Scientific Research Publishing

Intelligent Information Management, 2023, 15, 259-283
https://www.scirp.org/journal/iim
ISSN Online: 2160-5920
ISSN Print: 2160-5912

Factors Influencing Employees on Compliance with Cybersecurity Policies and Their Implications for Protection of Information and Technology Assets in Saudi Arabia

Sami Saad Alsemairi

Department of Digital Transformation and Information Programs, Institute of Public Administration, Jeddah, Saudi Arabia
Email: semairis@ipa.edu.sa

How to cite this paper: Alsemairi, S.S. (2023) Factors Influencing Employees on Compliance with Cybersecurity Policies and Their Implications for Protection of Information and Technology Assets in Saudi Arabia. *Intelligent Information Management*, **15**, 259-283.
https://doi.org/10.4236/iim.2023.154013

Received: June 1, 2023
Accepted: July 17, 2023
Published: July 20, 2023

Abstract

In the current digital era, it is difficult to preserve the confidentiality, integrity, and availability of an organization's information and technology assets against cyber attacks. Organizations cannot rely solely on technical solutions for defense, since many cyber attacks attempt to exploit non-technical vulnerabilities such as how well employees comply with the organization's cybersecurity policies. This study surveyed 245 randomly selected employees of government organizations in the Kingdom of Saudi Arabia with an electronically distributed questionnaire about factors that influence employees' compliance with cybersecurity policies. The study found that ethical factors had the most influence on employee compliance with cybersecurity policies, followed in decreasing order of influence by legislative factors, technical factors, and administrative factors.

Keywords

Cybersecurity Policies, Compliance, Protection, Information and Technology Assets

1. Introduction

Rapid global developments have posed a great challenge in the field of information and communication technology: reliance on digital technologies has become an indicator of development. This rapid digital renaissance has been accompanied by a global trend toward harnessing the benefits arising from the use of information and communication technologies to stimulate economic growth, increase productivity, improve services and capabilities, and provide access to businesses and information [1].

In the same context, with the increasing reliance of societies on digital technologies, technologies are still vulnerable; the confidentiality, integrity, and availability (CIA) of information and the infrastructure of communications technology are exposed to cyber attacks including disabling services and destroying information and technology assets, whether inside or outside the Kingdom of Saudi Arabia. As a guiding concept, CIA can be used to define an organization's cybersecurity policies [2].

Organizations around the world rely heavily on digital technology to execute government services and activities more efficiently [3]. The increased use of digital technology has led to the emergence of cybercrimes that pose a threat to information and technology assets. Among all Middle Eastern countries, Saudi Arabia is the most frequently targeted by cyber attacks. With the intention of causing economic instability, an estimated 60 million attacks are launched each day against organizations [4].

In order to fully benefit from the potential of technology, the Kingdom of Saudi Arabia has had to align its National Economic Vision 2030 with its national security priorities. A royal order was issued in 2017 to establish the National Cybersecurity Authority, which is the Kingdom's cybersecurity competent authority [5]. The National Cybersecurity Authority has developed cybersecurity policies and obligated government organizations to adhere to these policies in order to protect the information and communications technology infrastructure, services, and government activities [6].

Many organizations are aware that using technology alone to address the security issue is rarely enough [7]. To protect information and technology assets, technical solutions and non technical solutions are needed. Examples of technical solutions are anti-virus software, a firewall, and data backup. Examples of non-technical solutions are standards of employee behavior and organization procedures [8]. Triplett [9] found that the most vulnerable point in information technology security is the human factor, which is the most significant threat to security by 86%.

The purpose of the study is to determine and highlight some of the factors that influence the compliance of employees in government organizations to the cybersecurity policies issued by the National Authority for Cybersecurity in the Kingdom of Saudi Arabia, which may contribute and help decision makers in government organizations to enhance the strengths and improve the weaknesses of these factors in order to raise the level of protection of information and technology assets.

The remainder of the study is organized as follows: Section 2 has a review of the literature in the area of the study. Section 3 presents the study problem and the research questions. Section 4 lists the study's objectives and the importance of the study. Section 5 presents the study model and the hypotheses. Section 6 provides the theoretical background. Section 7 describes the study's methodology. Section 8 has the results. Section 9 has the study's conclusion. Final section presents limitations and future work.

2. Literature Review

Threats and risks related to cybersecurity have increased significantly, burdening countries severely. Particularly exposed are organizations, whose cybersecurity vulnerabilities are attracting increased attention. The reasons for an organization's security vulnerabilities are numerous. Employees, not systems, are the main targets of cyber attacks. In actuality, human failures are to blame for the majority of attacks. Most research in cybersecurity has mainly focused on employees' behaviors toward information security where "employees" are the least effective linkage in the protection of organization's assets against cybersecurity threats [10]. Therefore, cybersecurity policies for employees should be considered when thinking about an organization's cybersecurity [11]. Organizations fail to prevent security breaches due to employees not complying with cybersecurity policies [12].

The report [13] indicated that 92% of the respondents stated that the number of attacks they faced increased from last year. Specifically, 84% of respondents also stated that cyber attacks have increased along with the increase in the number of employees working remotely. To deal with the risks of cyber threats, organizations have implemented a variety of security technologies, such as intrusion detection systems, networking security protocols, and database security protection, to safeguard their information and technology assets against cyber attacks [11], cyber breaches continue to be a problem for a number of organizations due to a lack of focus on employees [14].

Many researchers have studied the factors that influence compliance with cybersecurity policies. AlGhamdi *et al.* [15] showed that understanding employee intentions toward compliance with information security is an important step in determining the factors that shape employees' intentions toward compliance. The results of the study identified several of these factors; one factor was related to the social or organizational environment. Another factor was related to the administration's approach to dealing with an awareness program for information security without regard to the size of the organization and the local culture of the employees. Another factor emerged from the results of the study: the lack of a strategy for information security that would provide strong protection for the organization.

Alanazi *et al.* [16] sought to determine the applicability of a theory based model and to pinpoint indications of Information Security Compliance Behavior (ISCB) among 433 health workers in public hospitals in the city of Arar in the Kingdom of Saudi Arabia. This study had two parts: formulation of a hypothetical model, and the identification of ISCB predictors. According to the findings, ISCB is not affected by demographic factors such as age, marital status, and work history, but it is affected by moderate and non-common elements such as religion and morality.

According to Koohang *et al.* [17], the leaders in organizations are responsible for developing an information security culture to enhance compliance with the information security policy (ISP) and to protect information and technology assets from cyber threats. It is also the responsibility of leaders to motivate their employees to follow this policy. When this study looked at the leadership influence among 237 university employees, the study discovered a clear positive correlation between leadership and ISP compliance.

The study Addae *et al.* [18] examined factors influencing information security compliance behavior in the Ghanaian banking sector. Some of the study's suggestions are that managers should remind employees that serious sanctions will be applied for noncompliance.

As for the ethics as part of the culture of countries, Connolly *et al.* [19] addressed the fact that behaviors differ according to the culture of countries, where culture affects information security behavior (ISB) in compliance with information security policies (ISP).

Five factors identified by Alqahtani and Braun [20] as influencing user behavior with regard to cybersecurity compliance. These factors include end user awareness, technical controls and measures, accountability, monitoring and control, and organizational commitment. The findings showed that technical security measures are promoting cyber security compliance by assisting users in adhering to organizational security policies.

3. Study Problem and Questions

Due to the significance of asset security, government organizations in the Kingdom of Saudi Arabia must implement appropriate procedures to protect information and technology assets from cybercrimes. Among these procedures are "cybersecurity policies," which must be defined by the cybersecurity department of the government organization. They must be documented and approved by the organization's authority holder before they can be published to the government's employees [5]. It must be noted that cybersecurity involves both people and technology, since the human factor plays a role in protecting information and technology assets against cyber attacks. Hence, cybersecurity requires that the people involved be sufficiently knowledgeable about cybersecurity to understand and comply with cybersecurity policies and procedures. Hence, the study problem can be formulated in the following questions:

Question Q1: Is there an impact of factors (administrative, legislative, technical, and ethical) on employees' compliance with cybersecurity policies?

Question Q2: Is there an impact of factors (administrative, legislative, technical, and ethical) on the protection of information and technology assets through employees' compliance with cybersecurity policies as an intermediate variable?

Question Q3: Is there an impact of government employees' compliance with cybersecurity policies on the protection of information and technology assets?

4. Study Objectives and Importance

This study seeks to determine the impact of factors (administrative, legislative, technical, and ethical) on employees' compliance with cybersecurity policies and the implications for the protection of information and technology assets. These are the study's objectives:

- Determine the most important factors influencing compliance with cybersecurity policies from the viewpoint of government employees in the Kingdom of Saudi Arabia.
- Determine the impact of government employee compliance with cybersecurity policies on the protection of information and technology assets.

Government organizations in the Kingdom of Saudi Arabia have recently witnessed significant changes in terms of increasing the role of digital technology in support of the main administrative units, providing electronic services, integrating with government organizations and other institutions, and other relevant aspects. All of this has led to a significant increase in the importance of cybersecurity for government organizations. The importance lies in developing cybersecurity policies and procedures, in line with the cybersecurity risks faced by those government organizations.

Cybersecurity policies and procedures provide a framework of best practices that can be followed by all employees. The policies and procedures help to ensure that risks are reduced to a minimum, and that any security incidents are responded to effectively. The policies and procedures will also help engage employees in the efforts of the concerned government organization to protect their information and technology assets. Keeping employees compliant with cybersecurity policies and procedures is very beneficial as it allows all employees to participate in maintaining the organization's cybersecurity. Moreover, it also minimizes the risk of potential security breaches that may arise due to the errors that are caused by the human factor, as this relates to a variety of problems such as employees revealing information to unknown (or unauthorized) sources, unsafe or improper use of the Internet, and many other dangerous activities.

5. Study Model and Hypotheses

5.1. Study Model

The study model shows the relationship that is hypothesized to exist between the independent variable with all its factors (administrative, legislative, technical, and ethical), the intermediate variable, and the dependent variable, leading to the identification of the presumed results between the aforementioned variables as results through which it is possible to infer the nature of the existing relationships. **Figure 1** shows the proposed model for the study.

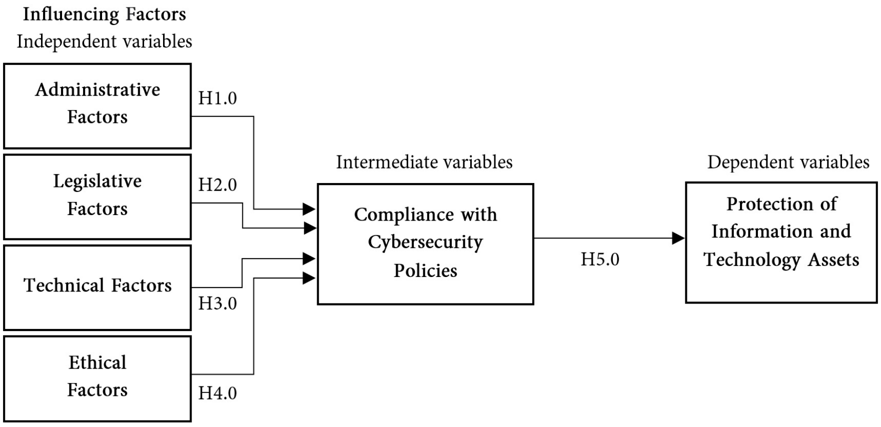

Figure 1. Study model.

5.2. Hypotheses

The study adopted a set of hypotheses in order to analyze and test the potential effect between the independent variables and their factors on the one hand, and the intermediate variable on the other hand, as well as between the intermediate variable and the dependent variable. The study adopted the null hypothesis method in the formulation; in the event of rejection of the null hypothesis, the alternative hypothesis is accepted.

5.2.1. Administrative Factors

Hypothesis (H1): There is no statistically significant effect of administrative factors on employees' compliance with cybersecurity policies at the level of significance ($\alpha \leq 0.05$).

5.2.2. Legislative Factors

Hypothesis (H2): There is no statistically significant effect of legislative factors on employees' compliance with cybersecurity policies at the level of significance ($\alpha \leq 0.05$).

5.2.3. Technical Factors

Hypothesis (H3): There is no statistically significant effect of technical factors on employees' compliance with cybersecurity policies at the level of significance ($\alpha \leq 0.05$).

5.2.4. Ethical Factors

Hypothesis (H4): There is no statistically significant effect of ethical factors on employees' compliance with cybersecurity policies at the level of significance ($\alpha \leq 0.05$).

5.2.5. Compliance with Cybersecurity Policies

Hypothesis (H5): There is no statistically significant effect of employees' compliance with cybersecurity policies on the protection of information and technology assets at the level of significance ($\alpha \leq 0.05$).

6. Theoretical Background

6.1. Cybersecurity

Cybersecurity is a relatively recent concept that has been developed in the context of the digital revolution and contemporary technology, which has caused the increased collection and transmission of information and data using many means of communication through different digital devices. Cybersecurity is concerned with the security aspect, to protect the transmission of information and data between different digital devices. Cybersecurity is defined by the International Telecommunication Union (ITU) this way: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" [21]. When protecting those assets, three primary goals of cybersecurity need to be considered: confidentiality, integrity, and availability (CIA). Accordingly, cybersecurity has become one of the most important pillars in the field of information and communication technologies for government organizations. It is the combination of people, processes, and technologies that come together to protect organizations' assets from cyber attacks. The human element is an important factor in the protection system [22]. This indicates the importance of complying with cybersecurity policies to reduce cyber threats.

6.2. Cybersecurity Policies

In the current era, digital technologies are the main driver of all organizations. These technologies have become more complex with the advancement of technology. Each organization needs to prepare cybersecurity policies, address the technology aspects, stay updated on the latest security threats, and educate employees about them; all this is done within the framework of support for the country's cybersecurity policy, in addition to the organization's commitment to follow up implementation. Many global organizations have addressed cyber threats by incorporating cybersecurity policies through well-defined strategies so that the policies are used in a way that ensures the protection of digital technologies. The Kingdom of Saudi Arabia has taken care to include cybersecurity policies in each government organization within the Kingdom and to stress the importance of enacting laws and legislation to support those policies and secure the Kingdom's digital infrastructure. Each government organization's cybersecurity department is entrusted with defining cybersecurity standards and then documenting and publishing its policies in a way that ensures the organization's compliance with them [5].

6.3. Administrative Factors

A royal decree (number 37140) was issued on 12 January 2017 providing for the establishment of an independent department concerned with cybersecurity in government organizations in the Kingdom of Saudi Arabia [5]. The department adopts regulations to strengthen cybersecurity, protect information and technology assets, and manage the risks of potential cybercrime, in order to ensure business continuity. The administrative measures available to prevent cyber attacks include these measures:

- Preparing and publishing cybersecurity policies: the cybersecurity administration must provide cybersecurity policies based on best practices and standards related to cybersecurity, to reduce the risks of cyber attacks and protect information and technology assets from internal and external threats. This is done by focusing on the basic objectives of the protection of information: confidentiality, integrity, and availability (CIA).
- Cybersecurity awareness and training: the cybersecurity administration is required to ensure that employees have the necessary awareness of their cybersecurity responsibilities and that employees are provided with the skills and training courses required to protect information and technology assets.

6.4. Legislative Factors

Reliance on computer devices and systems is increasing in all governmental organizations, and thus the need for legislative regulation for the use of these systems has increased, especially after governmental organizations kept pace with the development and began using the World Wide Web for electronic services. Therefore, the legislators in the Kingdom of Saudi Arabia found that the availability of laws regulating the issue of cybersecurity is a necessity from a legal point of view. For example, the Kingdom of Saudi Arabia issued an Anti-Cyber Crime Law [23]. Thus, cyber legislation is considered an essential component of the regulatory and legal environment necessary for the informational and technical development of organizations. It is also an important element for providing security and confidence to users of cyberspace.

6.5. Technical Factors

All organizations, whether inside or outside the Kingdom of Saudi Arabia, are currently using technologies and tools in order to protect information and technology assets, since cyber attacks of these assets have become commonplace, and therefore their protection has become very important. When employees use office Internet, the chances of their office computers being infected increase. The following are the most important technologies and tools for protecting information and technology assets:

- Installing an appropriate anti-virus program: this program is one of the most important defenses needed to protect office computers from viruses, including worms and Trojan horses. Cybersecurity managers are advised to install an appropriate anti-virus program on the computer.
- Installing firewall software: the aim of a firewall program is to protect computers from intrusions and attacks by hackers. A firewall controls data traffic

across the network, examining the data packets that pass through the network and choosing whether to allow these packets to pass to the computer. Without this software, hackers could more easily steal all the confidential information stored on the computer, or they could damage the computer's operating system.

- Updating operating systems: it is best to update operating systems and software programs periodically. In general, official updates include some improvements, such as enhanced security and improved performance.
- Using a complex password: in order to protect data, a long and complex password of letters, numbers, and symbols should be created, making it impossible for hackers to steal it. In addition, the password should be changed periodically.

Today, all organizations of all sizes and areas of work are responsible for the security of their data and assets. Decision makers and cybersecurity managers must apply security policies and controls that suit the organization in which they work, and managers must ensure that employees comply with cybersecurity policies and controls that aim to protect the organization's assets from cyber attacks or other security incidents.

6.6. Ethical Factors

Ethics in the work environment is a desirable behavior that employees in organizations must adopt. Work ethics are defined as rules of good behavior in the work environment. Failure to comply with these rules exposes an employee to alienation from other employees and may reach the extent of imposing penalties. In any organization, a cybersecurity defense strategy should include ethics, since employees cannot secure systems and data without clear ethical rules [24]. Therefore, understanding the role of ethical values in information technology is indispensable [25].

7. Study Methodology

The study combined two approaches: the deductive approach was used to test the validity of the study hypotheses in order to accept or reject them; the descriptive approach was used to describe the factors influencing government employees' commitment to cybersecurity policies. The methodology used in this study has two main parts: the first part was the design and publication of anelectronic questionnaire to collect the necessary data needed to evaluate the hypotheses. The questionnaire was built by reviewing the theoretical frameworks and previous Arab and foreign studies in the field of cybersecurity; the second part was the statistical analysis of the questionnaire data using several statistical methods.

7.1. Study Population and Sample

The study population consists of all government organizations in the Kingdom of Saudi Arabia, and since the study population is distributed over all regions of the Kingdom, the random method was relied upon in order to obtain the most representative sample. The author published the electronic questionnaire on a number of employees of government organizations distributed in all regions of the Kingdom, who enrolled in some training programs at the Institute of Public Administration (IPA)—IPA is an institute in the Kingdom to train employees of government organizations in various fields—during the period from 4 December 2022 to 21 February 2023; the author received 271 responses, of which 245 were complete responses and 26 were excluded for not meeting the conditions of the study. This sample size is in the range of 30 to 500 individuals that is considered appropriate for most types of research [26].

7.2. Data Collection Tool

The author relied on obtaining special data through an electronic questionnaire for the purpose of measuring the factors influencing employees in government organizations in the Kingdom. A five-weight Likert scale was used (strongly disagree, disagree, neutral, agree, and strongly agree) as shown in **Table 1**. The questionnaire consisted of three main axes. The first axis was used for measurements of the influencing factors; 12 items were chosen and divided into these 4 groups in order to measure the independent variables: administrative factors, legislative factors, technical factors, and ethical factors. The second axis was used for measurements of the compliance with cybersecurity policies; 3 items were chosen to measure the intermediate variable. The third axis was used for measurements of the protection of information and technology assets; 3 items were chosen to measure the dependent variable.

7.3. Data Analysis Methods

In analyzing the level and results of the research, the author relied on a set of statistical methods that fit the nature of the research questions and hypotheses. These were the methods used:

1) Frequencies and percentages were used to determine the measurement indicators adopted in the study and to analyze the characteristics of the study sample.

Table 1. Five-weight likert scale.

Likert Description	Value
Strongly Disagree	1
Disagree	2
Neutral	3
Agree	4
Strongly Agree	5

2) Arithmetic means were used to determine the relative importance of the study sample's responses toward the dimensions of the study.

3) The standard deviation was used to identify the deviation from the arithmetic mean of the responses of the study sample for each of the study variables and for each of the main axes.

4) The category length equation, which was required to measure the importance level of the study variables, was calculated according to the following equation [27]:

Category length = (highest value of the alternative − lowest value of alternative) divided by the number of levels:

$$\text{Category length} = \frac{(5-1)}{3} = \frac{4}{3} = 1.33$$

Thus, these were the levels of importance: low level was from 1.00 to 2.33; average level was from 2.34 to 3.66; high level was from 3.67 to 5.00.

5) Pearson correlation analysis was used to measure the strength and direction of the relationship between variables.

6) The Cronbach alpha coefficient was used to measure the stability of the study tool (the questionnaire) and the amount of its internal consistency, in addition to the degree of reliability of the answers to the questionnaire.

7) A one-tailed T-test was used to verify the significance of the items of the prepared questionnaire compared to the hypothetical mean.

8) Factor Inflation Variance (VIF) and the Tolerance Test were used to ensure that there was no multicollinearity between the independent variables.

The above mentioned statistical methods were implemented using the statistical program SPSS (v. 29) to obtain the results of the research.

8. Results

8.1. Face Validity

The main tool for this study was the questionnaire; it consists of six dimensions, and each dimension includes three statements. In order to verify the validity of the questionnaire after its initial formulation, it was presented to a group of arbitrators in the field of research and information technology at the Institute of Public Administration (IPA) in the Kingdom of Saudi Arabia. Based on their views on the questionnaire's statements and on the validity of its statements linguistically, some of the original statements were reformulated.

8.2. Construct Validity

After confirming the face validity of the questionnaire, the author calculated the Pearson correlation coefficients to determine the internal validity of the questionnaire in terms of the degree of consistency of each statement of the questionnaire with the total degree of the factor (dimension) to which the statement belongs. Since the author subjected the study tool statements to measurement, Table 2 shows the degree of each statement of the questionnaire according to its correlation coefficient with the administrative factor to which the statement belongs, as through it, the correlation coefficients between the degree of each statement of the first factor (administrative) are revealed. The correlation coefficients are positive and statistically significant at the level ($\alpha \le 0.01$), and thus the administrative factor is considered true to what was set to measure it. The correlation coefficient was calculated between each of the statements of the study tool according to the legislative factor to which the statement belongs. Table 2 shows that the correlation coefficients are positive and statistically significant at the level of ($\alpha \le 0.01$), and thus the legislative factor is considered valid for what was set to measure it. For each statement of the technical factor, Table 2 indicates that the correlation coefficients are positive and statistically significant at the level of ($\alpha \le 0.01$). Thus, the technical factor is considered true to what was set to measure it. For each statement of the ethical factor, Table 2 shows that the correlation coefficients are positive and statistically significant at the level ($\alpha \le 0.01$), and thus the ethical factor is considered true to what was set to measure it. Table 2 shows the degree of each statement of the commitment dimension and the total score of the dimension; the correlation coefficients are positive and statistically significant at the level of ($\alpha \le 0.01$), and thus the commitment dimension is considered true to what was set to measure it. Table 2 also shows the degree of

Table 2. Pearson correlation coefficients.

#	Legislative Factors	Pearson correlation coefficient
1	The government organization to which I belong prevents unauthorized employees from accessing information and technology assets (for example: data)	0.782**
2	The government organization I belong to has cybersecurity policies in place (for example: internet acceptable use policy)	0.788**
3	The government organization to which I belong has strict procedures for violating cybersecurity policies	0.816**
#	**Administrative Factors**	**Pearson correlation coefficient**
1	In the government organization to which I belong, there is a department/section for cybersecurity	0.847**
2	The government organization to which I belong implements awareness programs on the importance f adhering to cybersecurity policies to increase awareness of cyber risks	0.862**
3	Cybersecurity policies can be viewed in the government organization to which I belong when needed	0.851**

Continued

#	Technical Factors	Pearson correlation coefficient
1	A message appears periodically (for example: every 90 or 180 days) on my desktop of the government organization I belong to requiring me to change my password	0.813**
2	The government organization I belong to adopts security technologies and tools (for example: anti-virus software)	0.867**
3	The operating system on my office computer of the government organization to which I belong is automatically updated	0.814**
#	**Ethical Factors**	**Pearson correlation coefficient**
1	Violating our cybersecurity policies is against my ethical and religious principles	0.822**
2	My co-workers and I classify employees who violate cybersecurity policies as unethical	0.876**
3	Good employee ethical (For example: honesty) contribute to compliance with cybersecurity policies	0.743**
#	**Commitment Dimension**	**Pearson correlation coefficient**
1	I do not install software on my desktop computer of the government organization to which I belong without prior authorization	0.724**
2	I do not open suspicious emails from my office computer	0.765**
3	I do not enable the password saving feature in the web browser	0.781**
#	**Protection Dimension**	**Pearson correlation coefficient**
1	The electronic systems of the government organization to which I belong have never been disrupted due to a cybercrime	0.789**
2	The wired or wireless communication network is available in the government organization to which I belong almost always	0.791**
3	Confidential documents and information related to the government organization to which I belong have never been published on the Internet or through social networking applications	0.708**

**There is statistical significance at the significance level ($\alpha \leq 0.01$).

each statement of the protection dimension and the total score of the dimension; the correlation coefficients are positive and statistically significant at the level ($\alpha \leq 0.01$), and thus the protection dimension is considered true to what was set to measure it. To stand on the values of the correlation coefficients for the factors and dimensions of the questionnaire with the total score of the resolution, Table 3 shows that they ranged between (0.577) and (0.783) and are statistically significant at the level of ($\alpha \leq 0.01$), which means that there is a high degree of validity resolution.

8.3. Reliability

The questionnaire's reliability indicates if it would give the same result when distributed to the study sample more than once in certain time periods. To measure the reliability of the study tool, the reliability coefficient was calculated using Cronbach's alpha coefficient. The values of the stability coefficient for the study factors ranged between (0.610) and (0.813), and the value of Cronbach's alpha coefficient for all factors and dimensions was (0.882), as shown in Table 4. The value of Cronbach's alpha coefficient for the factors and dimensions was greater than (0.60), which is the minimum recommended by statisticians [28] to show from the foregoing the validity and reliability of the study tool.

Table 3. Values of the correlation coefficients for the factors and dimensions.

#	Factors and Dimensions	Pearson correlation coefficient
1	Administrative factors	0.767**
2	Legislative factors	0.733**
3	Technical factors	0.783**
4	Ethical factors	0.577**
5	Commitment dimension	0.754**
6	Protection dimension	0.696**

**There is statistical significance at the significance level ($\alpha \leq 0.01$).

Table 4. Cronbach's alpha coefficient.

#	Factors and Dimensions	Statements	Cronbach's alpha coefficient
1	Administrative factors	3	0.813
2	Legislative factors	3	0.708
3	Technical factors	3	0.770
4	Ethical factors	3	0.740
5	Commitment dimension	3	0.610
6	Protection dimension	3	0.641
	Total	**18**	**0.882**

8.4. Statistical Analysis

In this study, the author distributed the questionnaire electronically to the study sample. The author received 271 forms in response, of which 245 completed the conditions; the rest of the forms were excluded as a result of not meeting the requirements of the study, as shown in Table 5. This study was conducted on employees of government organizations; their educational backgrounds are shown by Table 6. The most frequent background was a bachelor's degree; 71.84% of the study sample held a bachelor's degree in their specialization. The second most frequent background was a secondary school certificate at a frequency of (17.14%), followed by a master's degree at (8.98%) and a doctorate degree at (2.04%). There was a diversity in the years of experience for the employees of the study sample. Table 7 shows that 38.37% had more than 15 years of experience in the functional field, followed by 33.06% with 11 to 15 years' experience, 23.27% with 6 to 10 years, and 5.31% with 1 to 5 years.

Table 5. Completed and incomplete questionnaires.

Questionnaire	Frequency	Percentage
A completed questionnaire	245	90.41
Incomplete questionnaire	26	9.59
Total	**271**	**100**

Table 6. Distribution of the study sample according to educational qualification.

Qualification	Frequency	Percentage
Secondary	42	17.14
Bachelor	176	71.84
Master	22	8.98
Ph.D	5	2.04
Total	**245**	**100**

Table 7. Distribution of the study sample according to years of experience.

Years of Experience	Frequency	Percentage
1 to 5 years	13	5.31
6 to 10 years	57	23.27
11 to 15 years	81	33.06
More than 15 years	94	38.37
Total	**245**	**100**

8.5. Analysis of the Questionnaire Data

8.5.1. Administrative Factors

Table 8 shows that the administrative factors came with a high degree of agreement: an arithmetic mean of 4.05, a standard deviation of 1.06, and an approval rate of 80.93%. The highest rate of 83.02% came for the statement: "In the government organization to which I belong, there is a department/section for cybersecurity." The author attributes this to royal decree No. 37140 dated 12 January 2017, establishing a department concerned with cybersecurity in every government organization. The lowest percentage was 77.39% for the statement: "Cybersecurity policies can be viewed in the government organization to which I belong when needed." The author attributes this to the recent application of cybersecurity policies in government organizations.

8.5.2. Legislative Factors

Through the study sample, Table 9 shows that the legislative factors came with a high degree of approval: an arithmetic mean of 4.19, a standard deviation of 0.94, and an approval rate of 83.73%. The highest rate of 85.71% came for the statement: "The government organization to which I belong prevents unauthorized employees from accessing information and technology assets (for example: data)." The author attributes this to the distribution of powers in the government organization based on the roles and tasks of the employees. The lowest percentage was 82.37% for the statement: "The government organization to which I belong has strict procedures for violating cybersecurity policies." The author describes that perhaps the recent application of cybersecurity policies, and therefore their violation is not a phenomenon that deserves strict procedure towards employees.

Table 8. Arithmetic means, standard deviations, and the level of importance of administrative factors.

#	Administrative Factors	Arithmetic Mean	Standard Deviation	Percentage	Degree of Approval	Statement order
1	In the government organization to which I belong, there is a department/section for cybersecurity	4.15	1.08	83.02	High	1
2	The government organization to which I belong implements awareness programs on the importance of adhering to cybersecurity policies to increase awareness of cyber risks	4.12	1.03	82.37	High	2
3	Cybersecurity policies can be viewed in the government organization to which I belong when needed	3.87	1.08	77.39	High	3
	Total	**4.05**	**1.06**	**80.93**	**High**	

Table 9. Arithmetic means, standard deviations, and the level of importance of legislative factors.

#	Legislative Factors	Arithmetic Mean	Standard Deviation	Percentage	Degree of Approval	Statement order
1	The government organization to which I belong prevents unauthorized employees from accessing information and technology assets (for example: data)	4.29	0.98	85.71	High	1
2	The government organization I belong to has cybersecurity policies in place (for example: internet acceptable use policy)	4.16	0.90	83.10	High	2
3	The government organization to which I belong has strict procedures for violating cybersecurity policies	4.12	0.94	82.37	High	3
	Total	**4.19**	**0.94**	**83.73**	**High**	

8.5.3. Technical Factors

Table 10 shows that the technical factors came with a high degree of agreement: an arithmetic mean of 4.12, a standard deviation of 1.13, and an approval rate of 82.40%. The highest rate of 84.57% came for the statement: "The government organization I belong to adopts security technologies and tools (for example: anti-virus software)." The author attributes this to the first roles that cybersecurity departments play in protection from cyber risks. The lowest percentage of 80.82% came for the statement: "The operating system on my office computer of the government organization to which I belong is automatically updated." The author attributes this to the possibility that non-specialists in information technology may not be aware of this procedure, which usually happens in the background.

8.5.4. Ethical Factors

Table 11 shows that the ethical factors have a high degree of approval: an arithmetic mean of 4.44, a standard deviation of 0.83, and an approval rate of 88.85%. The highest rate of 91.76% came for the statement: "Good employee ethical (For example: honesty) contribute to compliance with cybersecurity policies." The author attributes this to the fact that the job is a trust and assignment in the Islamic religion, as the employee is keen to perform his work with all sincerity and discipline. The lowest rate was 85.31% for the statement: "I and my co-workers classify employees who violate cybersecurity policies as unethical." The author attributes this to the fact that an employee who violates the security policies has undesirable characteristics, and a violation of the policies may cause serious consequences for the organization.

8.5.5. Commitment Dimension

Table 12 shows that the commitment dimension received a high degree of approval: an arithmetic mean of 4.25, a standard deviation of 0.97, and an approval

Table 10. Arithmetic means, standard deviations, and the level of importance of technical factors.

#	Technical Factors	Arithmetic Mean	Standard Deviation	Percentage	Degree of Approval	Statement order
1	A message appears periodically (for example: every 90 or 180 days) on my desktop of the government organization I belong to requiring me to change my password	4.09	1.20	81.80	High	2
2	The government organization I belong to adopts security technologies and tools (for example: anti-virus software)	4.23	1.03	84.57	High	1
3	The operating system on my office computer of the government organization to which I belong is automatically updated	4.04	1.16	80.82	High	3
	Total	**4.12**	**1.13**	**82.40**	**High**	

Table 11. Arithmetic means, standard deviations, and the level of importance of ethical factors.

#	Ethical Factors	Arithmetic Mean	Standard Deviation	Percentage	Degree of Approval	Statement order
1	Violating our cybersecurity policies is against my ethical and religious principles	4.47	0.82	89.47	High	2
2	My co-workers and I classify employees who violate cybersecurity policies as unethical	4.27	1.02	85.31	High	3
3	Good employee ethical (For example: honesty) contribute to compliance with cybersecurity policies	4.59	0.66	91.76	High	1
	Total	**4.44**	**0.83**	**88.85**	**High**	

Table 12. Arithmetic means, standard deviations, and the level of importance of commitment dimensions.

#	Commitment dimensions	Arithmetic Mean	Standard Deviation	Percentage	Degree of Approval	Statement order
1	I do not install software on my desktop computer of the government organization to which I belong without prior authorization	4.34	0.92	86.86	High	2
2	I do not open suspicious emails from my office computer	4.46	0.82	89.22	High	1
3	I do not enable the password saving feature in the web browser	3.94	1.18	78.86	High	3
	Total	**4.25**	**0.97**	**84.98**	**High**	

rate of 84.98%. The highest rate of 89.22% came for the statement: "I do not open suspicious emails from my office computer." The author attributes this to possibly using the spam filter as a security measure against the cyber threat. The lowest percentage was 78.86% for the statement: "I do not enable the password saving feature in the web browser." The author attributes this to the employees' lack of awareness of the danger of activating the password's preservation due to the possibility of revealing it when the security procedures of the office computer are weak.

8.5.6. Protection Dimension

Table 13 shows that the protection dimension has a high degree of approval: an arithmetic mean of 4.11, a standard deviation of 1.01, and an approval rate of 82.26%. The highest percentage of 88.08% was for the statement: "Confidential documents and information related to the government organization to which I belong have never been published on the Internet or through social networking applications." The author attributes this to the existence of the Anti-Cyber Crime Law in the Kingdom of Saudi Arabia. The lowest percentage was 76.49% for the statement: "The electronic systems of the government organization to which I belong have never been disrupted due to a cybercrime." The author attributes this to the fact that some government organizations within the Kingdom of Saudi Arabia may have been subjected to cyber attacks that affected electronic systems.

Table 14 shows that among the study's factors and dimensions, the ethical factor comes out on top, followed by the commitment dimension. The legislative factor ranks third. The technical factor comes in fourth rank. The protection dimension appears before the last one. The administrative factor comes in sixth and last rank.

Table 13. Arithmetic means, standard deviations, and the level of importance of protection dimensions.

#	Protection dimensions	Arithmetic Mean	Standard Deviation	Percentage	Degree of Approval	Statement order
1	The electronic systems of the government organization to which I belong have never been disrupted due to a cybercrime	3.82	1.12	76.49	High	3
2	The wired or wireless communication network is available in the government organization to which I belong almost always	4.11	0.99	82.20	High	2
3	Confidential documents and information related to the government organization to which I belong have never been published on the Internet or through social networking applications	4.40	0.93	88.08	High	1
	Total	**4.11**	**1.01**	**82.26**	**High**	

Table 14. Arithmetic means, standard deviations, and the level of importance of all factors and dimensions.

#	Factors and Dimensions	Arithmetic Mean	Standard Deviation	Degree of Approval	Statement order
1	Administrative factors	4.05	1.06	High	6
2	Legislative factors	4.19	0.94	High	3
3	Technical factors	4.12	1.13	High	4
4	Ethical factors	4.44	0.83	High	1
5	Commitment dimension	4.25	0.97	High	2
6	Protection dimension	4.11	1.01	High	5
	Total	**4.19**	**0.99**	**High**	

8.5.7. Test for Multicollinearity

Before starting the application of regression analysis to test the hypotheses of the study, the author conducted some tests in order to ensure that the data are appropriate to the assumptions of the regression analysis. As shown in Table 15, the Variance Inflation Factor (VIF) does not exceed the value of (10), and the value of Tolerance is greater than (0.05) for each variable of the study. As shown in Table 15, there is no multicollinearity. Multicollinearity would be an indication of a high correlation between the independent variables (administrative, legislative, technical, and ethical).

8.5.8. Tests of the Study Hypotheses

Table 16 shows the analysis of the results of the independent variable (administrative factors) on the intermediate variable (commitment). The results of the statistical analysis show that there is a statistically significant effect of the administrative factors on the commitment of employees of government organizations in the Kingdom of Saudi Arabia to cybersecurity policies, since the correlation coefficient (R) was (0.416) at the level ($\alpha \leq 0.05$). The coefficient of determination R2 was (0.173), meaning that its value is (0.416) of changes in the protection of information and technology assets resulting from the change in the administrative factors ($\alpha \leq 0.05$). This confirms the invalidity of accepting hypothesis (H1). Accordingly, the null hypothesis (H1) is rejected, and the alternative hypothesis is accepted, which indicates there is a statistically significant effect of administrative factors on the commitment of government employees to cybersecurity policies at the level of significance ($\alpha \leq 0.05$).

Table 16 shows the analysis of the results of the independent variable (legislative factors) on the intermediate variable (commitment). The results of the statistical analysis showed that there is a statistically significant effect of legislative factors on the commitment of employees of government organizations in the

Table 15. Test for Multicollinearity between the independent variables.

Independent Variables	VIF	Tolerance
Administrative factors	1.775	0.563
Legislative factors	1.608	0.622
Technical factors	1.602	0.624
Ethical factors	1.138	0.879

Table 16. Test the hypotheses.

Hypothesis	R	R2	F	Sig	T	Sig
H1	0.416	0.173	50.859	0.000	7.132	0.000
H2	0.399	0.160	46.144	0.000	6.793	0.000
H3	0.526	0.277	93.036	0.000	9.646	0.000
H4	0.422	0.178	52.607	0.000	7.253	0.000
H5	0.542	0.294	101.082	0.000	10.052	0.000

Kingdom of Saudi Arabia to cybersecurity policies, since the correlation coefficient (R) was (0.399) at the level ($\alpha \leq 0.05$). The coefficient of determination R2 was (0.160), meaning that its value is (0.399) of changes in the protection of information and technology assets resulting from the change in the legislative factors ($\alpha \leq 0.05$). This confirms the invalidity of accepting hypothesis (H2). Accordingly, the null hypothesis (H2) is rejected, and the alternative hypothesis is accepted, which indicates there is a statistically significant effect of legislative factors on the commitment of government employees to cybersecurity policies at the level of significance ($\alpha \leq 0.05$).

Table 16 shows the analysis of the results of the independent variable (technical factors) on the intermediate variable (commitment). The results of the statistical analysis showed that there is a statistically significant effect of technical factors on the commitment of employees of government organizations in the Kingdom of Saudi Arabia to cybersecurity policies, as the correlation coefficient (R) was (0.526) at the level ($\alpha \leq 0.05$). The coefficient of determination R2 was (0.277), meaning that its value is (0.526) of changes in the protection of information and technology assets resulting from the change in the dimension of technical factors ($\alpha \leq 0.05$). This confirms the invalidity of the acceptance of the hypothesis (H3). Accordingly, the null hypothesis (H3) is rejected, and the alternative hypothesis is accepted, which indicates there is a statistically significant effect of technical factors on government employees' commitment to cybersecurity policies at the level of significance ($\alpha \leq 0.05$).

Table 16 shows the analysis of the results of the independent variable (ethical factors) on the intermediate variable (commitment). The results of the statistical analysis showed that there is a statistically significant effect of ethical factors on the commitment of employees of government organizations in the Kingdom of Saudi Arabia to cybersecurity policies, since the correlation coefficient (R) was (0.422) at the level ($\alpha \leq 0.05$). The coefficient of determination R2 was (0.178), meaning that the value of (0.422) changes in the protection of information and technology assets resulted from the change in the dimension of ethical factors ($\alpha \leq 0.05$). This confirms the invalidity of accepting hypothesis (H4). Accordingly, the null hypothesis (H4) is rejected, and the alternative hypothesis is accepted, which indicates there is a statistically significant effect of ethical factors on government employees' commitment to cybersecurity policies at the level of significance ($\alpha \leq 0.05$).

Table 16 shows the analysis of the results of the intermediate variable (compliance with cybersecurity policies) on the dependent variable (protection of information and technology assets). The results of the statistical analysis showed that there is a statistically significant effect of government employees' commitment to cybersecurity policies on the protection of information and technology assets, since the correlation coefficient (R) was (0.542) at the level ($\alpha \leq 0.05$). The coefficient of determination R2 was (0.294), meaning that the value of (0.542) changes in the protection of information and technology assets results from the change in compliance with cybersecurity policies ($\alpha \leq 0.05$). This confirms the invalidity of the acceptance of hypothesis (H5). Accordingly, the null hypothesis (H5) is rejected, and the alternative hypothesis is accepted, which indicates there is a statistically significant effect of government employees' commitment to cybersecurity policies on the protection of information and technology assets at the level of significance ($\alpha \leq 0.05$).

9. Conclusion

Today's digital age makes it challenging to protect an organization's information and technology assets from cyber attacks; organizations can be vulnerable to cyber attacks because of the behavior of employees. The purpose of the study was to know some factors that influence employees of government organizations in the Kingdom of Saudi Arabia to comply with cybersecurity policies in order to protect information and technology assets. Employee noncompliance with the organization's Information Security Policy (ISP) exposes information and technology assets to cyber risks [17]. This study examined the following factors (administrative, legislative, technical, and ethical) and their impact on employees in order to comply with cybersecurity policies. The study found that these factors positively influence the employees of government organizations to a high degree to comply with cybersecurity policies. Ethical factors are considered one of the most important factors influencing compliance, from the point of view of the study sample of employees of government organizations in the Kingdom of Saudi Arabia. Results indicate that there is a significant role play by ethical factors, on employee towards cybersecurity compliance which is consistent with the study [29]. The results of the study also showed that the legislative factors ranked second in terms of influence, followed by the technical factors. Administrative factors are less influential compared to other factors. This study may contribute and help decision makers in government organizations to enhance strengths and improve weaknesses, taking into account the results of this study in order to raise the level of protection of information and technology assets.

10. Limitations and Future Work

Since this study examined the factors influencing government employees' compliance with cybersecurity policies, it has some limitations that can be addressed in future work, such as increasing the influencing factors, as the number of factors in the current study amounted to four factors. Another limitation is that the study was restricted to employees of government organizations. In the future, private sector employees must be added. It should also take into account the increase in the number of participants in the questionnaire.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Brodny, J. and Tutak, M. (2022) Analyzing the Level of Digitalization among the Enterprises of the European Union Member States and Their Impact on Economic Growth. *Journal of Open Innovation*: *Technology*, *Market*, *and Complexity*, **8**, Article 70. https://doi.org/10.3390/joitmc8020070

[2] Antunes, M., Maximiano, M., Gomes, R. and Pinto, D. (2021) Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, **1**, 219-238. https://doi.org/10.3390/jcp1020012

[3] de Reuver, M., Sørensen, C. and Basole, R.C. (2018) The Digital Platform: A Research Agenda. *Journal of Information Technology*, **33**, 124-135. https://doi.org/10.1057/s41265-016-0033-3

[4] International Data Corporation (2020) Cybersecurity and Its Impact on Digital Saudi. https://resources.trendmicro.com/rs/945-CXD-062/images/Cybersecurity-and-its-Impact-on-Digital-Saudi.pdf

[5] National Cybersecurity Authority (2018) Essential Cybersecurity Controls. https://www.nca.gov.sa/ecc-en.pdf

[6] Alsemairi, S.S. (2022) The Reality of Cybersecurity and Its Challenges in Saudi Arabia. *Scientific Journal of King Faisal University*: *Basic and Applied Sciences*, **23**, 66-74. https://doi.org/10.37575/b/cmp/210075

[7] Scholl, M.C., Fuhrmann, F. and Scholl, L.R. (2018) Scientific Knowledge of the Human Side of Information Security as a Basis for Sustainable Trainings in Organizational Practices. *Proceedings of the 51st Hawaii International Conference on System Sciences*, Hawaii, 3-6 January 2018, 2235-2244.

[8] Ifinedo, P. (2014) Information Systems Security Policy Compliance: An Empirical

Study of the Effects of Socialization Influence and Cognition. *Information & Management*, **51**, 69-79. https://doi.org/10.1016/j.im.2013.10.001

[9] Triplett, W.J. (2022) Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy*, **2**, 573-586. https://doi.org/10.3390/jcp2030029

[10] Koohang, A., Anderson, J., Nord, J.H. and Paliszkiewicz, J. (2020) Building an Awareness-Centered Information Security Policy Compliance Model. *Industrial Management & Data Systems*, **120**, 231-247. https://doi.org/10.1108/IMDS-07-2019-0412

[11] Sulaiman, N.S., Fauzi, M.A., Wider, W., Rajadurai, J., Hussain, S. and Harun, S.A. (2022) Cyber—Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review. *Social Sciences*, **11**, Article 386. https://doi.org/10.3390/socsci11090386

[12] Gwebu, K.L., Wang, J. and Hu, M.Y. (2020) Information Security Policy Noncompliance: An Integrative Social Influence Model. *Information Systems Journal*, **30**, 220-269. https://doi.org/10.1111/isj.12257

[13] VMware (2021) Saudi Arabia Security Insights Report 2021. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-global-security-insights-report-saudi-arabia.pdf

[14] Ifinedo, P. (2012) Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security*, **31**, 83-95. https://doi.org/10.1016/j.cose.2011.10.007

[15] AlGhamdi, S., Win K.T. and Vlahu-Gjorgievska, E. (2022) Employees' Intentions toward Complying with Information Security Controls in Saudi Arabia's Public Organisations. *Government Information Quarterly*, **39**, Article ID: 101721. https://doi.org/10.1016/j.giq.2022.101721

[16] Alanazi, T.S., Anbar, M., Ebad, A.S., Karuppayah, S. and Al-Ani, H.A. (2020) Theory-Based Model and Prediction Analysis of Information Security Compliance Behavior in the Saudi Healthcare Sector. *Symmetry*, **12**, Article 1544. https://doi.org/10.3390/sym12091544

[17] Koohang, A., Nowak, A., Paliszkiewicz, J. and Nord, J.H. (2020) Information Security Policy Compliance: Leadership Trust Role Values and Awareness. *Journal of Computer Information Systems*, **60**, 1-8. https://doi.org/10.1080/08874417.2019.1668738

[18] Addae, J.A., Simpson, G. and Ampong, G.O.A. (2019) Factors Influencing Information Security Policy Compliance Behavior. 2019 *International Conference on Cyber Security and Internet of Things*, Accra, 29-31 May 2019, 43-47.

[19] Connolly, L.Y., Lang, M. and Wall, D.S. (2019) Information Security Behavior: A Cross-Cultural Comparison of Irish and US Employees. *Information Systems Management*, **36**, 306-322. https://doi.org/10.1080/10580530.2019.1651113

[20] Alqahtani, M.A. and Braun, R. (2021) Examining the Impact of Technical Controls, Accountability and Monitoring towards Cyber Security Compliance in E-Government Organizations. https://doi.org/10.21203/rs.3.rs-196216/v1

[21] International Telecommunication Union (2008) X.1205: Overview of Cybersecurity. https://www.itu.int/rec/T-REC-X.1205-200804-I

[22] Jeong, J., Mihelcic, J., Oliver, G. and Rudolph, C. (2019) Towards an Improved Understanding of Human Factors in Cybersecurity. 2019 *IEEE 5th International Conference on Collaboration and Internet Computing* (*CIC*), Los Angeles, 12-14 De-

cember 2019, 338-345. https://doi.org/10.1109/CIC48465.2019.00047

[23] Communications and Information Technology Commission (CITC) (2007) Anti-Cyber Crime Law. https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/2

[24] Hamburg, I. (2021) Interdisciplinary Training and Mentoring for Cyber Security in Companies. In: Cruz-Cunha, M.M. and Mateus-Coelho, N.R., Eds., *Handbook of Research on Cyber Crime and Information Privacy*, 356-371. https://doi.org/10.4018/978-1-7998-5728-0.ch018

[25] Sullins, J. (2023) Information Technology and Moral Values. https://plato.stanford.edu/archives/spr2021/entries/it-moral-values

[26] Sekaran, U. and Bougie, R. (2016) Research Methods for Business: A Skill Building Approach. 7th Edition, John Wiley & Sons, West Sussex.

[27] Sekaran, U. (2003) Research Methods for Business: A Skill Building Approach. 4th Edition, John Wiley & Sons, West Sussex.

[28] Sekaran, U. and Bougie, R. (2010) Research Methods for Business: A Skill Building Approach. 5th Edition, John Wiley & Sons, Haddington.

[29] Borena, B. and Bélanger, F. (2013) Religiosity and Information Security Policy Compliance. *Americas Conference on Information Systems* (*AMCIS*), Chicago, 15-17 August 2013, 2848-2855.