%) are the highest among students, and the rates of having information about the measures taken by the government (45.0%) are the highest among employees. The relationship is not significant for other awareness characteristics (p>0.05).

Table 16: Relationship between Cyber Security Awareness Effectiveness and Place of Residence:

		Place of residence						X^2	p
		Large urban		District or town		Rural area			
		n	%	n	%	n	%		
Have you seen a public service announcement raising public awareness of cyber threats?	Yes	96	56,1	32	50,0	10	62,5	1,102	**0,576**
	No.	75	43,9	32	50,0	6	37,5		
Have you seen any posts on digital platforms informing the public about cyber threats?	Yes	108	63,2	39	60,9	4	25,0	8,821	**0,012***
	No.	63	36,8	25	39,1	12	75,0		
Have you ever attended any cyber-awareness training at school?	Yes	46	26,9	7	10,9	8	50,0	12,673	**0,001***
	No.	125	73,1	57	89,1	8	50,0		
Are you aware of the laws and rights of information security?	Yes	59	34,5	25	39,1	3	18,8	2,519	**0,284**
	No.	112	65,5	39	60,9	13	81,3		
Do you have any information about the policies taken by the government to ensure cyber security nationally and internationally?	Yes	70	40,9	9	14,1	5	31,3	16,730	**0,000***
	No.	101	59,1	55	85,9	11	68,8		
Have you heard of the European Union Agency for Network and Information Security (ENISA)?	Yes	72	42,1	35	54,7	1	6,3	14,647	**0,001***
	No.	99	57,9	29	45,3	15	93,8		
Would you prefer a company that has experienced a cyber security crisis before?	Yes	38	22,2	24	37,5	12	75,0	20,584	**0,000***
	No.	133	77,8	40	62,5	4	25,0		
Do you search about cyber security on the internet?	Yes	48	28,1	33	51,6	8	50,0	12,562	**0,002***
	No.	123	71,9	31	48,4	8	50,0		
Have you received information or joined training on cyber security at work?	Yes	38	22,2	15	23,4	3	18,8	0,169	**0,919**
	No.	133	77,8	49	76,6	13	81,3		

**p<0.05 significant relationship, p>0.05 no significant relationship; Chi-square test*

There is a statistically significant relationship between the place of residence and seeing informative posts on digital platforms, receiving cyber awareness training at school, having information about the measures taken by the government, hearing about the ENISA organization, stating that they would prefer a company that has experienced a cyber security crisis before, and searching about cyber security(p<0.05). Those living in Large urban areas have the highest rates of seeing informative posts on digital platforms (63.2%), and having information about the measures taken by the government (40.9%), those living in districts and towns have the highest rates of hearing about the ENISA organization (54.7%), searching about cyber security(51.6%),

those living in rural areas have the highest rates of receiving cyber awareness training at school (50.0%), stating that they would prefer a company that has experienced a cyber security crisis before (75.0%). The relationship is not significant for other awareness characteristics (p>0.05).

Table 17: Relationship between Cyber Security Awareness Effectiveness and Time Spent on Social Media:

		Time spent on social media per day								X^2	p
		Never		Less than 1 hour		1-2 hours		3-4 hours			
		n	%	n	%	n	%	n	%		
Have you seen a public service announcement raising public awareness of cyber threats?	Yes	43	65,2	55	53,9	30	50,0	10	43,5	4,683	**0,197**
	No.	23	34,8	47	46,1	30	50,0	13	56,5		
Have you seen any posts on digital platforms informing the public about cyber threats?	Yes	40	60,6	53	52,0	48	80,0	10	43,5	16,236	**0,001***
	No.	26	39,4	49	48,0	12	20,0	13	56,5		
Have you ever attended any cyber-awareness training at school?	Yes	23	34,8	18	17,6	20	33,3	0	0,0	21,598	**0,000***
	No.	43	65,2	84	82,4	40	66,7	23	100,0		
Are you aware of the laws and rights of information security	Yes	25	37,9	27	26,5	34	56,7	1	4,3	28,145	**0,000***
	No.	41	62,1	75	73,5	26	43,3	22	95,7		
Do you have any information about the policies taken by the government to ensure cyber security nationally and internationally?	Yes	22	33,3	42	41,2	20	33,3	0	0,0	21,380	**0,000***
	No.	44	66,7	60	58,8	40	66,7	23	100,0		
Have you heard of the European Union Agency for Network and Information Security (ENISA)?	Yes	28	42,4	40	39,2	39	65,0	1	4,3	30,549	**0,000***
	No.	38	57,6	62	60,8	21	35,0	22	95,7		
Would you prefer a company that has experienced a cyber security crisis before?	Yes	33	50,0	10	9,8	27	45,0	4	17,4	43,659	**0,000***
	No.	33	50,0	92	90,2	33	55,0	19	82,6		
Do you search about cyber security on the internet?	Yes	23	34,8	29	28,4	31	51,7	6	26,1	9,783	**0,021***
	No.	43	65,2	73	71,6	29	48,3	17	73,9		
Have you received information or joined training on cyber security at work?	Yes	15	22,7	15	14,7	26	43,3	0	0,0	28,429	**0,000***
	No.	51	77,3	87	85,3	34	56,7	23	100,0		

**p<0.05 significant relationship, p>0.05 no significant relationship; Chi-square test*

There is a statistically significant relationship between the time spent on social media per day and seeing informative posts on digital platforms, receiving cyber awareness training at school, having information about the laws imposed by the state, having information about the measures taken by the state, hearing about the ENISA organization, stating that they would prefer a company that has experienced a cyber security crisis before, searching about cyber-security, providing information and training on cyber security at work (p<0.05).

Among those who never use social media, the rate of receiving cyber awareness training at school (34.8%), stating that they would prefer a company that has experienced a cyber security crisis before (50.0%). And having information about the measures taken by the state (41.2%) among those who use social media for less than 1 hour.
Those who use 1-2 hours have the highest rates of seeing informative posts on digital platforms (80.0%), being informed about the laws set by the state (56.7%), hearing about the ENISA organization (65.0%), doing research on the subject (51.7%), and being informed and trained about cyber security at work (43.3%). The relationship is not significant for other awareness characteristics ($p>0.05$).

Summarizing the study results: Based on the survey results, the hypothesis presented below has been discussed:
H1. “The general public's awareness of cyber threats appears to be limited, and they may not proactively seek information on this subject.”

Based on the results of the question, "Do you search about cyber security on the internet?" only 35.5% of respondents indicated that they actively seek information about cyber security. This suggests that the general public has limited awareness of cyber threats and may not proactively educate themselves on the topic. Therefore, it highlights the importance of conducting cyber threat awareness campaigns to improve public knowledge and promote proactive measures against cyber-attacks.

H2. "Age and level of education are significant factors in determining the level of public awareness of cyber threats and protective measures."

Yes. As a result of a comparison of personal cyber security scale scores by age: Those aged 21-30 have a higher perception level of Avoiding Unreliability (13.87), Taking Preventive Measures (15.69), and Managing Digital Footprint (12.46), and those aged 31-40 have a higher perception level of Protecting Payment Information (8.16) and Ensuring Personal Cyber Security (87.04).

H3. “Public service announcements raising public awareness of cyber threats or posts on digital platforms informing the public about cyber threats effectively to reach target audiences.”

Yes, as a result of these questions: *"Have you seen a public service announcement raising public awareness of cyber threats? Have you seen any posts on digital platforms informing the public about cyber threats?"*

55.0% of the respondents have seen a public service announcement on the subject, and 60.2% have seen informative posts on digital platforms.

H4. "The training and events organized by public institutions and the private sector to raise awareness about cyber security are insufficient."

Regrettably, the responses to the questions "Have you ever attended any cyber-awareness training at school?" and "Have you received information or training on cyber security at work?" indicate that only 24.3% of respondents have received cyber-awareness training at school and 22.3% have received information and training on cyber security in the workplace. These results demonstrate that a very limited number of people have access to cyber security awareness training.

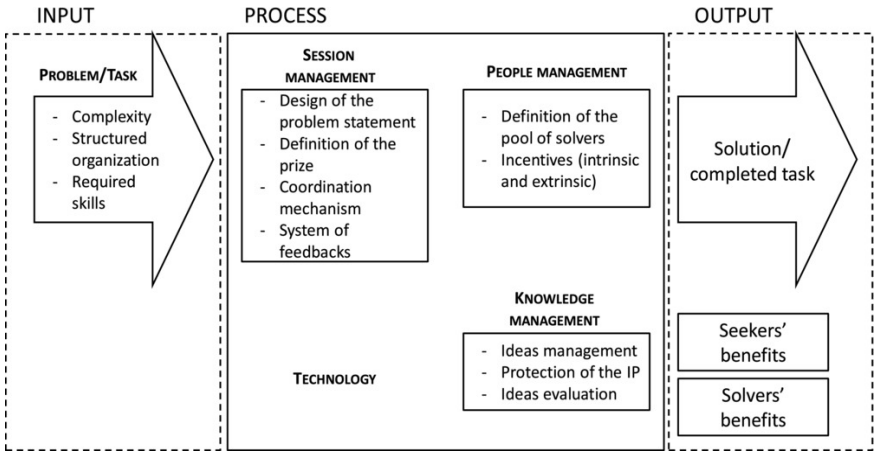
H5. "Cyber-attacks can damage a business's reputation and erode the trust its customers have in it."

Based on the survey question "*Would you prefer a company that has experienced a cyber security crisis before?*", 29.5% of respondents indicated a preference for such a company. This suggests that a significant majority, 70%, do not prefer a company that has experienced a cyber security crisis.

4. DESIGNING CONCEPTUAL MODEL OF PUBLIC RELATIONS STRATEGIES FOR CYBER THREAT AWARENESS-RAISING

4.1. Designing methodology

The study utilized the INPUT-PROCESS-OUTPUT (IPO) model, illustrated in Figure 11, as the conceptual framework for applying public relations strategies to raise awareness of cyber threats. The IPO model represents the input, process, and output involved in the application of these strategies. According to Armstrong (2001), input refers to what goes into the process, process refers to what causes the change, and output refers to what comes out of the process. The IPO model served as a general structure and guide for the study's direction.



source. Ghezzi et al. (2017).

Figure 11. The model structure

4.2. Model analysis

Public Relations strategies application for Cyber-threat awareness (see Figure 11) is developed on the basis of:

-Implementation of Strategic Plans in Public Relations Campaigns (see Section 1.3)

-Analysing Cyber Threat Awareness Activities (see Section 2.3)

-Identification of problems is based on the survey (See section 3)

The model of Public Relations strategies application for Cyber-threat awareness 3 parts: input process and output.

Input includes common Cyber-Threats, Problem analysis, and Identification, and Common Public Relations strategies.

Cyber Threats: Crytomining, data spill, denial of service, hacking, identity theft, malicious insiders, malware, phishing-scam emails.

Problem Analysis and Identification: Goals and objectives, target audiences, avaliable resouces, and budget, key messaging, and themes.

Public Relations Strategies on the Model:

Thought Leadership: Establishing a thought leadership position by sharing expert insights and commentary on cybersecurity issues. This can be done through blog posts, social media updates, and contributed articles to relevant publications. By positioning the organization as a trusted source of information on cyber security, it can build awareness and credibility.

Partnerships and Collaborations: Partnering with other organizations or experts in the field to promote cyber security awareness. This can include joint events, co-branded content, and shared resources. By leveraging the reach and influence of other organizations, the campaign can expand its impact and credibility.

Influencer Outreach: Reaching out to influencers and thought leaders in the industry to promote cyber security awareness. This can include working with bloggers, social media personalities, and other online influencers to create and share content. By leveraging the reach and influence of these individuals, the campaign can reach a broader audience and build credibility.

Social Media Campaigns: Creating social media campaigns that raise awareness about cyber security issues and promote best practices. This can include creating engaging social media content, using hashtags to drive engagement, and leveraging paid social media ads to reach a larger audience.

Events and Training: Hosting events and training sessions that educate people about cyber security best practices. This can include webinars, workshops, and other educational events. By providing hands-on training and education, the campaign can help people understand the importance of cyber security and how to protect themselves.

Crisis Communications: Developing a crisis communications plan that outlines how the organization will respond to cyber security incidents. This can include developing messaging, coordinating with internal and external stakeholders, and establishing a communication protocol. By being prepared for a cyber security incident, the organization can minimize the impact of an attack and maintain its credibility with stakeholders.

These are shown on the model as a few potential PR strategies. they can be used to promote cybersecurity awareness.

Process includes: Implementation, Problems and Solution

Output includes Evaluation, Continous monitoring, Outcomes

Outcomes can be described as a result of the PR strategies application for cyber-threat awareness. Expected results from the target audience:

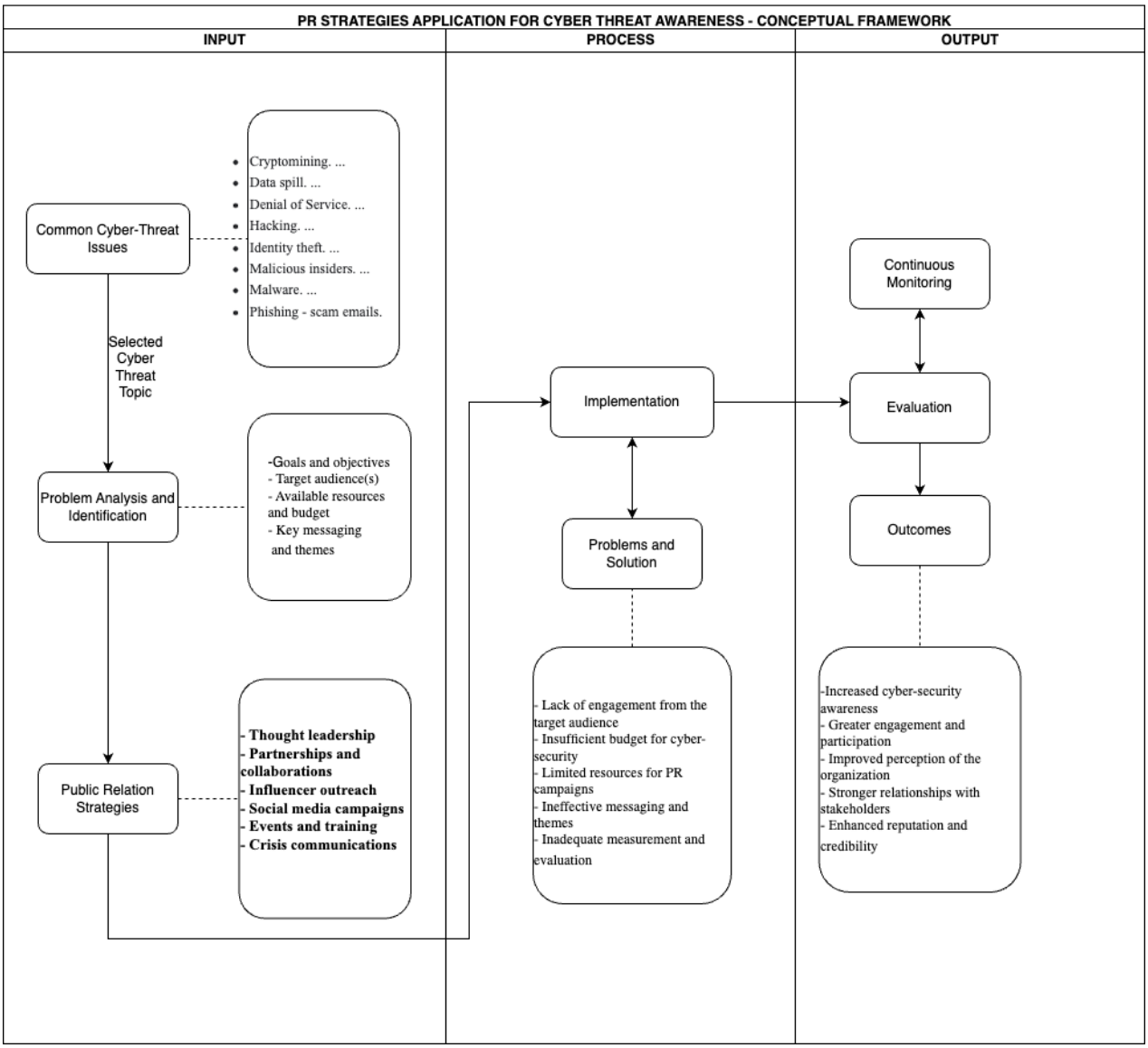
-Increased cyber-security awareness

-Greater engagement and participation

-Improved perception of the organization

-Stronger relationships with stakeholders

-Enhanced reputation and credibility



Source: developed by the author

Figure 12. Public Relations Strategies Application for Cyber-threat Awareness

CONCLUSIONS

Based on the research question and hypotheses, it is evident that the general public has limited awareness of the specific cyber threats they face and the measures that can be taken to protect against them. However, targeted public awareness campaigns utilizing social media and digital platforms can be more effective in increasing public knowledge and understanding of cyber threats than traditional forms of education. Age, level of education, and place of live are significant factors in determining the level of public awareness of cyber threats and protective measures. Additionally, Cyber-crisis can damage a business's reputation and erode the trust its customers have in it.

To address these issues, the Public Relations strategies application for the Cyber-threat awareness model can be implemented to promote cybersecurity awareness effectively. This model includes several strategies such as establishing a thought leadership position, partnering with other organizations or experts in the field, reaching out to influencers and thought leaders, creating engaging social media campaigns, hosting events and training sessions, and developing a crisis communications plan.

The implementation of these strategies is expected to result in increased cyber-security awareness, greater engagement and participation, improved perception of the organization, stronger relationships with stakeholders, and enhanced reputation and credibility. Continuous monitoring and evaluation of the outcomes are necessary to ensure the success of the campaign.

In conclusion, the Public Relations strategies application for the Cyber-threat awareness model provides a comprehensive approach to promoting cyber-security awareness. By implementing these strategies, organizations can increase public knowledge and understanding of cyber threats and protective measures, and create a safer online environment for everyone.

LIST OF REFERENCES

Agee, D. L. (1998). Public Relations: Strategies and Tactics (Vol. 5). New York : Longman: Addison-Wesley Educational Publisher Inc. p.6

Armstrong, M. (2001). A handbook of MANAGEMENT techniques: the best-selling guide to modern management methods. Kogan Page Publishers.

Babbie, E. (2007). The practice of social research. 11th. *Belmont, CA: Thomson Wadsworth*, *24*(511), 66.

Başok, N., & Coşkun, G. (2012). Teoriden Pratiğe Halkla İlişkiler Projeleri: Ödüllü Örnek Uygulamalar (*Public Relations Projects from Theory to Practice*). *İstanbul: Nobel Yayıncılık*. p.75,129

Bhardwaj, A. and Goundar, S. (2019). A framework to define the relationship between cyber

Bicakci, I. (1999). *İletişim ve halkla ilişkiler:" eleştirel bir yaklaşım*" (*Communication and public relations: a "critical approach*"). MediaCat Kitapları.

Biga, N. E. N. A. D., Jovanovic, M., Perkovic, M., & Mitic, D. (2016). Modern business environment: information technology as a shield against cyber security threats. In *Proceedings of the 8th International Conference on Business Information Security, BISEC*.

Canoz, K. (2008). Kamuda halkla iliskilerin yeni yuzu: Bilgi edinme yasasi (*The New Face of Public Relations in The State Administration: The Law of Freedom of Information*). *Selcuk İletisim*, *5*(3), 141-152.

Chatchalermpun, S., Wuttidittachotti, P., & Daengsi, T. (2020, April). Cybersecurity Drill Test Using Phishing Attack: A Pilot Study of a Large Financial Services Firm in Thailand. In *2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*. p. 283-286

Clarke, R. A., & Knake, R. K. Cyber War: The Next Threat to National Security and What to Do about It (New York: Ecco, 2010); Joel Brenner. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, p.74-85

Daud, M., Rasiah, R., George, M., Asirvatham, D. and Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations? International Journal of Business and Society, 19(1), p.161-180.

Ettredge, M., Guo, F. and Li, Y. (2018). Trade secrets and cyber security breaches. Journal of Accounting and Public Policy, 37(6), p.564-585.

Fischer, R., Halibozek, E., Halibozek, E. P., & Walters, D. (2012). *Introduction to security*. Butterworth-Heinemann.

Furnell, S. (2002). Cybercrime: Vandalizing the information society London: Addison-Wesley

Gordon, J. C. (1997). Interpreting definitions of public relations: Self-assessment and a symbolic interactionism-based alternative. *Public Relations Review*, *23*(1), p.57-66.

GÜNDÜZALP, C. (2021). Üniversite çalışanlarının dijital veri ve kişisel siber güvenlik farkındalıkları (bilgi işlem daire başkanlıkları örneği). *Journal of Computer and Education Research*, *9*(18), 598-625.

Harlow, R. F. (1976). Building Public Relations Definitions. Public Relations Review, 36.

Harris, T. L. (1997). Interpreting Definitions of Public Relations: Self Assessment and a Symobolic Interactionisim-Based Alternatives. Public Relations Review, 57

Hovav, A., & Gnizy, I. (2017). Knowledge Sharing or Knowledge Protection? The Effects of Cyber Regulations and Security Policies on Firms' Market Orientation and Performance. *KM2017*.

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, p.15-25

Jain, A. (2005). Cyber Crime: Issues Threats and Management. Delhi: ISHA Books

Jeong, C.Y., Lee, S.Y.T. and Lim, J.H. (2019). Information security breaches and IT security investments: Impacts on competitors. Information & Management, 56(5), p.681- 695.

Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting & Information Management*.

Karadeniz, Mustafa (2010). Halkla İlişkiler Faaliyetlerinin Rolü ve Önemi (*The Role and Importance of Public Relations Activities*). Beta Yayım Dağıtım, Istanbul p.112,113

Korpela, K. (2015). Improving cyber security awareness and training programs with data analytics. *Information Security Journal: A Global Perspective*, *24*(1-3), p.72-77.

KORUCU, O. (2021). Yeni normal dünya düzeninin siber güvenlik ve bilgi güvenliğine etkileri (The effects of the new normal world order on cyber security and information security). *Yönetim Bilişim Sistemleri Dergisi*, *7*(1), 44-60.

Koziarski, J., & Lee, J. R. (2020). Connecting evidence-based policing and cybercrime. Policing: An International Journal. p.199

Kritzinger, E. & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840-847.

L'Etang, J. (2008). Public Relations Concepts, Practice And Critique. Los Angeles: London: SAGE. p.110

LeClair, J., & Keeley, G. (2015). *Cybersecurity in our digital lives*. Hudson Whitman/Excelsior College Press.

Li, J. X. (2017). Cyber Crime and Legal Countermeasures: A Historical Analysis. *International Journal of Criminal Justice Sciences*, *12*(2). p.196-207

Lopez, J., Setola, R., & Wolthusen, S. (Eds.). (2012). *Critical Infrastructure Protection: Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense* (Vol. 7130). Springer.

Okay, Ayla ve Okay, Aydemir (2014). Halkla İlişkiler Kavram Strateji ve Uygulamaları (*Public Relations Concept Strategy and Practices*). Der Yayınları, Istanbul p.248,265

OZDEMİR, A., & ULUYOL, C. (2019), KAMU KURUM VE KURULUŞLARINDA BİLGİ GÜVENLİĞİ FARKINDALIĞI (*Turkish Journal of Social Research), Türkiye Sosyal Araştırmalar Dergisi*, *25*(3), p.649-666.

Özer, M. A. (2012). *Halkla ilişkiler dersleri* (*Public Relations Lessons*). Adalet Yayınevi. p.74,79

Parker, D. B. (1989). Computer Crime: Criminal Justice Resource Manual. p.2

Pogrebna, G., & Skilton, M. (2019). *Navigating new cyber risks: How businesses can plan, build and manage safe spaces in the digital age*. Springer.

Quinn Kiser, (2020) Cybersecurity A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering. New York.

Reber, D. L. (2015). Public Relations Strategies and Tactics (Vol. Eleventh Edition). Harlow, England: Pearson Education p.1

Ryder, R. D., & Madhavan, A. (2019). *Cyber crisis management: overcoming the challenges in cyberspace*. Bloomsbury Publishing. p.2

security and cloud performance. Computer Fraud & Security, 2019(2), p.12-19.

Sen, F. (2012). Kamu Yonetiminde Halkla İliskileri Yeniden Dusunmek (*Rethinking Public Relations in Public Sector*). Akdeniz Universitesi İletisim Fakultesi Dergisi, (16), 63-79. Retrieved from https://dergipark.org.tr/tr/pub/akil/issue/48079/607890

Sezgin, Murat (2007). Halkla İliskiler (*Public Relations),* Yuce Medya Basım Yayım Dağıtım, Konya.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, p.989-1015.

Smith, P. R., Zook, Z. (2011) Marketing Communications Integrating Offline and Online with Social Media. London: Kogan Page Limited

Tari Schreider, S. S. C. P., CISM, C., & CISO, I. (2017). *Building Effective Cybersecurity Programs: A Security Manager's Handbook*. Rothstein Publishing.

Treaty, L. (2009). Treaty on the Functioning of the European Union.

Trim, P., & Yang-Im, L. (2014). Cyber Security Management: A Governance, Risk and Compliance Framework. New York: Gower Publishing. p.141

Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, *5*(6), e02010.

Unal, A. N., & Ergen, A. (2018). SİBER UZAYDA YETERİNCE GÜVENLİ DAVRANIYOR MUYUZ? İSTANBUL İLİNDE YÜRÜTÜLEN NİCEL BİR ARAŞTIRMA *(Are We Safe in Cyberspace?). Manisa Celal Bayar Üniversitesi Sosyal Bilimler Dergisi*, *16*(2), p.191-216.

Westby, J. R. (2004). International guide to cyber security. American Bar Association. p.2,3

Whitler, K.A. and Farris, P.W. (2017). The impact of cyber attacks on brand image: Why proactive marketing expertise is needed for managing data breaches. Journal of Advertising Research, 57(1),p.3-9.

Wilcox, D. A. (1992). Public Relations: Strategies and Tactics. HarperCollins. Retrieved December 12, 2019, from https://books.google.com.tr/books?id=K4SSQgAACAAJ p.27

Yeboah-Boateng, E. O. (2018). Cyber-security concerns with cloud computing: Business value creation and performance perspectives. In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications* p. 995-1026

Yu, W., Xu, G., Chen, Z., & Moulema, P. (2013, October). A cloud computing-based architecture for cyber security situation awareness. In *2013 iEEE conference on communications and network security (cNS)* (pp. 488-492). IEEE.

Legal acts:

ENISA-Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 p.16

EU Commission, 2001/279, "Proposal for a Council Decision adopting a specific program 2002-2006 for research, technological development and demonstration to be carried out by means of direct actions by the Joint Research Centre", 2001.

Plan, A. (2000). eEurope 2002, an information society for all, action plan.

Online sources:

Awareness (2023 02 January), https://www.merriamwebster.com/dictionary/awareness

Ankara Üniversitesi Bilgi İşlem Daire Başkanlığı, "Cyber-Security Awareness" 2018, Retrieved from http://bid.ankara.edu.tr/2018/10/02/siber-guvenlik-farkindaligi

Cyber-edge 2020 Retrieved from https://cyber-edge.com/wp-content/uploads/2021/04/CyberEdge-2021-CDR-Report-v1.1-1.pdf

ENISA Overview of Cybersecurity and Related Terminology 2017, p.6. Retrieved from https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

ENISA, "Cyber Awareness Material https://www.enisa.europa.eu/media/multimedia/posters/enisa-cyber-poster

ENISA, "Overview of Cybersecurity and Related Terminology" 2023

ENISA, "Review of Cyber Hygiene Practices", 2016, p.6. Retrieved from https://www.enisa.europa.eu/publications/cyber-hygiene/@@download/fullReport

European Cyber Security Month, Retrieved from https://cybersecuritymonth.eu/

European Union Agency for "Cybersecurity, Review of Cyber Hygiene Practices", European Network, and Information Security Agency, 2017, p.15 Retrieved from https://data.europa.eu/doi/10.2824/352617

Mjdsystems 2020 Retrieved from https://www.mjdsystems.co.uk/what-is-the-human-os-and-why-is-it-important/

Seyma Topaloglu. Designing a conceptual model of public relations strategies for cyber threat awareness raising / Master's Work in Cyber-Security Management. Supervisor assoc. prof. dr. T. Limba. – Vilnius: Mykolas Romeris University, Faculty of Public Governance and Business, 2023. – 64 p.

ANNOTATION

This thesis examines public relations strategies for raising cyber threat awareness and presents a conceptual framework for addressing the issue. The research is divided into four main sections that explore the definition and practice of public relations, the concepts of cyber security and cyber threats, the analysis of the results of the Cyber Security Awareness Survey, and the presentation of a model designed to implement public relations strategies aimed at raising awareness of cyber threats. The study highlights the significant consequences of cyber threats for organizations and emphasizes the importance of increasing awareness to protect against such threats. The research question and hypotheses focus on the extent of public awareness of cyber threats and propose solutions for increasing awareness and education. The thesis concludes with recommendations for improving the implementation of public relations strategies to effectively raise awareness of cyber threats.

Key words: Cyber-Security, cyber threat, cyber threat awareness, public relations strategy of cyber threat awareness

SUMMARY

This thesis aims to explore public relations strategies for cyber threat awareness and develop a conceptual framework for raising cyber threat awareness. The study explains that cyber threats can have significant consequences for organizations and one of the ways to protect against cyber threats is to increase awareness. The research design is divided into four main sections covering the definition and practice of public relations, the concepts of cyber security and cyber threats, the analysis of the results of the Cyber Security Awareness Survey, and the presentation of a model designed to implement public relations strategies aimed at raising awareness of cyber threats. The research question and hypotheses explore the extent of public awareness of cyber threats and what can be done to increase public awareness and education. The thesis concludes with recommendations for improving the implementation of public relations strategies to effectively raise awareness of cyber threats.

LIST OF ANNEXES

Annex 1. The questionnaire of the survey

A. Personal Information

1. Gender?	☐ Male ☐ Female ☐ Other
2. Age?	.....
3. What is the highest level of education that you have completed?	☐ Primary school ☐ Middle school ☐ High school ☐ University ☐ master's and doctorate
4. What is your employment status?	☐ Employed ☐ Unemployed ☐ Retired ☐ Student
5. What type of community do you live in?	☐ Large City ☐ Small City or Town ☐ Rural Area

B. Social Media Usage and Cyber Security Information

1. Time spent on social media per day	☐ Never ☐ Less than 1 hour ☐ 1-2 hours ☐ 3-4 hours ☐ More than 4 hours
2. Social Media Networks that you use (you can select more than one)	☐ I don't use ☐ Facebook ☐ Instagram ☐ Twitter ☐ Youtube ☐ TikTok ☐ WhatsApp ☐ Other…….(please specify)
3. Being victim of cybercrime on the internet, social media	☐ Yes ☐ No
4. What are some cyber scams you have experienced? (you can select more than one)	☐ I didn't experience it. ☐Identity theft on social media ☐Identity theft in a bank account

	☐ Scam in sms or e-mail ☐ Frauds in online shopping ☐ Other……..(please specify)
5. Do you use mobile banking applications?	☐ Yes ☐ No
6. Do you use e-government services?	☐ Yes ☐ No

C. Cyber Security and Awareness

Please answer all the question below		**YES**	**NO**
1	Have you seen a public service announcement raising public awareness of cyber threats?		
2	Have you seen any posts on digital platforms informing the public about cyber threats?		
3	Have you ever attended any cyber-awareness training at school?		
4	Are you aware of the laws and rights of information security?		
5	Do you have any information about the policies taken by the government to ensure cyber security nationally and internationally?		
6	Have you heard of the European Union Agency for Network and Information Security (ENISA)?		
7	Would you be a customer of a company that has experienced a cyber security crisis before?		
8	Do you search about cyber security on the internet?		
9	Have you received information or joined training on cyber security at work?		

D. Personal Cyber Security Provision Scale

1: Strongly disagree, 2: Disagree, 3: Undecided, 4: Agree, 5: Strongly disagree

Please indicate your level of agreement/disagreement to the following statements.		**1**	**2**	**3**	**4**	**5**
1	I purchase products on social media ads					
2	I open e-mail attachments from people I do not know					
3	I respond to emails from banks and online shopping website					
4	I share my personal information on the internet when necessary (ID No, date of birth, etc.)					
5	I share my personal information on social media					
6	I make video or voice calls with people I don't know					
7	I create passwords easy to remember ("123", birthday, etc...)					
8	I often share my location on the internet					
9	I reply to authentication messages received by e-mail					
10	I use same password for all my internet accounts					

11	I don’t sign up for websites that I don’t trust.					
12	I don’t accept unusual payment requests					
13	I don’t accept friend requests that I don't know on social media					
14	I download files from insecure websites					
15	I update the software I use					
16	I have antivirus software on my computers					
17	I check an SSL certificate on any website					
18	I avoid using simple strings when setting my passwords					
19	I change the security settings of my web browser					
20	I do online shopping from my personal device					
21	I do internet banking transactions from my personal device					
22	I change the passwords regularly (email, social networks etc..)					
23	I clear my browsing data					
24	I log out of my internet accounts					
25	I make sure no personal data is left on other devices					