Ardahan Üniversitesi
İktisadi ve İdari Bilimler Fakültesi Dergisi
https://dergipark.org.tr/tr/pub/aruiibfdergisi

Determination of cyber security awareness of the public personnel*

Kamu personelinin siber güvenlik farkındalığının tespiti

*Barış Daşdemir[a**], Salih Serkan Kaleli[b]*

[a] *Yüksek Lisans Öğrencisi, Ardahan İl Emniyet Personeli, Ardahan, bdasdemir91@gmail.com, ORCID: 0009-0009-0080-4395*

[b] *Dr. Öğretim Üyesi, Ardahan Üniversitesi, Sosyal Bilimler Meslek Yüksekokulu,Ardahan, salihserkankaleli@gmail.com, ORCID: 0000-0003-2196-6050*

ARTICLE INFO

Article history:
Received: 20 September 2024
Accepted: 9 October 2024

Keywords:
Information and Communication Technologies,
Information,
Information Security,
Cyber Security,
Cyber Security Awareness

Article type:
Research article

ABSTRACT

Today, information and communication technologies play an indispensable role in almost every aspect of our lives and this situation transforms cyber security from an individual or institutional issue into a national security problem. The main purpose of this study is to determine the cyber security awareness levels of public personnel working in Ardahan Provincial Police Directorate and to evaluate their practical applications in this field. The research was conducted with a total of 302 public personnel participants and an analysis was carried out on six different dimensions (confidentiality, control /possession, integrity, authenticity, availability and utility) using the Cyber Security Scale (CSS). IBM SPSS 28 and AMOS 24 statistical package programs were used to analyze the data obtained in the study and various statistical tests were applied on the data set. The findings of the research show that the cyber security awareness levels of public personnel are generally sufficient, but more awareness raising activities are needed in the benefit dimension. As a result of the research, it is evaluated that contributing to the development of cyber security training programs and policies will help to create strategies to increase the cyber security awareness of public personnel.

MAKALE BİLGİSİ

Makale geçmişi:
Başvuru: 20 Eylül 2024
Kabul: 9 Ekim 2024

Anahtar kelimeler:
Bilgi ve İletişim Teknolojileri,
Bilgi,
Bilgi Güvenliği,
Siber Güvenlik,
Siber Güvenlik Farkındalığı

Makale türü:
Araştırma makalesi

ÖZET

Günümüzde bilgi ve iletişim teknolojileri, yaşamımızın neredeyse her alanında vazgeçilmez bir rol oynamakta ve bu durum, siber güvenliği sadece bireysel ya da kurumsal bir mesele olmaktan çıkararak, ulusal bir güvenlik sorununa dönüştürmektedir. Bu çalışmadaki temel amaç, Ardahan İl Emniyet Müdürlüğü'nde görev yapan kamu personelinin siber güvenlik farkındalık düzeylerinin belirlenmesi ve bu alandaki pratik uygulamalarının değerlendirilmesidir. Araştırma, toplam 302 kamu personeli katılımcı ile yürütülmüş olup, Siber Güvenlik Ölçeği (SGÖ) kullanılarak altı farklı boyut (gizlilik, kontrol/sahiplik, bütünlük, gerçeklik, erişilebilirlik ve fayda) üzerinden bir analiz gerçekleştirilmiştir. Çalışmada elde edilen verilerin analizi için IBM SPSS 28 ve AMOS 24 istatistik paket programından faydalanılmış ve veri seti üzerinde çeşitli istatistiksel testler uygulanmıştır. Araştırma bulguları, kamu personelinin genel olarak siber güvenlik farkındalık düzeylerinin yeterli olduğunu, ancak fayda boyutunda daha fazla bilinçlendirme çalışmasına ihtiyaç duyulduğunu göstermektedir. Araştırma sonucunda, siber güvenlik eğitim programlarının ve politikalarının geliştirilmesine katkı sağlamanın, kamu personelinin siber güvenlik farkındalığını artırmaya yönelik stratejilerin oluşturulmasına yardımcı olacağı değerlendirilmektedir.

* *Çalışma, Barış Daşdemir'in 2024 yılındaki yüksek lisans tezinden türetilmiştir.*

** *Sorumlu yazar / Corresponding author*

E-posta / E-mail: bdasdemir91@gmail.com

Atıf / Citation: Daşdemir, B. and Kaleli, S. S. (2024). Determination of cyber security awareness of public personnel. *Ardahan Üniversitesi İİBF Dergisi*, *6*(2), 120-133. http://doi.org/10.58588/aru-jfeas.1540483

1. Introduction

In human history, there has been a three-stage transition from an agricultural society to an industrial society and finally to an information society. The Industrial Revolution completed this process and marked the beginning of a new era by creating its own culture in terms of modes of production and socio-economic structuring (Özdemirci & Torunlar, 2018). The remarkable developments in information and communication technologies worldwide since the 1970s have led to this new era being called the "Information Age" (Aldemir & Merve, 2020). This period is also defined by various terms such as "post-capitalist society", "information society", "knowledge economy". Among these definitions, the most widely accepted and unified expression in all societies is the term "information age" and its synonym "information society" (Bekar & Sağlam, 2023). The information age has brought with it the concept of "information society", which defines the direction and character of a new process of change (Ögün et al. 2020). Defining the 21st century as an age in which knowledge is at the center is a widely accepted approach in the scientific world and the general society (Aldemir & Merve, 2020). Since the second half of the 20th century, rapid progress in information and communication technologies has accelerated the transition from the industrial age to the information age. In this new era, the increasing value of information and technology has led to the popularization of concepts such as "information age" and "information society" (Aldemir & Merve, 2020). The current period is defined as a period characterized by the replacement of mechanical technologies in production by programmable digital technologies and the rapid development of information communication technologies in the world. This process is also referred to as the "informatic era" (Yıldırım, 2020). Today's technological developments are triggering a new industrial revolution called Industry 4.0. This revolution focuses on production processes based on cyber-physical systems and provides a competitive advantage to those using innovative information communication technologies that increase productivity, such as cloud computing (Bai et al., 2020). The replacement of manpower by machines in some production systems as machines become "smart" is an important factor in the emergence of the Industry 4.0 concept. For Industry 4.0 to achieve its goals, tools such as the Internet of Things and cyber-physical systems are needed. In this new configuration, cyber-physical systems and the Internet of Things play a critical role (You & Feng, 2020).

As the public sector is becoming increasingly digitalized under the influence of these technologies, it is of great importance that public personnel have sufficient knowledge about cyber security and reach an effective awareness in this field. Cyber security is an important discipline that aims to protect digital data, especially computers, networks, software applications and critical systems. Determining the cyber security awareness of public personnel and increasing their level of knowledge in this field is a critical step to ensure both the protection of personal data and the uninterrupted execution of public services. Protecting sensitive data from unauthorized access and preventing interruptions in business operations due to unwanted network activity requires the effective use of cyber security measures and tools. In addition, factors such as cyber-attacks, natural disasters or terrorist incidents that may occur in the digital environment can damage the information systems of countries, which directly affects national security.

This research aims to reveal the extent to which cyber security culture is adopted among public employees and how prepared they are against cyber threats. The main objective of the research is to determine the level of cyber security awareness of public employees and to make recommendations for increasing the necessary training and measures in this field. The study aims to provide a comprehensive perspective on how information security policies and practices can be improved by examining in depth the cyber security awareness and training needs of the personnel working in public institutions in Turkey. The development of cybersecurity training and awareness programs will play an important role in mitigating these threats and ensuring a more secure computing environment in the public sector.

2. Conceptual Framework

Today, knowledge plays a key role not only in understanding the present and shaping the future, but also in understanding the past. The value of knowledge has been understood from the earliest ages of human history in various fields from education to health, from art to life, and has been passed on to future generations in different ways. In early times, knowledge was passed from generation to generation through tales, stories and epics, and in later periods it was spread through madrasas, churches, universities and written sources. However, recently, with the development of technology, communication between people has accelerated and cooperation has increased (Ecek & Çakmak, 2022). This marked the beginning of a new era called the "information age". Today, information not only directs people's daily lives, but is also a fundamental element that determines the direction of human life in the future (Korucu, 2021). The concept of information security includes elements such as the development of data protection concepts, encryption methods and the implementation of security policies, covering various dimensions and ways of thinking (Wylde et al. 2022). Information security, which also includes sub-fields such as cryptography, intrusion detection and information flow security, has been shaped to meet the requirements of modern information security policies (Nair and Tyagi, 2021).

2.1. Cyber Security

The increasing number of internet users worldwide has increased the importance of the concept of cyber security. According to the International Telecommunication Union (ITU) 2021 data, by the end of 2021, approximately 4.9 billion people (63%) worldwide were internet users, an increase of 17% compared to 2019 (International Telecommunication Union, 2022). With increasing internet usage, the number of users exposed to cyber threats and attacks is also increasing, and cybercrimes are diversifying and increasing with technological developments (Salem, Moreb, & Rabayah, 2021). With the rapid development of information technologies, cyber attack methods are also renewed, which keeps the issue of cyber security on the agenda (Tanrıverdi, 2020).

Cybersecurity is of vital importance in today's digital age. This concept is defined by Schatz, Behrend, and Meyer (2017) as the process of protecting computer networks, devices, and valuable data from unauthorized access and ensuring the confidentiality, integrity, and availability of information. The fact that the majority of people spend their time in digital environments leads to an increase in threats arising from the digital world, which further increases the importance of the concept of cyber security. The increasing frequency of cyber-attacks reveals that security software alone is not enough and that internet users need to be equipped with cyber security knowledge (Aksogan, Akçayol, & Akgül, 2018).

The term cyber security was introduced by computer scientists in the early 1990s to describe the security problems of networked computers. Although the terms cybersecurity and information security are often used interchangeably, there are important differences between these two concepts. While information security focuses on ensuring the confidentiality, integrity and availability of information, cybersecurity encompasses these elements as well as the security of all assets and individuals accessible through cyberspace (Solms & Niekerk, 2013). Cybersecurity also includes additional security elements such as non-repudiation and authentication.

Today, cyber-attacks cause significant problems at personal, corporate and state levels (Gönç, 2022). Attackers use various cyber threat methods to infiltrate information systems and carry out their attacks. Cyber threats include not only new types of crimes that have emerged through the misuse of information and communication technologies, but also cyber-enabled versions of traditional crimes (Gönç, 2022). Cyber threats include various forms such as bulk e-mail, loggers, social engineering attacks, viruses, worms, Trojan horses, ransomware, spyware and adware. The definitions and characteristics of these threats increase the cybersecurity knowledge of users and enable them to protect themselves against these threats more consciously and effectively (Sagiroglu,

2018). Users' lack of cybersecurity knowledge and their lack of safe behavior cause them to feel insecure in the cyber environment. Therefore, it is necessary to raise awareness and educate people about security in order to reduce or prevent security problems (Kovačević, Putnik, & Tošković, 2020).

2.2. Cyber Security in Turkey

Turkey is a global actor in the field of cyber security, both as a source and target of attacks. The fact that it ranks high in the world rankings especially in DDoS attacks shows its effectiveness in this field. This situation shows that the effective utilization of information and communication technologies depends on the continuity and effectiveness of national cyber security efforts. Ensuring cybersecurity is critical for Turkey's economic growth at individual, institutional and national levels. The COVID-19 pandemic accelerated technological transformation and further increased cyber security needs (infrastructure, new technologies, human resources, awareness) (Çakır & Uzun, 2021). Since cyber security products and solutions purchased from foreign countries themselves pose cyber security risks and threats (backdoors, etc. vulnerabilities), Turkey attaches great importance to the development and use of domestic and national products and solutions (Aydemir, 2022).

Cyber-attacks go beyond the personal and institutional level and threaten national security, going beyond cyber espionage and reaching the dimensions of cyber warfare. In this context, the field of cybersecurity is of critical importance worldwide and creates a great need for human resources not only in Turkey but also worldwide. As of 2019, it is estimated that 1.5 million workforce is needed worldwide in the field of cybersecurity, while Turkey needs approximately 15-20,000 cybersecurity experts (Altıner, 2021). In Turkey, cybersecurity was initially dealt with in the field of public order and law, but over time it has become an issue that has reached the dimension of national security. In this process, cyberspace, which armies see as a fifth battlefield, has caused states to focus on legal regulations. In Turkey, the first legal regulation within the scope of combating cybercrimes was made on June 6, 1991 with the Turkish Penal Code No. 3756. This regulation defined various criminal elements under the title of "Crimes in the Field of Informatics" (Kiziltan, 2007). With the Turkish Criminal Code No. 5237, adopted on September 26, 2004, more comprehensive regulations were made in this area, and Articles 243, 244, 245 were elaborated (Kiziltan, 2007). On July 18, 2006, with the amendments made to the Anti-Terrorism Law No. 3713, some IT crimes were included in the scope of terrorism crimes (Öcal, 2021). Law No. 5651, which entered into force on 23 May 2007, includes regulations on broadcasts on the internet and crimes committed through these broadcasts. Another important step in Turkey's fight against cybercrime was its accession to the European Convention on Cybercrime. This convention is important as the first international agreement that emphasizes international cooperation in the fight against cybercrime and entered into force on July 1, 2004 (Ozbek, 2015).

In recent years, cybersecurity efforts in Turkey have gained significant momentum, and various policies and strategies have been determined with the Electronic Communications Law No. 5809, and cybersecurity procedures and standards have been established. Within the scope of these duties and responsibilities assigned to the Ministry of Transport and Infrastructure, training and awareness activities are also of great importance (National Cyber Security Strategy and Action Plan, 2020). Established on July 10, 2018, the Digital Transformation Office undertook the task of developing projects on cybersecurity and Information and Communication Security Measures were determined with the Presidential Circular No. 2019/12. In addition, the Information and Communication Technologies Authority (ICTA) was authorized to prevent cyber-attacks and impose sanctions (Altıner, 2021).

3. Literature Review

Cybersecurity is a critical aspect of modern technological systems and gathering intelligence against cyber threats is vital to ensure the protection of systems, networks and data in cyberspace (Humayun et al., 2020). The

use of social media platforms such as Twitter has been studied as a tool for gathering cyber threat intelligence, and research has been conducted on the use of techniques such as deep neural networks in cyber threat detection (Dionísio et al., 2019). Furthermore, the integration of artificial intelligence (AI) has been highlighted as an important advancement in defending against potential cyber threats and attacks (Srivastava, 2019). There are many studies in the literature on cyber security and the measures to be taken against cyber attacks. In one of these studies, Kott and Linkov (2021) stated that measuring the level of cyber resilience of cyber systems is a challenge and that strict and quantitative measurement of cyber security should be developed. Kumar et al. (2023) emphasized the importance of transparency and interpretability in AI-based cyber security systems, drawing attention to the necessity of explainable artificial intelligence when designing security mechanisms for cyber threat hunting. Ünver et al., (2009) research focuses on information security vulnerabilities and examines how identification numbers used in online transactions pose a danger in accessing personal information.

In a study conducted by Vroom and von Solms (2004), it was stated that in addition to information security policies and corporate information activities, corporate culture and personal characteristics are also effective in the formation of information security awareness. Tekerek and Tekerek (2013) determined the level of awareness of these students on ethical and technical issues in information security with a unique scale applied to primary and secondary school students in Kahramanmaraş province. As a result of the research, it was determined that students had sufficient awareness of ethical issues but showed deficiencies in technical issues. Inadequate information and computer security training and activities were shown as the reason for this situation and suggestions were made to increase the training in this field. In another study, Eminagaoglu and Goksen (2009) emphasized that the key to success in information security is conscious and informed users. They stated that data losses and damage can be prevented significantly if advanced hardware and software are used by users who are knowledgeable and conscious about information security. In the study conducted by Yıldırım and Varol (2013), the awareness of instructors, university students and other social network users about the security measures that can be taken in social networks was evaluated using a descriptive survey model. A total of 211 students, 72 lecturers and 23 other institutional employees from two state universities participated in the study. The findings showed that students and other users did not have sufficient awareness of security measures on social networks and were exposed to misuse of their personal information. The study conducted by Özdemir and Uluyol (2021) aimed to reveal the information security awareness of public employees. This quantitative research was conducted with 501 participants using a descriptive survey model and data were collected using the Information Security Awareness Scale. As a result of the research, it was determined that the information security awareness of public employees is at a medium level and especially information technology employees with technical education and participants under the age of 40 have high awareness levels. Karakaya and Yetgin (2020) conducted research on personal cyber security for Karabük University employees. In this study, hypotheses were tested on topics such as not accepting friend requests from social networks, not keeping information on devices other than personal computers, and using antivirus software. The study revealed that the participants were aware of external threats but showed deficiencies in the use of anti-virus software.

Özbilen and Çağlar (2020) conducted a study to determine the current state of information and information security in the Turkish public sector. This study focused on the concept of cyber security and the responsibilities of relevant institutions, and data were collected and analyzed from secondary sources. The study emphasized that important steps have been taken in the field of information and information security in Turkey, but further preparation is needed.

4. Method

In this study, it is aimed to determine the cyber security awareness levels of public personnel and to evaluate their practical applications in this field. The sample of the research consists of the personnel in Ardahan Provincial Security Directorate. In the research, it was tried to reach the widest possible sample within the temporal and financial possibilities. For the survey application, the approval of Ardahan University Ethics Committee dated 23.11.2023 and numbered 2300037382 was obtained. The research was conducted with a total of 302 public personnel participants and an analysis was carried out on six different dimensions (confidentiality, control/ possession, integrity, authenticity, accessibility and utility) using the Cyber Security Scale (CSS). The study was designed in line with the following questions.

- Do cyber security levels differ according to general characteristics?
- Does the dimension of privacy differ according to general characteristics?
- Does the control- possession dimension differ according to general characteristics?
- Does the integrity dimension differ according to general characteristics?
- Does the dimension of authenticity differ according to general characteristics?
- Does the accessibility dimension differ according to general characteristics?
- Does the dimension of utility differ according to general characteristics?

IBM SPSS 28 and AMOS 24 statistical package programs were used to analyze the data obtained in the study and various statistical tests were applied on the data set. In order to increase the reliability and validity level of the research, frequency and cross tabulations were analyzed with the help of descriptive statistics, number and percentage values for categorical parameters, and mean, standard deviation, minimum and maximum values for numerical variables. In order to evaluate the distribution characteristics of the numerical variables, normality assumptions were examined with skewness and kurtosis values. The findings revealed that the data showed a normal distribution.

4.1. Modeling and Data Collection

In the study, the 24-question cyber security scale developed by Arpaci & Sevinç (2022) was used. The scale consists of confidentiality (1-3 questions), control- possession (4-8), integrity (9-12), authenticity (13-17), accessibility (18-21) and utility (22-24) dimensions. The scale uses a 5-point Likert scale ranging from “strongly disagree” to “strongly agree”. The range of points that can be obtained from the scale varies between 24 and 120. Questions 11, 13, 14, 15, 16, 17, and 21 of the scale were reverse coded.

Table 1. Reliability and distributional properties

	Cronbach Alfa	No. of items	Skewness	Kurtosis
Cyber Security Scale	0,880	24	0,286	-0,280
Confidentiality	0,810	3	-0,152	-0,068
Control / Possession	0,822	5	-0,416	-0,381
Integrity	0,752	4	-0,078	-0,351
Authenticity	0,771	5	-0,939	1,007
Availability	0,807	4	0,074	-0,524
Utility	0,704	3	-0,539	0,435

For reliability analysis, Cronbach Alpha coefficient is generally used. It is desired that the Cronbach Alpha coefficient should be at least 0.7 (Karagöz, 2021). According to Karagöz (2021), the Cronbach Alpha coefficient of the cyber security scale and its dimensions is reliable. One of the ways to understand whether the data are normally distributed is to look at the skewness and kurtosis values. Skewness and kurtosis values between -1.5 and +1.5 indicate that the data have a normal distribution (Tabachnick and Fidell; 2013). According to Tabachnick and Fidell (2013), it is seen that the skewness and kurtosis values of the cyber security scale and dimensions used in the study are within the normal distribution limits. Since the data were found to be normally distributed, independent sample T-test and Anova (one-way variance) analysis were used. In case the Anova analysis was significant, the Bonferroni test, one of the Post-Hoc tests, was used to determine which groups the difference was significant. While creating the research report, 95% confidence interval ($p<.05$) was used for significance level.

5. Findings

5.1. Demographic Findings for Participants

Descriptive information about the 302 security personnel who participated in the study is shown in Table 2.

Table 2. Findings on socio-demographic characteristics

General Information		**n**	**%**
Gender	Male	273	90,4
	Female	29	9,6
Age	18-25	6	2,0
	26-35	229	75,8
	36-45	44	14,6
	46 +	23	7,6
Education	High School	7	2,3
	Associate degree	32	10,6
	License	232	76,8
	Master's Degree	31	10,3
Duration in the profession	2-5 Years	36	11,9
	6-10 Years	186	61,7
	11-15 Years	40	13,2
	16 Years and Over	40	13,2
Daily Internet Usage	1-2 Hours	42	13,9
	3-4 Hours	154	51,0
	5-7 Hours	74	24,5
	8 Hours and Over	32	10,6
Purpose of Internet Use*	Mobile Banking	260	86,1
	E-government Services	193	63,9
	E-commerce Shopping	189	62,6
	Other	51	16,9

***** Multiple Answer

Of the participants, 273 (90.4%) were male and 229 (75.8%) were between the ages of 26-35. Of the police personnel participating in the study, 232 (76.8%) were undergraduate graduates and 186 (61.7%) had 6-10 years of professional experience. 154 (51%) of the participants stated that they use the internet 3-4 hours a day. 260 (88.1%) of the police personnel stated that mobile banking, 193 (63.9%) e-government services and 189 (62.6%)

e-commerce shopping were the purposes of internet use. On the other hand, 51 of the participants stated that they use the internet for other reasons such as news, entertainment and social media.

5.2. Findings Related to Cyber Security Scale

The mean scores of the participants on the cyber security scale, their minimum and maximum mean scores and descriptive statistics are shown in Table 3.

Table 3. Findings on socio-demographic characteristics

Scale and Subscales	$\bar{X}$	Ss	Points received	
			Min.	Maks.
Cyber Security Scale	94,41	9,71	73	120
Confidentiality	12,72	1,56	7	15
Control / Possession	21,73	2,71	12	25
Integrity	16,27	2,35	8	20
Authenticity	20,04	4,06	5	25
Availability	13,31	3,69	4	20
Utility	10,34	2,48	3	15

Since it was determined that the participants had a total average score of 94.41 from the cyber security scale, it can be said that the cyber security awareness levels of the public personnel participating in the survey are at a medium level. The total score that can be obtained from the scale varies between 24 and 120. Whether cyber security awareness differs in terms of general characteristics is shown in Table 4. The values shown in bold in the Table are the factors for which a statistically significant difference was detected.

Table 4. Cyber security and general features comparison

General Information		$\bar{X}$	Ss	Test	p
Gender	Male	94,50	9,80	t=0,914	0,435
	Female	93,44	8,93		
Age	18-25	94,50	9,69	F=1,434	0,233
	26-35	94,13	9,54		
	36-45	96,52	10,71		
	46 +	93,00	9,43		
Education	High School	87,85	6,91	F=3,006	**0,031***
	Associate degree	94,93	9,74		
	License	90,78	8,11		
	Master's Degree	95,64	10,47		
Duration in the profession	2-5 Years	95,25	8,73	F=2,044	0,108
	6-10 Years	94,54	9,73		
	11-15 Years	91,20	8,13		
	16 Years and Over	96,22	11,38		
Daily Internet Usage	1-2 Hours	96,00	9,30	F=4,104	**0,007***
	3-4 Hours	93,53	9,28		
	5-7 Hours	93,16	10,19		
	8 Hours and Over	99,37	9,77		

*** p<0,05**

It was observed that males ($\bar{X}$=94.50) had higher cyber security total score average than females ($\bar{X}$=93.44). However, the score difference determined according to gender was not statistically significant (t=0.914; p>0.05). It was observed that high school graduates ($\bar{X}$=87.85), associate degree graduates ($\bar{X}$=94.93), bachelor's degree graduates ($\bar{X}$=90.78) and master's degree graduates ($\bar{X}$=95.64) had higher cyber security total score average (F=3.006; p<0.05). According to the Bonferroni test conducted to determine between which groups the difference lies; it was determined that the total cyber security score averages of the participants with an associate degree were statistically significantly higher than the participants with a bachelor's degree. It was observed that the participants with a daily internet use time of 1-2 hours ($\bar{X}$=96.00), participants with 3-4 hours ($\bar{X}$=93.53), participants with 5-7 hours ($\bar{X}$=93.16) and participants with more than 8 hours ($\bar{X}$=99.37) had a higher total cyber security score average (F=4.104; p<0.05). According to the Bonferroni test conducted to determine between which groups the difference lies; it was determined that the total cyber security score averages of the participants with more than 8 hours of internet use were statistically significantly higher than the participants with 3-4 hours and 5-7 hours of internet use. Statistically significant differences in cyber security awareness of the dimensions of confidentiality, control / possession, integrity, authenticity, availability and utility used in the cyber security scale are given in Table 5 below.

Tablo 5. Cyber security dimensions and general features

Dimensions	General Information		$\bar{X}$	Ss	Test	p
Confidentiality	**Education**	High School	11,85	1,06	F=2,775	0,042*
		Associate degree	12,71	1,58		
		License	12,34	1,51		
		Master's Degree	13,29	1,32		
	Daily Internet Usage	1-2 Hours	13,00	1,62	F=2,650	0,049*
		3-4 Hours	12,63	1,48		
		5-7 Hours	12,47	1,61		
		8 Hours and Over	13,28	1,54		
Control / Possession	**Daily Internet Usage**	1-2 Hours	22,00	2,69	F=2,717	0,045*
		3-4 Hours	21,46	2,83		
		5-7 Hours	21,60	2,40		
		8 Hours and Over	22,90	2,56		
Integrity	**Daily Internet Usage**	1-2 Hours	16,69	2,31	F=3,311	0,020*
		3-4 Hours	15,90	2,23		
		5-7 Hours	16,39	2,52		
		8 Hours and Over	17,15	2,30		
Availability	**Duration in the profession**	2-5 Years	13,02	3,68	F=3,723	0,012*
		6-10 Years	13,26	3,69		
		11-15 Years	12,22	3,20		
		16 Years and Over	14,87	3,78		
Utility	**Age**	18-25	11,66	1,86	F=4,976	0,002*
		26-35	10,58	2,32		
		36-45	9,61	2,72		
		46 +	9,00	2,98		
	Education	High School	8,28	1,63	F=2,775	0,042*
		Associate degree	10,48	2,29		
		License	9,56	3,09		
		Master's Degree	10,51	2,98		
	Duration in the profession	2-5 Years	10,61	2,67	F=2,186	0,090*
		6-10 Years	10,54	2,31		
		11-15 Years	9,77	2,49		
		16 Years and Over	9,70	2,90		

* **p<0,05**

When the confidentiality dimension was analysed according to sociodemographic characteristics, it was seen that the participants who graduated from high school ($\bar{X}$=11.85), the participants who graduated from associate degree ($\bar{X}$=12.71), the participants who graduated from bachelor's degree ($\bar{X}$=12.34) and the participants who graduated from master's degree ($\bar{X}$=13.29) had the mean total score of the confidentiality dimension (F=2.775; p<0.05). According to the Bonferroni test conducted to determine between which groups the difference was between; it was determined that the mean total score of the privacy dimension of the participants with a master's degree was statistically significantly higher than the participants with a bachelor's degree. It was observed that the participants whose daily internet usage time was 1-2 hours ($\bar{X}$=13,00), 3-4 hours ($\bar{X}$=12,63), 5-7 hours ($\bar{X}$=12,47) and over 8 hours ($\bar{X}$=13,28) had the mean total score of the privacy dimension (F=2,650; p<0,05). According to the Bonferroni test conducted to determine between which groups the difference is between; it was determined that the mean total score of the privacy dimension of the participants with over 8 hours of internet use was statistically significantly higher than the participants with 5-7 hours of internet use. When the control / possession dimension was analysed, it was seen that the participants whose daily internet usage time was 1-2 hours ($\bar{X}$=22,00), 3-4 hours ($\bar{X}$=21,46), 5-7 hours ($\bar{X}$=21,60) and over 8 hours ($\bar{X}$=22,90) had the mean total score of the control- possession dimension (F=2,717; p<0,05). According to the Bonferroni test conducted to determine between which groups the difference was between; it was determined that the mean total score of the control / possession dimension of the participants with over 8 hours of internet use was statistically significantly higher than the participants with 3-4 hours of internet use.

In the integrity dimension, there is a significant difference between daily internet use and cyber security awareness. It was observed that participants with daily internet usage time of 1-2 hours ($\bar{X}$=16,69), 3-4 hours ($\bar{X}$=15,90), 5-7 hours ($\bar{X}$=16,39) and over 8 hours ($\bar{X}$=17,15) had a total mean score of integrity dimension (F=3,311; p<0,05). According to the Bonferroni test conducted to determine between which groups the difference was between; it was determined that the mean total score of the integrity dimension of the participants with over 8 hours of internet use was statistically significantly higher than the participants with 3-4 hours of internet use. No significant relationship was found between the socio-demographic characteristics in the authenticity dimension and the factors used in the cyber security scale. A statistically significant relationship was also found between the availability dimension and the time in the profession. According to the table, it was seen that the participants with a professional period of 2-5 years ($\bar{X}$=13,02), 6-10 years ($\bar{X}$=13,26), 11-15 years ($\bar{X}$=12,22) and over 16 years ($\bar{X}$=14,87) had the mean total score of the availability dimension (F=3,723; p<0,05). It was determined that the mean total score of the availability dimension of the participants with an occupational duration of more than 16 years was statistically significantly higher than the participants with an occupational duration between 6-10 years and 11-15 years. In the utility dimension, it was observed that the participants between the ages of 18-25 ($\bar{X}$=11,66), 26-35 ($\bar{X}$=10,58), 36-45 ($\bar{X}$=9,61) and over 46 ($\bar{X}$=9,00) had the mean total score of the utility dimension (F=4,976; p<0,05). In addition, it was determined that the utility dimension total mean scores of the participants over the age of 46 were statistically significantly lower than the participants between the ages of 26-35. Considering the educational level of the participants, it was determined that the mean total score of the utility dimension of the participants with associate's degree was statistically significantly higher than that of the participants with high school graduates.

Finally, it was seen that the participants with an occupational duration of 2-5 years ($\bar{X}$=10,61), 6-10 years ($\bar{X}$=10,54), 11-15 years ($\bar{X}$=9,77) and over 16 years ($\bar{X}$=9,70) had a total mean score of the benefit dimension (F=2,186; p<0.05) and it was determined that the mean total score of the benefit dimension of the participants with an occupational period over 16 years was statistically significantly lower than the participants with an occupational period between 6-10 years.

6. Conclusion and Discussion

The main purpose of this study is to determine the cyber security awareness levels of public personnel and to evaluate their practical applications in this field. The study was conducted with a total of 302 public personnel participants and an analysis was carried out on six different dimensions (confidentiality, control/ possession, integrity, authenticity, availability and utility) using the Cyber Security Scale (CSS). In the study, the majority of the participants (90.4%) were male and 75.8% were between the ages of 26-35. This demographic structure allows the results of the study to be generalised especially over this age group and gender. In terms of education level, the majority of the participants (76.8%) are bachelor's degree graduates, and their professional years generally range between 6-10 years (61.7%). These findings indicate that police personnel generally have a high level of education and a medium level of professional experience. When the daily internet usage time was analysed, more than half of the participants (51%) stated that they spend 3-4 hours on the internet daily. Mobile banking (88.1%), e-government services (63.9%) and e-commerce (62.6%) were the most frequently repeated reasons for using the Internet. This situation shows that public personnel use the Internet for functional and daily life facilitating services. In the study of Masum (2022) in the literature, it is stated that internet use is more likely to be done by women for social media. In this study, on the other hand, social media is included at a low rate (17.3%) as the purpose of internet use, which may indicate differences arising from demographic structure. These findings highlight the effect of gender on cyber security behaviors and a similar trend is observed in our study. It was determined that male participants took cyber security measures more actively and participated in trainings on this subject more frequently.

In the study, the cyber security status of the participants was evaluated under various dimensions. As a result of the analyses made on the cyber security scale, the average total score of the participants was 94.41. The total score range of this scale varies between 24 and 120, so the average score obtained is in the upper middle segment of the scale and it can be interpreted that the participants generally have sufficient awareness of cyber security. The scores obtained by the participants from the sub-dimensions of the cyber security scale were analysed separately. The average score obtained from the confidentiality dimension is 12.72 and the possible score range for this dimension varies between 3 and 15. This result means that the participants showed a high level of awareness about privacy. These findings are in line with wider research and indicate that privacy concerns are common among Internet users (Malhotra et al., 2004). It includes various dimensions such as information privacy, personal communication privacy and data privacy, and covers a broad construct (Crossler, 2011). Factors such as education level have been associated with differences in privacy concerns, and higher education levels are generally associated with increased awareness and concerns about privacy (Wang et al., 2022). Furthermore, studies on how the duration of internet use may affect individuals' perceptions of privacy have revealed that longer duration of use is associated with higher concerns (Denis et al., 2023).

Within the scope of the results obtained from the study, it was determined that public personnel have a general knowledge on cyber security issues; however, they do not have sufficient knowledge and practice, especially against advanced threats. It was concluded that the training required to increase the cyber security awareness of public personnel are insufficient and that these trainings should be made more effective, applied and continuous. The content of training programmes should be expanded to cover current cyber threats and should include practical applications to make the personnel more aware and equipped against these threats. According to the results of the analysis, although there are cyber security policies in public institutions, there are serious deficiencies in the applicability and effectiveness of these policies. It is recommended that these policies should be reviewed, made realistic and applicable, and internal audit mechanisms should be strengthened. In addition, considering the seriousness of the damage caused by cybercrimes and security breaches, it is of great importance to promote information security culture among employees at all levels to better protect public personnel against these threats.

Ethics Committee Declaration

The study was evaluated by Ardahan University Scientific Research and Publication Ethics Committee and found ethically appropriate with the decision numbered E-67796128-000-2300037382 on November 17, 2023. In addition, the relevant document has been uploaded to the DergiPark system by the corresponding author.

Author Contribution Rate Statement

The data were collected by Barış Daşdemir. The analysis was conducted by Barış Daşdemir and Salih Serkan Kaleli. The literature review was conducted by Barış Daşdemir. The conclusion and discussion section were written jointly by the authors.

Conflict Statement

There is no conflict of interest between the authors.

Statement of Support

No support was received from any institution for this study.

References

Aksoğan, M., Bayer, H., Gülada, M., & Çelik, E. (2018). İletişim fakültesi öğrencilerinin siber güvenlik farkındalığı: İnönü Üniversitesi örneği. *Kesit Akademi Dergisi, 4*(13), 271-288.

Aldemir, C., & Merve, K. (2020). Bilgi toplumu, siber güvenlik ve Türkiye uygulamaları. *Kamu Yönetimi ve Politikaları Dergisi, 1*(1), 6-27.

Altıner, İ. (2021). *Öğretmenlerin kişisel siber güvenlik farkındalık düzeylerinin farklı değişkenlere göre değerlendirilmesi* [Yüksek Lisans Tezi], Ankara Üniversitesi.

Arpaci, I., & Sevinc, K. (2022). Development of the Cybersecurity Scale (CS-S): evidence of validity and reliability. *Information Development, 38*(2), 218-226. https://doi.org/10.1177/0266666921997512

Aydemir, M. (2022). The use of communication technologies in web attacks and hacker tagging: Analysis of the zone-h model: iletişim teknolojilerinin web saldırılarında kullanımı ve hacker etiketlemesi: Zone-H modelinin analizi. *Ases Ulusal Sosyal Bilimler Dergisi, 2*(1), 158-179.

Bai, C., Dallasega, P., Orzes, G., & Sarkis, J. (2020). Industry 4.0 technologies assessment: a sustainability perspective. *International Journal of Production Economics, 229*, 107776.

Bekar, S., & Sağlam, M. (2023). Siber âlem: yeni medya ve dijital yurttaşlık. *Niğde Ömer Halisdemir Üniversitesi İletişim Fakültesi Akademik Dergisi, 2*(2), 133-144.

Çakır, H., & Uzun, S. A. (2021). Türkiye'nin siber güvenlik eylem planlarının değerlendirilmesi. *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi, 7*(2), 353-379.

Crossler, R. (2011). Privacy in the digital age: A review of information privacy research in information systems. *Mis Quarterly, 35*(4), 1017. https://doi.org/10.2307/41409971

Denis, N., Laurent, M., & Chabridon, S. (2023). Integrating usage control into distributed ledger technology for internet of things privacy. *IEEE Internet of Things Journal, 10*(22), 20120-20133. https://doi.org/10.1109/jiot.2023.3283300

Dionísio, N., Alves, F., Ferreira, P., & Bessani, A. (2019). Cyberthreat detection from twitter using deep neural networks. *2019 International Joint Conference on Neural Networks (IJCNN)*, Budapest, Hungary. https://doi.org/10.1109/ijcnn.2019.8852475

Ecek, N., & Çakmak, A. F. (2022). Çalışanların bilgi güvenliği önlemlerine dair tutumları: ampirik bir değerlendirme. *International Journal of Applied Economic and Finance Studies, 7*(2), 26-44.

Eminağaoğlu, M., & Gökşen, Y. (2009). Bilgi güvenliği nedir, ne değildir, Türkiye' de bilgi güvenliği sorunları ve çözüm önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *11*(4), 1-15.

Gönç, D. (2022). Siber tehdit taksonomilere siber aktivizm çerçevesinde bir değerlendirme, *Bilgi ve İletişim Teknolojileri Dergisi, 4(2),* 171-196. https://doi.org/10.53694/bited.1112219.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering, 45,* 3171-3189.

International Telecommunication Union. (2022). 2.9 billion people still offline. https://www.itu.int/en/mediacentre/Pages/PR-2021-11-29-FactsFigures.aspx

Karagöz Yalçın, Y. (2021). *Bilimsel araştırma yöntemleri*. Atlas Akademik Basım Yayın.

Karakaya, A., & Yetgin, M. A. (2020). Karabük Üniversitesi çalışanlarına yönelik kişisel siber güvenlik üzerine araştırma. *Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *10*(2), 157-172.

Kızıltan, M. B. (2007). *5237 sayılı Türk ceza kanununda bilişim sistemine girme, sistemi engelleme ve bozma suçları* [Yüksek Lisans tezi, Sosyal Bilimler Enstitüsü].

Korucu, O. (2021). Yeni normal dünya düzeninin siber güvenlik ve bilgi güvenliğine etkileri. *Yönetim Bilişim Sistemleri Dergisi*, *7*(1), 44-60.

Kott, A., & Linkov, I. (2021). To improve cyber resilience, measure it. *Computer*, *54*(2), 80-85. https://doi.org/10.1109/mc.2020.3038411

Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors related to cyber security behavior. *IEEE Access*, *8*(1), 125140-125148.

Kumar, P., Wazid, M., Singh, D., Singh, J., Das, A., & Rodrigues, J. (2023). Explainable artificial intelligence envisioned security mechanism for cyber threat hunting. *Security and Privacy*, *6*(6). https://doi.org/10.1002/spy2.312

Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355. https://doi.org/10.1287/isre.1040.0032

Nair, M. M., & Tyagi, A. K. (2021). Privacy: History, statistics, policy, laws, preservation and threat analysis. *Journal of Information Assurance ve Security*, *16*(1).

Öcal, S. T. A. (2021). Siber güvenlik perspektifinde Türkiye'nin güvenlik stratejileri. *İstanbul Üniversitesi İktisat Fakültesi Mecmuası*, *89*.

Öğün, M. N., Öznacar, B., Tatar, A., & Debeş, G. (2020). Information technologies and reaching to information society. *REICE: Revista Electrónica de Investigación En Ciencias Económicas*, *8*(16), 412-449.

Özbek, M. (2015). The impacts of European cybercrime convention on Turkish criminal law. *GSI Articletter*, *13*, 73.

Özbilen, T., & Çağlar, A. (2020). Türk kamu sektöründe bilgi ve bilişim güvenliği. *Kamu Yönetimi ve Teknoloji Dergisi*, *2*(1), 72-94.

Özdemir, A., & Uluyol, Ç. (2021). Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı. *Türkiye Sosyal Araştırmalar Dergisi*, *25*(3), 649-666.

Özdemirci, F., & Torunlar, M. (2018). Bilgi-değişim-siber güvenlik-bağımsızlık. *Bilgi Yönetimi*, *1*(1), 78-83.

Sağıroğlu, Ş., Şenol, M., Bayındır, R., Bilge, Y., Bensghır, T. K., Akleylek, S., & San, G., (2019). *Siber güvenlik ve savunma: Problemler ve çözümler*. Grafiker Yayınevi.

Salem, Y., Moreb, M., & Rabayah, K. S. (2021). Evaluation of information security awareness among Palestinian learners. In *International Conference on Information Technology* (pp. 21-26).

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *The Journal of Digital Forensics, Security and Law*, *12*(2), 53-74.

Solms, R. V., & Niekerk, J. V. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102.

Srivastava, K. (2019). A new approach of artificial intelligence (ai) to cyber security. *International Journal of Research in Advent Technology*, *7*(1), 410-412. https://doi.org/10.32622/ijrat.71201980

Tanrıverdi, M. (2020). A systematic review of privacy preserving healthcare data sharing on blockchain. *Journal of Cybersecurity and Information Management*, *5*, 31-37.

Tekerek, M., & Tekerek, A. (2013). A research on students' information security awareness. *Turkish Journal of Education*, *2*(3).

Yıldırım, N., ve Varol, A. (2013). Sosyal ağlarda güvenlik: Bitlis Eren ve Fırat Üniversitelerinde gerçekleştirilen bir alan çalışması. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, *6*(1).

Yıldırım, Y. (2020). Farklı disiplinlerde endüstri 4.0. *OPUS International Journal of Society Researches*, *15*(21), 756-789.

You, Z., & Feng, L. (2020). Integration of industry 4.0 related technologies in construction industry: A framework of cyber-physical system. *IEEE Access*, *8*, 122908-122922.

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. *SN Computer Science*, *3*(2), 127.