Interdisciplinary Description of Complex Systems 24(5), 574-589, 2026

INFORMATION SECURITY AWARENESS OF PRIVATE SECTOR AND PUBLIC INSTITUTION EMPLOYEES AGAINST CYBER RISKS

Cebrail Yakışır*

Presidency of Religious Affairs
Ankara, Türkiye

DOI: 10.7906/indecs.24.5.4
Regular article

Received: 6 December 2025.
Accepted: 12 July 2026.

ABSTRACT

This study aims to comparatively examine the information security awareness levels of public and private sector employees in Türkiye in the face of growing cyber risks. Conducted using quantitative methods, the research collected data from 430 participants through a valid and reliable scale, and analyzed the results using statistical techniques such as factor analysis, t-tests, ANOVA, and chi-square tests. The findings, consistent with the existing literature, indicate that information security awareness can be conceptualized across four fundamental dimensions: confidentiality, integrity, privacy, and availability. One of the key results of the study is that public sector employees exhibit significantly higher levels of awareness in the dimensions of confidentiality, integrity, and privacy compared to their counterparts in the private sector. In contrast, demographic variables such as gender, education level, and tenure were not found to have a significant impact on awareness. The research highlights that information security awareness is shaped by sector-specific dynamics and underscores the importance of organizational culture. Consequently, it is recommended that comprehensive, continuous, and multidimensional security awareness programs be developed for all employees. Future studies are advised to employ qualitative methods to explore the underlying reasons for these differences in greater depth.

KEY WORDS

information security awareness, cybersecurity, organizational culture, private sector, public sector

CLASSIFICATION

JEL: K24, L33

*Corresponding author, η: cebrailyakisir@hotmail.com; +90 533 297 64 27;
Merkez Mahallesi Külleci Sokak 40/22 Pursaklar, Ankara, Türkiye

INTRODUCTION

The rapid advancements in information and communication technologies have increased institutions' dependence on digital infrastructures, consequently creating a need for stronger measures against cyber threats. Public institutions and private-sector organizations, in particular, conduct a substantial portion of their operations through digital systems, making information security risks a critical managerial responsibility [1]. Information security is not merely a technical issue but also a phenomenon closely linked to employees' awareness levels and organizational decision-making processes [2]. In the context of public administration, information systems security has become an integral component of internal control and risk management processes. Studies conducted within public institutions reveal that standards, guidelines, and audit practices have been adopted to identify, measure, and mitigate risks [3]. However, the establishment of a robust security culture in the public sector cannot be achieved solely through technical measures; it also requires organizational awareness, continuous monitoring, and a balanced approach to privacy and service delivery [4].

In the private sector, awareness levels vary significantly across industries. Studies conducted particularly within SMEs indicate that while managers tend to exhibit relatively high awareness of cyber threats, a comprehensive security culture has not yet been fully established at the employee level [5]. In highly regulated sectors such as banking, the protection of personal data and information security are more strongly embraced at the managerial level due to the binding nature of legal requirements [6]. Moreover, the financial management of cyber risks also influences the issue of awareness. Research on cyber insurance in Türkiye indicates that due to employees' lack of awareness, insurance products are not sufficiently adopted, resulting in limited utilization of risk-transfer mechanisms [7]. This situation highlights the necessity for employees in both the private and public sectors to actively engage with and support institutional information security policies.

In this study, the information security awareness of public institution employees and private-sector employees in the face of cyber risks will be examined comparatively. In light of the existing literature, similarities and differences in managerial awareness levels, as well as areas requiring improvement, will be discussed.

LITERATURE

Studies on information security and cyber risk awareness reveal both similarities and differences between the public and private sectors. From the perspective of public institutions, the security of information systems is largely shaped by legal and organizational infrastructures. In Türkiye, the explicit definition of public administrations' responsibilities under the *Law on the Protection of Personal Data No. 6698* (*KVKK*) has been one of the most significant factors contributing to increased awareness in this field [3]. Furthermore, research conducted in public institutions emphasizes the importance of implementing standards in the management of information security risks [8]. Despite this, it is noted that awareness levels are not fully reflected in managerial decisions, and challenges persist particularly in maintaining consistent top-management support.

From the perspective of the private sector, cybersecurity awareness is primarily driven by competition, customer trust, and financial risk management. Studies in the banking sector indicate that while managers demonstrate high levels of awareness regarding the protection of customer data and information security management processes, vulnerabilities arise in practice due to employees' lack of training [9]. Similarly, research conducted in the e-commerce domain shows that managerial awareness regarding the protection of personal data has increased, yet discrepancies exist between technical measures and user practices [10].

Studies focusing particularly on SMEs in the private sector present a different picture. Field research conducted in SMEs indicates that while managers acknowledge the potential risks of cyberattacks, they often lack sufficient knowledge about the measures that should be taken to mitigate these risks [5]. Consequently, despite the presence of awareness, a systematic security culture has not been fully established at the organizational level. Additionally, the literature highlights the role of cyber insurance in the context of awareness. The low adoption rates of cyber insurance products in Türkiye reveal a disconnect between managers' risk perception and financial risk mitigation mechanisms [11]. This suggests that private sector managers are insufficiently integrating cybersecurity strategies with financial risk management.

Finally, international studies have compared the awareness levels of public and private sector managers within the context of the European Union's *General Data Protection Regulation* (GDPR), revealing that awareness is linked not only to technical aspects but also to ethical and legal responsibilities [12].

METHOD

This study aims to examine the information security awareness and awareness levels of public institution and private-sector employees in the face of cyber risks. It also seeks to identify the relationship between this awareness and various sociodemographic characteristics. The research was conducted using a quantitative survey model. The research model and hypotheses developed in line with this approach are presented in the following section.

RESEARCH MODEL AND HYPOTHESES

The hypotheses developed in accordance with the research model are presented in Figure 1.

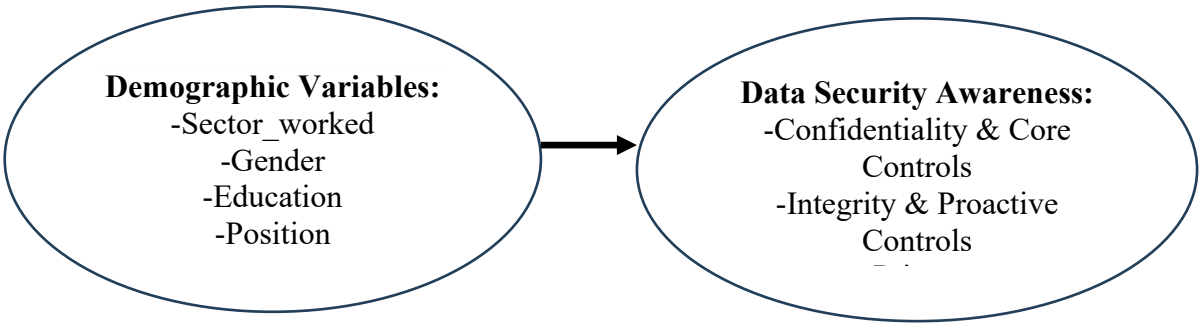


Figure 1. Research model.

H_1: Information security awareness significantly differs according to the sector of employment.
H_2: There is a significant relationship between the sector of employment and information security awareness levels.
H_3: Information security awareness significantly differs according to gender.
H_4: There is a significant relationship between gender and information security awareness levels.
H_5: Information security awareness differs depending on whether a computer has antivirus software installed.
H_6: There is a significant relationship between having antivirus software on the computer and information security awareness levels.
H_7: Information security awareness differs according to education level.
H_8: There is a significant relationship between education level and information security awareness levels.
H_9: Information security awareness differs according to job position.

H_{10}: There is a significant relationship between job position and information security awareness levels.
H_{11}: Information security awareness differs according to tenure.
H_{12}: There is a significant relationship between tenure and information security awareness levels.

DATA COLLECTION INSTRUMENTS

Firstly, ethical approval for conducting the research was obtained from the Istanbul Gelişim University Ethics Committee with decision number 2025-15. Subsequently, an online survey was designed using Google Forms, consisting of questions on participants' sociodemographic characteristics and the information security awareness scale developed by [13], whose reliability and validity have been established. The survey was structured to measure employees' perceptions, awareness, and behaviors regarding information security. A 5-point Likert scale was employed for the survey items (1 – Strongly Disagree, ..., 5 – Strongly Agree), allowing participants to quantitatively express their attitudes and perceptions.

POPULATION AND SAMPLE

A total of 430 public and private sector employees working in Türkiye participated in the study. Participants were selected using purposive sampling, and the survey link was shared with volunteers. The purpose of the research was explained to the participants, and principles of anonymity and confidentiality were strictly observed. The collected data were used solely for scientific purposes.

LIMITATIONS OF THE STUDY

Although the participant distribution covers the whole of Türkiye, the sample is based on voluntary participation; therefore, the generalizability of the results is limited. Since the survey used in the study is self-reported, discrepancies may exist between participants' actual behaviors and their perceptions. Additionally, the literature review included only accessible academic studies, while grey literature (such as institutional reports and policy documents) was excluded.

STATISTICAL ANALYSES

First, frequency analyses were conducted to present the findings related to the sociodemographic characteristics of the participants. Next, exploratory factor analysis was applied to identify the dimensions of the information security awareness scale for the research sample. Descriptive statistics and reliability analyses for the dimensions obtained from the factor analysis were then provided. To test the research hypotheses, various statistical techniques were employed. Specifically, an independent samples t-test, a parametric test, was conducted to determine the difference in information security awareness levels between public and private sector participants. Additionally, a chi-square test of independence was performed to evaluate the distribution of awareness levels (low, medium, high) according to sector type, allowing both mean differences and distributional variations to be assessed. Furthermore, independent samples t-tests and one-way ANOVA tests were used to determine whether information security awareness levels differed according to various sociodemographic variables. The analyses were performed using IBM SPSS 23 software.

FINDINGS

In this section of the study, the findings of the statistical analyses conducted to reveal the demographic characteristics of the participants and to test the research hypotheses are presented. These analyses include frequency distributions, normality tests, factor analysis, reliability tests, correlation analyses, independent samples t-tests, ANOVA, and chi-square tests.

DEMOGRAPHIC FINDINGS

The descriptive findings regarding the participants' gender, age, education level, job position, and tenure are presented in Table 1.

Table 1. Demographic findings.

Demo info	Groups	*n*	%	Demo info	Groups	*n*	%
Gender	Female	71	16,5	*Sector worked*	Public	313	72,8
	Male	359	83,5		Private	117	27,2
Age Range	20-29	31	7,2	*Company age*	0-5	23	5,3
	30-39	87	20,2		6-10	24	5,6
	40-49	172	40,0		11-15	34	7,9
	50-59	121	28,1		16-20	49	11,4
	more than 60	19	4,4		more than 21	300	69,8
Income (Monthly)	22 000-40 000 TRY	34	7,9	*Education*	High School or Below	22	5,1
	40 000-60 000 TRY	125	29,1		Associate Degree	33	7,7
	60 000-85 000 TRY	148	34,4		Bachelor's Degree	220	51,2
	more than 85 000 TRY	123	28,6		Postgraduate	155	36,0
Position	Top Management	120	27,9	*Company size*	0-10	55	12,8
	Mid-Level Management	91	21,2		11-49	96	22,3
	Technical Staff	77	17,9		50-249	87	20,2
	Administrative Staff	142	33,0		more than 250	192	44,7
Aut method	No technique used	73	17,0	*Tenure*	0-5 year	93	21,6
	Single factor (username + password)	235	54,7		6-10 year	60	14,0
	Hardware (smart cards)	46	10,7		11-15 year	71	16,5
	Two-factor (digital certificates + token)	61	14,2		16-20 year	48	11,2
	Third factor (biometrics)	15	3,5		more than 21	158	36,7
Password creation	Use default password	12	2,8	*Password change*	Never change	40	9,3
	Use easy-to-remember password	69	16,0		Change if compromised	44	10,2
	Use at least 6 characters	36	8,4		Change if shared	30	7,0
	Use complex password (mixed characters)	288	67,0		Change very often	38	8,8
	Use same password everywhere	14	3,3		Change at least every 6 months	215	50,0
	Use short passwords	11	2,6		Change at least yearly	63	14,7
Antivirus update	Less than 6 months ago	104	24,2	*Antivirus available in PC*	Yes	316	73,5
	Less than 1 year ago	172	40,0		No	114	26,5
	Less than 2 years ago	26	6,0				
	3 years ago or more	24	5,6				
	Never updated	104	24,2				

Table 1 shows that 72,8% of the participants work in public institutions, while 27,2% are employed in the private sector. Regarding gender distribution, 16,5% of the participants are female, and 83,5% are male. Examining the age distribution, the largest group (40%) falls

within the 40-49 age range, followed by the 50-59 age group at 28,1%. In terms of monthly income, 34,4% of participants earn between 60 000 TRY and 85 000 TRY, while 29,1% earn between 40 000 TRY and 60 000 TRY. According to job position within their organizations, 33% of participants are technical staff, 27,9% are senior managers, 21,2% are middle-level managers, and 17,9% are administrative personnel. This indicates a balanced participation in terms of organizational positions. Seventeen percent of the participants reported not using any authentication method when accessing their computers, while the majority (54,7%) indicated using single-factor authentication (username-password), and 14,2% reported using two-factor authentication methods. These results suggest that, in terms of information security awareness, technical practices and the level of consciousness are not yet sufficiently widespread.

When examining password creation habits, 67% of participants reported creating complex and strong passwords, while 23,7% fell into categories considered weak password practices, such as using default passwords, easy-to-remember passwords, the same password everywhere, or short passwords – a non-negligible proportion. Additionally, 50% of participants change their passwords every six months, indicating a certain level of awareness. On the other hand, 14,7% update their passwords annually, and 9,4% have never changed their passwords. Findings related to antivirus usage indicate that 73,5% of the participants have antivirus software installed on their computers, while 26,5% do not use any antivirus program. Regarding education level, 51,2% of the participants hold a bachelor's degree, 36% have a postgraduate degree, and 7,7% possess an associate degree. These results indicate that the sample generally has a high level of education. In terms of organizational size, 44,7% of participants work in institutions with 250 or more employees, 22,1% in institutions with 11-49 employees, and 20,2% in institutions with 50-249 employees. Regarding tenure, 36,7% of participants have 21 years or more of work experience, while the proportions of the other groups are relatively balanced.

NORMALITY TEST, FACTOR ANALYSES, AND RELIABILITY ANALYSES FINDINGS

Before testing the research hypotheses, the data were examined to determine whether they met the assumption of normal distribution. Skewness and kurtosis values for the items of the information security awareness scale were observed to be between –2 and +2. Therefore, the scale data were considered to be normally distributed [14]. Once the normality assumption was confirmed, factor analysis was conducted.

FINDINGS OF FACTOR AND RELIABILITY ANALYSIS OF THE INFORMATION SECURITY AWARENESS SCALE

The results obtained from the factor analysis of the information security awareness scale, along with the calculated Cronbach's Alpha coefficients, are presented in Table 2.

During the factor analysis of the information security awareness scale, the principal component analysis method was used, and Varimax rotation, which is widely adopted in the literature, was applied. Items with low factor loadings (below 0,40) or those that loaded on multiple dimensions were removed from the scale. Accordingly, five items (Items 19, 28, 29, 30, and 37) were excluded due to low factor loadings. After removing these items, factor analysis was conducted with the remaining 28 items. When eigenvalues were used as the primary criterion for determining the number of factors, the items appeared to group into three dimensions, differing from the original scale. However, considering the alignment with the original scale, the fact that the fourth factor's eigenvalue was very close to 1, and the examination of the scree plot (Figure 2), it was decided that the number of factors should be set to four.

Table 2. Data security awareness scale: factor and reliability analysis findings. Assessment Criteria: KMO Sample Adequacy 0,963; Bartlett's Test for Sphericity 15757,749; p = 0,000 < 0,001; Factor extraction method Principal components analysis (PCA); Rotation method Varimax; Explained Variance Total 79,111; and Cronbach's Alpha 0,979.

Compo-nent	Item	Factor load	Explained Variance	Eigen-value	Cronbach's Alpha
Confidentiality & Core Controls	4. We have a secure document repository.	0,822	63,212	17,699	0,969
	6. A secure information storage area is used.	0,821			
	5. General security policies are implemented.	0,818			
	3. We use information classification.	0,814			
	7. End-user training is prioritized.	0,806			
	9. We protect data integrity in customer communications.	0,790			
	11. Unauthorized data modification is prevented.	0,768			
	8. Downloaded files are scanned for viruses.	0,756			
	1. Unauthorized file access is prevented.	0,750			
	10. A cyber attack would significantly impact us.	0,655			
	13. Email viruses are prevented.	0,619			
	12. System failures significantly slow our work.	0,556			
	16. Third-party system access requires management approval.	0,496			
Integrity & Proactive Controls	22. Spyware installation is blocked.	0,744	7,056	1,976	0,966
	21. Important document alteration is prevented.	0,718			
	24. System failure sources are identifiable from records.	0,715			
	20. Cybersecurity risks are addressed.	0,710			
	25. Problems from system changes are prevented.	0,708			
	23. I know measures against identity theft.	0,664			
	26. Security policy violators face formal discipline.	0,655			
Privacy	35. I understand personal privacy.	0,817	5,486	1,536	0,963
	36. I respect personal privacy in relationships	0,814			
	32. Personal information is not used without consent.	0,728			
	33. Individuals are informed before their data is shared.	0,722			
	34. Personal information is protected against threats.	0,715			
Availability	31. Users who delete documents cannot be identified.	0,824	3,357	0,940	0,743
	15. Measures against malicious email files are neglected.	0,793			
	27. I can download personal files to my work computer.	0,741			

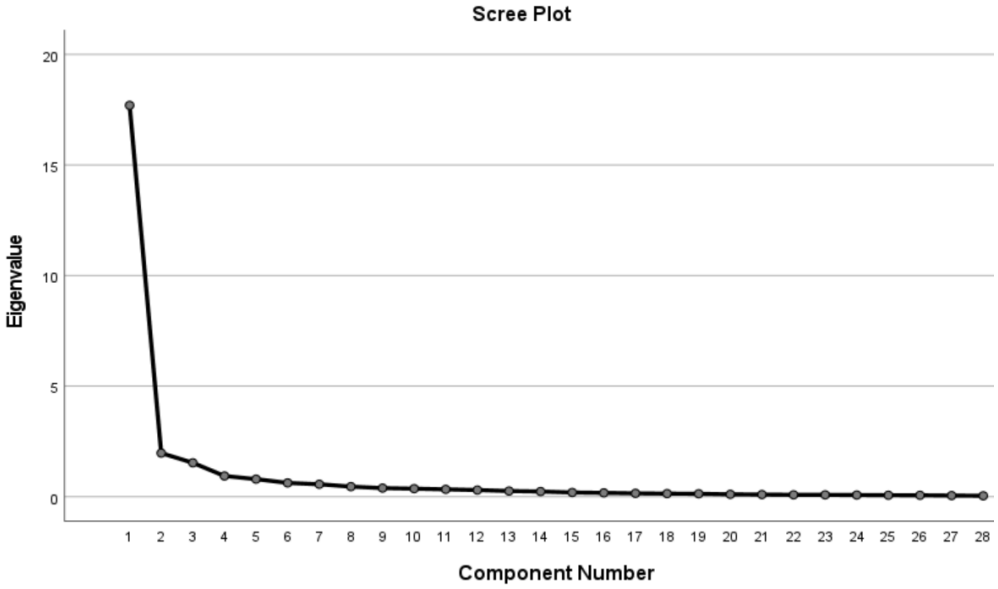


Figure 2. Scree plot.

From Table 2, which displays the results of the factor analysis, it was determined that the first factor consists of thirteen items, the second has seven, the third has five, and the fourth factor has three items.

The loadings of the first factor changes between 0,822 and 0,496. Since the questions grouped under the first factor bring together elements such as "secure document repository", "information classification", and "prevention of unauthorized access", this factor was renamed "Confidentiality & Core Controls", closely aligning with its original term in the scale. The loadings of the second factor range from 0,655 to 0,744. This dimension includes pure "Integrity" items, such as preventing document alteration and maintaining data integrity, as well as items related to traceability and auditing, which are used to ensure integrity. Therefore, this factor was named "Integrity & Proactive Controls", closely aligning with the original scale's designation. The loadings of the third factor range from 0,715 to 0,817. Since most of the items grouped under this factor pertain directly to privacy, this dimension was named "Privacy", consistent with the original scale.

Finally, the items grouped under the fourth dimension of the scale aim to measure behaviors that threaten the availability of the system and information, such as failing to keep records, neglecting security measures, or using the system for personal purposes. Therefore, this factor was named "Availability", consistent with the original scale. Moreover, as seen in Table 2, the total explained variance of the data security awareness scale is 79,11%. Therefore, it can be stated that the four emerging factors together account for a large portion of the variance (almost 80%). Examining the distribution of eigenvalues and explained variances, the Confidentiality & Core Controls factor, which relates to quality maintenance, has the highest eigenvalue (17,699) and the largest explained variance (63,212%). This indicates that among the variables explaining data security awareness, Confidentiality & Core Controls contributes the most. Conversely, the Availability dimension has the lowest eigenvalue (0,940) and the smallest explained variance (3,357%). Additionally, the reliability of the scale and its subdimensions was assessed using Cronbach's Alpha coefficient. Generally, a Cronbach's Alpha value above 0,60 is considered the minimum threshold for acceptable reliability, while a value of 0,70 or higher indicates high internal consistency and strong reliability [14].

Accordingly, after removing the five items excluded during the factor analysis, the remaining 28 items of the data security awareness scale achieved an overall Cronbach's Alpha reliability coefficient of 0,979. As shown in Table 2, the reliability coefficients for the subdimensions are as follows: Confidentiality & Core Controls – 0,969, Integrity & Proactive Controls – 0,966,

Privacy – 0,963, and Availability – 0,743. These results indicate that the first three subdimensions have very high reliability, while the fourth subdimension demonstrates high reliability.

DESCRIPTIVE STATISTICS FOR THE INFORMATION SECURITY AWARENESS SCALE

After the exploratory factor analysis, descriptive statistics were examined by considering the subdimensions. The overall mean values of the scale, the means and standard deviations for each dimension, and the correlation analysis results showing the relationships between the dimensions are presented in Table 3.

Table 3. Descriptive statistics of variables and their dimensions.

Variable	Descriptives				Correlations				
	Mean	Std. Dev.	Skewness	Kurtosis	1	2	3	4	5
1. Confidentiality & Core Controls	3,670	1,166	–0,986	0,007	1	0,819**	0,747**	0,300**	0,941**
2. Integrity & Proactive Controls	3,639	1,192	–0,926	–0,105	0,819**	1	0,824**	0,355**	0,927**
3. Privacy	3,824	1,241	–1,132	0,191	0,747**	0,824**	1	0,363**	0,855**
4. Availability	2,717	1,174	0,313	–0,780	0,300**	0,355**	0,363**	1	0,468**
5. Data security awareness scale	3,5858	1,03372	–1,077	0,462	0,941**	0,927**	0,885**	0,468**	1

*significant at the 0,05 level
**significant at the 0,01 level

As shown in Table 3, the overall Data Security Awareness scale and all of its subdimensions, except for the Availability subdimension, have relatively high mean values. The Availability subdimension has the lowest mean, calculated as 2,717. To ensure that the variables could be subjected to parametric tests, skewness and kurtosis values for each variable were also provided in Table 3. Since all skewness and kurtosis values fall between –2 and +2, the assumption of normal distribution is considered to be met.

Furthermore, the results of the correlation analysis conducted to examine the relationships between the Data Security Awareness variable and its subdimensions are presented in Table 3. As shown in Table 3, the correlations between the Data Security Awareness variable and its subdimensions are significant, positive, and range from moderate to high levels. According to [14], correlation values between 0,00 and 0,30 indicate a low-level relationship, values between 0,30 and 0,70 indicate a moderate-level relationship, and values between 0,70 and 1,00 indicate a high-level or excellent relationship.

Within this framework, examining the correlation analysis results in Table 3 reveals that Confidentiality & Core Controls has a high, positive, and significant relationship with Integrity & Proactive Controls, Privacy, and the overall Data Security wareness variable. In contrast, Confidentiality & Core Controls shows a low-level positive relationship with Integrity & Proactive Controls and Availability. Similar patterns are observed for the other variables, with the exception of the Availability dimension, which exhibits only weak to moderate relationships with all other variables.

FINDINGS RELATED TO THE HYPOTHESES

Determination of Data Security Awareness According to Socio-Demographic Characteristics

To test the first main hypothesis, “Information security awareness differs significantly according to the sector of employment”, and to determine whether there is a difference in the mean awareness scores between groups, an independent samples t-test was conducted. The results are presented in Table 4.

Table 4. T-test results of information security awareness by sector of employment.

Variable	Sector worked	*N*	Mean	Std. Dev.	*t*	*p*
Confidentiality & Core Controls	Public	313	3,74	1,104	1,904	0,059
	Private	117	3,48	1,303		
Integrity & Proactive Controls	Public	313	3,73	1,121	2,461	0,025
	Private	117	3,41	1,344		
Privacy	Public	313	3,95	1,167	3,392	0,002
	Private	117	3,50	1,371		
Availability	Public	313	2,70	1,124	–0,409	0,703
	Private	117	2,76	1,305		

As shown in Table 4, the mean values for the Integrity & Proactive Controls and Privacy subdimensions differ according to the sector of employment. Specifically, the public and private sector means for these dimensions show a considerable gap. However, the mean values for Confidentiality & Core Controls and Availability do not differ significantly between sectors. Notably, the similarity in the Availability dimension means between groups is clearly observable. In light of these findings, the first hypothesis (**H_1**), "Information security awareness differs significantly according to the sector of employment", is partially supported.

Furthermore, to enrich the findings obtained for **H_1**, the second hypothesis (**H_2**), "Information security awareness levels are related to the sector of employment", was tested using a chi-square test of independence to determine whether awareness levels (low/medium/high) are associated with the sector. The results are presented in Table 5.

Table 5. Chi-square results on the relationship between sector worked and dimensions of data security awarenes.

Confidentiality & Core Controls_Level					
Sector worked		**Low**	**Medium**	**High**	
Public	Count	46	42	225	Pearson Chi-Square (χ2) = 6,023 sd: 2 *p* = 0,049 Cramer's V = 0,118
	%	14,7	13,4	71,9	
Private	Count	29	14	74	
	%	24,8	12,0	63,2	
Total	Count	75	56	299	
	%	17,4	13,0	69,5	
Integrity & Proactive Controls_Level					
Public	Count	45	46	222	Pearson Chi-Square (χ2) = 9,901 sd: 2 *p* = 0,007 Cramer's V = 0,152
	%	14,4	14,7	70,9	
Private	Count	32	13	72	
	%	27,4	11,1	61,5	
Total	Count	77	59	294	
	%	17,9	13,7	68,4	
Privacy_Level					
Public	Count	44	25	244	Pearson Chi-Square(χ2) = 10,647 sd: 2 *p* = 0,005 Cramer's V = 0,157
	%	14,1	8,0	78,0	
Private	Count	28	16	73	
	%	23,9	13,7	62,4	
Total	Count	72	41	317	
	%	16,7	9,5	73,7%	
Availability_Level					
Public	Count	147	89	77	Pearson Chi-Square (χ2) =4,766 sd: 2 *p* = 0,092 Cramer's V = 0,105
	%	47,0	28,4	24,6	
Private	Count	58	22	37	
	%	49,6	18,8	31,6	
Total	Count	205	111	114	
	%	47,7	25,8	26,5	

As shown in Table 5, there is a statistically significant relationship between public and private sector employees' Confidentiality & Core Controls awareness levels [$\chi^2(2) = 6{,}023$, $p = 0{,}049$]. The findings indicate that public sector employees (71,9%) have a higher proportion in the "High" confidentiality awareness category compared to private sector employees (63,2%). According to Cramer's V coefficient, the strength of this relationship is weak (V = 0,118).

As can be seen in Table 5, there is a statistically significant relationship between public and private sector employees' Integrity & Proactive Controls awareness levels [$\chi^2(2) = 9{,}901$, $p = 0{,}007$]. This finding further reinforces the pattern observed in the confidentiality dimension. Public sector employees (70,9%) are noticeably more likely than private sector employees (61,5%) to have "High" integrity awareness. However, the strength of this relationship remains at a low-to-moderate level (Cramer's V = 0,152).

Another chi-square test of independence indicates a statistically significant relationship between the sector of employment (public/private) and individuals' Privacy awareness levels [$\chi^2(2) = 10{,}647$, $p = 0{,}005$]. The findings show that public sector employees (78,0%) have a higher proportion in the "High" privacy awareness category compared to private sector employees (62,4%). In contrast, private sector employees report relatively higher proportions in the low and medium privacy awareness categories. However, the strength of this relationship is considered weak (Phi/Cramer's V = 0,157).

Finally, the chi-square analysis examining Availability awareness levels according to the sector of employment is presented in Table 5. The findings indicate that there is no statistically significant relationship between these two variables [$\chi^2(2) = 4{,}776$, $p = 0{,}092$]. Although the table shows a relatively higher proportion of "High Concern" among private sector employees, this difference is not statistically significant. In both sectors, the most common attitude is "Low Concern".

To test the third hypothesis, "Information security awareness differs significantly according to gender", an independent samples t-test was conducted to compare the mean awareness scores between groups. The results are presented in Table 6.

Table 6. T-test results of information security awareness by gender.

Variable	Gender	*N*	Mean	Std. Dev.	*t*	*p*
Confidentiality & Core Controls	Female	71	3,75	0,960	0,728	0,468
	Male	359	3,65	1,203		
Integrity & Proactive Controls	Female	71	3,65	1,018	0,076	0,940
	Male	359	3,64	1,226		
Privacy	Female	71	3,84	1,109	0,138	0,891
	Male	359	3,82	1,267		
Availability	Female	71	2,76	1,057	0,451	0,652
	Male	359	2,71	1,197		

As shown in Table 6, the t-test results indicate that information security awareness does not differ significantly by gender. The similarity in the mean values between groups is directly observable. In light of these findings, the third hypothesis ($\mathbf{H_3}$), "Information security awareness differs significantly according to gender", is rejected.

Furthermore, to enrich the findings of $\mathbf{H_3}$, the fourth hypothesis ($\mathbf{H_3}$), "Information security awareness levels are related to gender", was tested using a chi-square test of independence to examine whether awareness levels (low/medium/high) are associated with gender. The results are as follows.

- Confidentiality & Core Controls: $\chi^2(2) = 3{,}953$, $p = 0{,}139$.
- Integrity & Proactive Controls: $\chi^2(2) = 4{,}758$, $p = 0{,}093$.
- Privacy: $\chi^2(2) = 4{,}048$, $p = 0{,}132$.
- Availability: $\chi^2(2) = 0{,}395$, $p = 0{,}821$.

These findings indicate that there is no statistically significant relationship between gender and any of the awareness subdimensions. Therefore, the **H4** hypothesis, "Information security awareness levels are related to gender", is rejected.

To test the fifth hypothesis, "Information security awareness differs according to whether a computer has antivirus software installed", an independent samples t-test was conducted to compare the mean awareness scores between groups. The results are presented in Table 7.

Table 7. T-test results of information security awareness according to the presence of antivirus software on the computer.

Variable	Virus program availability in PC	*N*	Mean	Std. Dev.	*t*	*p*
Confidentiality & Core Controls	Yes	316	3,74	1,123	1,900	0,059
	No	114	3,48	1,264		
Integrity & Proactive Controls	Yes	316	3,69	1,167	1,376	0,169
	No	114	3,51	1,257		
Privacy	Yes	316	3,85	1,236	0,766	0,444
	No	114	3,75	1,258		
Availability	Yes	316	2,62	1,166	–2,838	0,005
	No	114	2,98	1,163		

As shown in Table 7, the t-test results indicate that information security awareness does not differ significantly across the presence of antivirus software for the first three subdimensions. Only the Availability subdimension shows a noticeable difference. Specifically, the mean values for the first three dimensions are similar between groups, while the mean for Availability is relatively farther apart. In light of these findings, the fifth hypothesis (**H5**), "Information security awareness differs according to whether a computer has antivirus software installed", is largely rejected.

Furthermore, to enrich the findings of **H5**, the sixth hypothesis (**H5**), "The presence of antivirus software on the computer is related to information security awareness levels", was tested using a chi-square test of independence to examine whether awareness levels (low/medium/high) are associated with antivirus presence. The results are as follows:

- Confidentiality & Core Controls: $\chi^2(2) = 4{,}206$, $p = 0{,}122$.
- Integrity & Proactive Controls: $\chi^2(2) = 3{,}485$, $p = 0{,}175$.
- Privacy: $\chi^2(2) = 2{,}401$, $p = 0{,}301$.
- Availability: $\chi^2(2) = 9{,}875$, $p = 0{,}007$.

These findings indicate that, for the first three subdimensions, there is no statistically significant relationship between antivirus presence and awareness levels. However, a significant relationship exists for the *Availability* dimension, although the strength of this relationship is weak (Phi/Cramer's V = 0,157). Thus, the **H6** hypothesis is largely rejected.

To test the next hypothesis, **H7**, "Information security awareness differs according to employees' education level", an independent samples t-test was conducted. The results are presented in Table 8.

As shown in Table 8, the ANOVA analysis indicates that information security awareness does not differ significantly across education levels. Based on these findings, the **H7** hypothesis, "Information security awareness differs according to employees' education level", is rejected.

Furthermore, to enrich the findings of **H7**, the eighth hypothesis (**H8**), "There is a significant relationship between education level and information security awareness levels", was tested using a chi-square test of independence to examine whether awareness levels (low/medium/high) are associated with education level.

The results indicate the following chi-square values and significance levels for the relationship between education level and information security awareness subdimensions.

Table 8. ANOVA test results of information security awareness by education level.

Variable	Education	*N*	Mean	Std. Dev.	*F*	*p*	Sources of difference
Confidentiality & Core Controls	High School or Below	22	3,7107	1,23335	0,800	0,495	-
	Associate Degree	33	3,3774	1,31918			
	Bachelor's Degree	220	3,6736	1,11708			
	Postgraduate	155	3,7208	1,19200			
Integrity & Proactive Controls	High School or Below	430	3,6698	1,16574	0,639	0,590	-
	Associate Degree	22	3,8117	1,36269			
	Bachelor's Degree	33	3,3939	1,33680			
	Postgraduate	220	3,6416	1,13750			
Privacy	High School or Below	155	3,6636	1,21696	0,584	0,625	-
	Associate Degree	430	3,6392	1,19278			
	Bachelor's Degree	22	3,9273	1,39734			
	Postgraduate	33	3,5636	1,41638			
Availability	High School or Below	220	3,8564	1,17264	1,600	0,189	-
	Associate Degree	155	3,8181	1,27786			
	Bachelor's Degree	430	3,8237	1,24083			
	Postgraduate	22	3,2121	1,38222			

- Confidentiality & Core Controls: $\chi^2(2) = 8{,}909$, $p = 0{,}179$.
- Integrity & Proactive Controls: $\chi^2(2) = 4{,}988$, $p = 0{,}545$.
- Privacy: $\chi^2(2) = 4{,}712$, $p = 0{,}581$.
- Availability: $\chi^2(2) = 10{,}339$, $p = 0{,}111$.

These findings show that there is no statistically significant relationship between education level and any of the awareness subdimensions. Therefore, the **H8** hypothesis, "There is a significant relationship between education level and information security awareness levels", is rejected.

In the ninth and tenth hypotheses, information security awareness was examined in relation to employees' positions using ANOVA and chi-square analyses, respectively. The findings revealed that there is neither a significant difference (ANOVA) nor a significant relationship (chi-square) between position and awareness. Therefore, **H9**, "Information security awareness differs according to employees' position", and **H10**, "There is a significant relationship between employees' position and information security awareness levels", were both rejected.

Finally, in the eleventh hypothesis, the study examined whether employees' information security awareness scores differed according to tenure, and in the twelfth hypothesis, whether there was a relationship between tenure and awareness levels. Similar to the findings for **H9** and **H10**, the results showed no significant differences in mean scores by tenure and no significant relationship between tenure and awareness levels. Accordingly, **H11**, "Information security awareness differs according to tenure", and **H12**, "There is a significant relationship between tenure and employees' information security awareness levels", were rejected.

RESULTS AND DISCUSSION

This study aimed to measure the information security awareness and awareness levels of public and private sector employees, and to examine whether this awareness is associated with various sociodemographic and organizational variables. The analysis of data collected using a valid and reliable scale developed in the literature yielded significant findings that contribute to the field of information security and provide guidance for practitioners.

The most notable finding of the study is that sectoral differences emerge as the primary determinant of information security awareness, whereas demographic and certain organizational variables (such as gender, education level, position, tenure, and the presence of

antivirus software on computers) surprisingly do not exhibit statistically significant differences or relationships. Accordingly, the analysis results indicate that public sector employees demonstrate significantly higher awareness than their private sector counterparts in the dimensions of Confidentiality, Integrity, and Privacy. This can be attributed to the public sector's stricter regulatory frameworks [15], higher levels of institutional formalization [16], and structural characteristics that prioritize data integrity [17, 18]. However, the observed weak-to-moderate strength of these relationships suggests that other factors beyond these variables may also play a role in shaping information security awareness.

On the other hand, one of the most striking findings of this study is that traditionally considered important socio-demographic variables – such as gender, education level, job position, and tenure – do not have a significant impact on information security awareness. This suggests that information security awareness may be more closely related to a cultural adoption within the organization rather than an individual's formal education or hierarchical status. In other words, being a university graduate or holding a managerial position does not automatically translate into higher security awareness; rather, it points to the importance of cultivating an organization-wide culture of security.

Besides these points, the study's findings indicate that different dimensions of information security may have distinct dynamics rather than being entirely uniform. For instance, the Availability dimension appears to represent a common baseline expectation for all employees, regardless of sector [19], and shows a significant association only with technical factors such as the presence of antivirus software. This finding highlights the necessity for organizations to adopt targeted approaches that address each dimension of security – Confidentiality, Integrity, and Availability – individually when developing their security strategies.

The findings and results of this study both align with the existing literature and offer a fresh perspective. In this context, the significant differences favoring the public sector support prior studies such as [15] and [16]. At the same time, they present an interesting contrast to Ifinedo [20], who argued that the intention to comply may be higher in the private sector. This highlights the critical distinction between "awareness" and "behavioral intention", demonstrating that high awareness does not necessarily translate into high compliance.

The lack of significance for demographic variables supports the argument highlighted by [21] that "general education" and "job-specific security training" are conceptually distinct. Moreover, it aligns with [22], who emphasized that "cybersecurity is everyone's responsibility" and suggested that organizational culture can overshadow hierarchical differences such as position or tenure. This study can be interpreted as indicating that such a culture, at least partially, exists within the organizations included in the examined sample.

This research clearly demonstrates that information security awareness is not a monolithic construct; rather, it is a multifaceted phenomenon influenced by structural, sectoral, and dimensional factors. Effective information security governance, therefore, does not rely solely on employees' demographic characteristics. Instead, it requires cultivating an integrated security culture that permeates the entire organization, is continuously nurtured, and encompasses all dimensions of security.

Based on all these findings and results, various recommendations can be made. First, inclusive and continuous information security training should be designed to cover all employees of the institution, not only those at certain educational levels or positions, and should be updated at regular intervals. Second, security should not be seen solely as the responsibility of the IT department; on the contrary, it should be adopted as a fundamental element of business processes for all employees. In achieving this, senior management should play an active role in developing and embedding this organizational culture. Third, information security

awareness programs should be enriched with content and approaches tailored to each dimension, considering that aspects such as confidentiality, integrity, and availability cannot be perceived similarly. Finally, private sector organizations can strengthen their internal audits and policy formalization by drawing inspiration from regulatory and structural practices in the public sector to further enhance their employees' awareness of confidentiality and integrity. In future similar studies, qualitative research is recommended to investigate in greater depth the reasons behind the differences in awareness levels between sectors. Additionally, while this study measured awareness levels, other studies could examine the extent to which this awareness translates into behavioral compliance. Beyond these, the finding that demographic variables were ineffective suggests that future research should also consider psychosocial and organizational variables such as senior management support, self-efficacy, motivation, and organizational culture. Finally, a similar study conducted in a different country could highlight the role of cultural differences in information security awareness.

REFERENCES

[1] Bayrakcı, E. and Koçman, M.A.: *Bilgi güvenliği ve elektronik harp.*
Necmettin Erbakan Üniversitesi Siyasal Bilgiler Fakültesi Dergisi **5**(1), 184-206, 2023,

[2] Çakır, H. and Yaşar, H.: *Kurumsal siber güvenliğe yönelik tehditler ve önlemleri.*
Düzce Üniversitesi Bilim ve Teknoloji Dergisi **3**(2), 488-507, 2015,

[3] Ertekin, İ.: *Kamu yönetimi ve halkla ilişkiler yönüyle kişisel verilerin korunması kanunu (KVKK).*
Ombudsman Akademik **8**(16), 39-67, 2022,

[4] Yıldırım, A.: *Türkiye'nin siber güvenlik politikasının eylem planları üzerinden analizi.*
Organizasyon ve Yönetim Bilimleri Dergisi **16**(1), 23-47, 2024,

[5] Eş, A. and Serdar, N.: *Siber saldırılara karşı KOBİ'lerin farkındalık düzeylerinin incelenmesi: Ankara ili örneği.*
Düzce Üniversitesi Sosyal Bilimler Dergisi **11**(1), 133-151, 2021,

[6] Özbilger, H.İ.; Sarıyar, B. and Ertürk, A.: *Bilgi ve iletişim güvenliği rehberinin uygulanması ve denetimlerine yönelik iyileştirme önerileri.*
Bilgi Teknolojileri ve İletişim Dergisi **1**(1), 1-41, 2023,

[7] Selimoğlu, S.; Altunel, M.: *Siber güvenlik risklerinden korunmada köprü ve katalizör olarak iç denetim.*
Denetişim **9**(19), 5-16, 2019,

[8] Dayıoğlu, E.: *Kamu idarelerinde bilgi sistemi güvenlik risklerinin yönetimi.*
Denetişim **4**, 71-81, 2016,

[9] Arslanhan, M.: *Bankaların bilgi güvenliği yönetimi kapsamında banka müşterilerinin kişisel verilerinin korunması.*
Kişisel Verileri Koruma Dergisi **6**(2), 33-53, 2024,

[10] Kuntoğlu, Ö.F.: *Elektronik ticarette kişisel verilerin korunması.*
Bilişim Hukuku Dergisi **3**(1), 176-229, 2021,

[11] Altuntaş, E.; Kara, E.; Soylu, A.B. and Kırkbeşoğlu, E.: *Siber sigortalar: Son gelişmeler, uygulamalar ve sorunlar.*
Bankacılık ve Sigortacılık Araştırmaları Dergisi **12**, 8-22, 2018,

[12] Erkal, A.: *Avrupa genel veri koruma düzenlemesi bağlamında memurların kişisel verilerinin korunması hakkı.*
Anayasa Yargısı **37**(2), 205-253, 2020,

[13] Çatuk, C. and Yurtsever, G.: *A scale development about information security awareness of SMEs against cyber risks: Sample of Gaziantep.*
Atlas Journal **4**(14), 1522-1543, 2018,
http://dx.doi.org/10.31568/atlas.206,

[14] Büyüköztürk, Ş.; Akgün, Ö.E.; Demirel, F.; Karadeniz, Ş. and Çakmak, E.K.: *Bilimsel araştırma yöntemleri.*
Pegem Akademi, 2015,

[15] Alshare, K.A.; Lane, P.L. and Lane, M.R.: *Information security policy compliance: A cross-country comparison.*
Information & Computer Security **26**(1), 91-108, 2018,
http://dx.doi.org/10.1108/ICS-09-2016-0073,

[16] D'Arcy, J.; Gupta, A.; Tarafdar, M. and Turel, O.: *Reflecting on the "dark side" of information technology use.*
Communications of the Association for Information Systems **35**(1), 109-118, 2014,
http://dx.doi.org/10.17705/1CAIS.03505,

[17] Vance, A.; Siponen, M. and Pahnila, S.: *Motivating IS security compliance: Insights from Habit and Protection Motivation Theory.*
Information & Management **49**(3-4), 190-198, 2012,
http://dx.doi.org/10.1016/j.im.2012.04.002,

[18] Whitman, M.E. and Mattord, H.J.: *Principles of information security.*
Cengage Learning, 2019,

[19] Cenfetelli, R.T. and Schwarz, A.: *Identifying and testing the inhibitors of technology usage intentions.*
Information Systems Research **22**(4), 808-823, 2011,
http://dx.doi.org/10.1287/isre.1100.0295,

[20] Ifinedo, P.: *Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition.*
Information & Management **51**(1), 69-79, 2014,
http://dx.doi.org/10.1016/j.im.2013.10.001,

[21] Puhakainen, P. and Siponen, M.: *Improving employees' compliance through information systems security training: An action research study.*
MIS Quarterly **34**(4), 757-778, 2010,
http://dx.doi.org/10.2307/25750704,

[22] Boss, S.R.; Kirsch, L.J.; Angermeier, I.; Shingler, R.A. and Boss, R.W.: *If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security.*
European Journal of Information Systems **18**(2), 151-164, 2009,
http://dx.doi.org/10.1057/ejis.2009.8.