Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR
JISCR

The Effect of Applying Information Security Awareness Concept of MOH Employees on Cybersecurity Department – Ministry of Health –Riyadh

Mohammed Masaad ALotibi[1*], and Abdulrahman Abdullah Alghamdi[2]

[1] Ministry of Health, Riyadh, Saudi Arabia.

[2] Department of Computer Science, College of Computing and information Technology, Shaqra, Saudi Arabia.

Received 09 Aug. 2022; Accepted 14 Sept. 2022; Available Online 15 Oct. 2022

Abstract

The proposed study focuses on the effect of applying the concept of information security awareness of MOH employees on the cybersecurity department at the Ministry of Health in Riyadh. The researcher used the descriptive analytical method in order to achieve the study objectives and used a questionnaire for collecting data. The study sample consisted of around (430) of MOH employees. The results of the study showed a high level of agreement on answering its questions. The study yielded numerous recommendations; it stressed that spreading the culture of awareness on the importance of personal information, through holding workshops, is considered as the most effective way to reduce cybersecurity risks. Also, it showed that the cybersecurity department is keen to develop guidelines to be followed by employees in order to limit the sharing of personal information and that paramount importance should be attached to the human element by familiarizing it with the tricks used by cybercriminals. In addition, the cybersecurity department is keen to create an electronic archive that includes monitoring and recording of cybersecurity incidents and should encourage employees to view this archive and consider it as a means of exchanging knowledge and raising awareness. Moreover, it is imperative to use the contribution of information security experts in order to design awareness programs. In addition, advanced technical training should be directed to employees to keep pace with the rapid development in methods and techniques of information crime. The researcher achieved various design of training and education program.

I. Introduction

The current era is characterized by great developments in the field of information and communication technology, which have become a major axis of development in any country and indicate that we are now living in the information society, or the information era.

On the negative side, this development contributes to the creation of a group of world crimes called “Cybercrime”, [1]. Cybercrime refers to a wide range of crimes that share in one feature that is they use digital technology and computers as tools, and the digital environment as a field for their practice.

Keywords: Cybersecurity, Information Security, Cybersecurity Department, Awareness, Ministry of Health.

Production and hosting by NAUSS

* Corresponding Author: Mohammed Masaad ALotibi
Email: mmaalotibi2@gmail.com

doi: 10.26735/JFLR5507

The digital environment means the use of information technology to transform the methodology of work, so that patient care includes the use of technologies such as Telehealth, predictive analytics, and artificial intelligence" [2]. The term "Cybercrime" is now used in the sense of referring to criminal activities that take place through: Electronic media such as hacking and malicious viruses breaching information security.

Cybersecurity is a wide international concern, it is associated with multi dimensions such as politics, national security, business, finance, reputation, country infrastructure and even more such as personal psychological issues related to digital bullying, digital blackmail, identity theft, spying and theft of finical assets. In the coming near future the information will be more valuable than cash, and the cybersecurity in any organization has its duty to defend and predict, recover, learn, report and educate for every single attack or system vulnerability [3]. One of the largest organizations in the Kingdom of Saudi Arabia is the Ministry of Health (MOH), it contains lots of sensitive information related to patients medical information, and staff personal information either medical and nonmedical, electronic transmission of other data required from other systems such as hospitals and health care centers, monitoring many diseases, especially infectious diseases [4].

Although large organizations have the technical means to protect their information security, they still routinely fall victim to cybercrime, and therefore providing employees with adequate knowledge about the increased possibility of this type of cyber-attack is an important first step to confront these threats. Examples include intentional acts of extortion, by using the information of the organization to blackmail it in order to achieve personal interests, as if someone in the organization obtained sensitive information and threatens to publish this information. Acts of intentional sabotage is another example. This type of threat arises from the presence of an individual or individuals within the organization who want to sabotage or destroy a computer system, or to perform acts harmful to the organization's information assts, and therefore providing employees with adequate knowledge about the increased possibility of this type of cyber-attack is an important first step to confront these threats [5].

Employees are the key stakeholders in the Ministry of Health (MOH); thus, it is extremely important for the cybersecurity department to prioritize their security level. As such, employees awareness remains a dominant phenomenon in improving information security because it improves cybersecurity for the whole organization, both in the technical sense, and by reducing risks. To incorporate these two functions, cybersecurity professionals have shifted their concern towards understanding both the information security awareness of security planning interventions that they use, and the systematic assessment of prevention delivery [6], [7]. This study has been ethically approved by the Saudi Ministry of Health under number (22-25 M).

Hence, the study came to identify the effectiveness of information security awareness in reducing risks of cybercrime from the viewpoint of the employees of the Ministry of Health in Riyadh.

II. Study Problem

Data exchange in all activities has become the hallmark of the twenty-first century society, moreover, the evaluation of organizations is related to the volume of information they possess, so the important aspect should not be obtaining information only, but rather protecting it from all attacks [8]. Despite the emergence of various systems and different mechanisms of protection with the aim of solving security problems, installing newest or latest applications showed that there is no guarantee to the complete protection of the system, as the critical element is the individual and not the device. [8]. On the other hand, cybercriminals have become more technologically efficient, as they use smarter deception methods to create and implement fraud and perpetrate cybercrime, and thus employees need to be more educated and knowledgeable regarding threats and vulnerabilities on the internet, as they are the most targeted category by cybercriminals.

Therefore, the study problem can be formulated in the following question: What are the effects

of applying the concept of information security awareness of employees on the cybersecurity department?.

Study Objectives:

- Measuring the level of awareness among MOH employees.
- Study the correlation between the importance of awareness and cybersecurity department improvement.
- Explore the deferent types of awareness and how to be effective in reducing risks.
- Knowledge of deferent ways of predictions of threats & best time of the cybersecurity professional's interventions.
- Design best cybersecurity education and awareness program.

III. Study Questions

-Q1: What are the effects of applying the concept of information security awareness of employees on the cybersecurity department?

-Q2: How do the Ministry of Health employees evaluate the cybersecurity department?

-Q3: Do employees understand the relationship between information security awareness and cybersecurity?

-Q4: What aspects of information security awareness affect cybersecurity department the most?

IV. Literature Review

Concept of Information Security

The concepts presented by the researchers differed with regard to the concept of information security, and among these definitions of information security it is defined as "protecting information from unauthorized access" [9].

In another definition of information security, it is defined as "maintaining confidentiality, availability and integrity of information in the stages of processing, preservation and transmission, and this is achieved through the actual application of security policies and through the promotion of awareness, learning and training" [10].

It is noted from the previous definition of the concept of information security that it is achieved through security measures and combating all forms of information abuse through training and learning [11]. In another definition of information security, it is "those policies, procedures and vision that are designed, customized then implemented at various levels, institutional and individual, which aim to achieve the various elements of maintenance and protection that ensure confidential information or reliability, safety and availability when needed." [12]. Through the previous definitions, we find that the concept of information security includes a wide range of practices, tools and concepts closely related to information security and technology, all of which focus on the following axes [6]:

1. Protection of information from any damage, whether the source of this damage is people (hacker) or programs (harmful viruses), and whether this damage was intentional or by unintended error.
2. Protecting information from unauthorized access to such information.
3. Protecting the facility's ability to continue and perform its business in the best possible way.
4. Protecting the information systems and programs to ensure that they operate in the organization at the most secure level.

The Importance of Information Security

The importance of information security stems from the globalization and comprehensiveness of information, as it is used by everyone, without exception, countries, companies, individuals, and therefore penetration of this information is a goal shared by those parties, and sometimes information is the difference between profit and loss for organizations, with the increase in the amount of information, the problem is not in obtaining data and converting it into information that can be used to meet the needs of decision makers, but also countermeasures to achieve security against any potential breaches of information systems [7].

In determining the importance of information security, the following points were noted [13]:

1. Protection of the important information assets of the facility, such as data centers,

databases, servers, local information, application programs and information storage devices (storage devices).

2. The business need of institutions for information, which constitutes the real wealth of these organizations, and electronic commerce is a good example of that.
3. The need for beneficiaries of electronic services to protect their information. For example: e-health services in which patients' health information is received electronically.
4. The spread of electronic services such as e-government services, e-procurement, distance learning and other services obtained electronically.
5. The abundance and diversity of information threats.
6. The spread of electronic attacks such as: network penetration, destruction of systems, and the emergence of computer viruses.

Human Information Security Threats

Threats to information security related to individuals working within the organization whose details of work are related to dealing with information systems include the following:

First: the wrong behavior of the employees" unintended actions"

This type of threat is the result of unintended actions of those dealing with the organization's information systems, as their mistakes lead to problems when they deal with the organization's information systems. This is due to lack of experience or lack of sufficient training to deal with these systems. Examples of these errors include disclosing organization's data, entering wrong data, accidentally deleting or modifying data, or storing data in incorrect locations. For example, storing data that is supposed to be viewed only by specific people, and is stored in a wrong way that can be viewed by anyone [14]. Study [15] showed that although some individuals have sufficient awareness of cyber threats, they may not adequately apply preventive measures.

Second: intentional actions

They are threats whose main aim is to harm the organization and its information systems. These acts include several forms, including [16]:

1. Acts of intentional infringement: This occurs when one of the employees of the organization who is not authorized to access specific information the organization is working to protect, and these acts negatively affect the confidentiality and privacy of information in the organization.
2. Intentional acts of extortion: by using the information of the organization to blackmail it in order to achieve personal interests, as if someone in the organization obtained sensitive information and threatens to publish this information.
3. Acts of intentional sabotage: This type of threat arises from the presence of an individual or individuals within the organization who want to sabotage or destroy a computer system, or to perform acts harmful to the organization's information assets.

As indicated by the study [17], a cybersecurity policy should be developed, in addition to cybersecurity risk assessment, and ongoing monitoring for user activity.

It is clear from the above that the absence of an information security policy in the organization, such as keeping additional copies of the information and software owned by the organization, will lead to the incurring of clear expenses and losses related to the time, effort and money spent to re-establish a new information system.

Information Security Awareness

In order to promote a culture of cybersecurity, all organizations need to focus on some fields, the most important of which are [18]:

First: Cybersecurity Training

Employees are one of the main sources of cybersecurity risk as it turns out that the reason for the success of many cybersecurity attacks that occurred in companies is that employees make mistakes such as unintentionally downloading

malware or responding to a phishing attack, that is why cybersecurity training is an essential component of any program. For cybersecurity, the best technical controls over security systems can be quickly breached due to lack of awareness by employees of cybersecurity risks. Thus, organizations must conduct analysis to determine where skills gap and vulnerabilities exist, and to develop and deliver training in these areas. This training should be directed at all managers and employees to ensure that they are aware of the latest threats and are able to conduct business in a safe manner as possible [19].

Second: Regular Auditing and Documentation

To identify weaknesses in information network infrastructure, process flow, and internal security to ensure data is secured once vulnerabilities are identified. The steps to be taken are documented to mitigate any potential downtime due to cyber-attacks [20].

Cybersecurity Awareness Campaign

Personal Factors and Awareness

The lack of awareness of the importance of information security leads employees in the company to not secure the information properly. This makes information more vulnerable to attacks. Some employees may be careful to secure their information, but some employees may not take the right approach. In addition, some employees may use company resources for their own personal use. For example, employees use the company's e-mail for personal communications, and some companies give mobile phones to some of their employees who use them for their personal communications. Some people may not own a personal computer and they might use the company-provided laptop or other device for everything including running personal software, leaving the application running and go away from office, or sending detailed information over the internet by emails and other means. So, employees should be careful not to confuse their personal life with their jobs. This requires that the company explains this matter to the employees and most importantly to make work rules and ethics clear to all employees and to increase employees awareness of information security [21].

Study [22] indicated the necessity of training individuals to acquire and master the skills necessary to exchange knowledge and benefit from information systems.

Cultural Factors and Awareness

Cultural factors are among the most important factors that should be taken with high consideration when designing any information security awareness messages. Therefore, it is necessary to take into account the extent to which the awareness message matches the prevailing culture among employees in order to achieve the positive impact of awareness messages [23].

Success Factors for Cyber Security Awareness

In order for the awareness campaign to succeed, it is necessary to take into account not only teaching employees new skills in effective and correct dealing with the internet, but also motivating employees to increase their capabilities with regard to the knowledge that they must possess when dealing with the Internet [24].

Views vary about security awareness campaigns and their impact on individuals awareness, and the extent to which they achieve safe use on the internet, and despite the provision of all possibilities for the success of security awareness, the presence of some shortcomings in the procedures may result in failure on achieving the objectives of security awareness, on the other hand. There may be no interest in measuring the impact of security awareness campaigns on employees in changing employee behaviors towards safe use of the internet.

In order for the awareness campaign to succeed, some common mistakes must be avoided which lead to the awareness campaign not having any positive impact on the behavior of individuals. The first of these errors is the insufficient understanding of security awareness, and secondly exaggeration of expectations for the impact of the awareness campaign. The third is the lack of effective participation of employees in the awareness campaign. The fourth

is not evaluating awareness programs and their success in making a positive impact on the behavior of individuals. Fifth is the dispersion in the objectives of the awareness campaign, not focusing on a specific aspect of the threat, and providing adequate training to confront this threat [25].

V. Methodology and Data Collection

The descriptive analytical approach was used to suit this study. The descriptive approach is related to the study of the problems related to the humanities. The current study population includes all employees of the Ministry of Health in Riyadh. A random sampling method was used, and the study sample consisted of (430) individuals. A questionnaire has been used to gather and collect data from the study sample individuals.

The questionnaire was divided into two parts, first where individuals are asked about their demographic information, the second is the study questions and was divided into four sections. Participants will be asked to fill out a written questionnaire electronically that will include statements about the effect of applying the concept of information security awareness of MOH employees on the cybersecurity department.

Data was analyzed using software (SPSS version 20).

Reliability of the Questionnaire

The questionnaire was presented to reviewers from the faculty members at Shaqra University to ensure the validity and reliability of the questionnaire's paragraphs, and it was approved after making modifications to some of the paragraphs and reformulating others.

The researcher distributed the questionnaire to an exploratory sample of the study sample in order to obtain feedback about the questionnaire in general before the questionnaire was distributed in its final form, and the internal consistency coefficient (Cronbach's alpha) was extracted. The following table shows the stability coefficients of the study tool.

Table I presents that the values of reliability coefficients are positive with the convergence of values for each axis, where it reached its highest limit for phrases third axis (0.861) and a minimum of phrases fourth axis (0.823), while the total reliability coefficient general reached (0.877), a corroborative treatment that reassures the researcher the availability of a high degree of reliability in addition to determining the validity.

Personal Data of the Study Sample

The researcher used percentages and frequencies to identify the distribution of study sample members according to personal variables, and the results were as shown in the following table.

Table II shows distribution of the study sample, the largest percentage in gender was males and amounted to (318) which equals 74.0% and the lowest percentage was females and amounted to (112) which equals 26.0%. In addition, it shows that the largest percentage in age was the age category 36-45 years and amounted to (234) which equals 54.42% and the lowest was the age category 18-25 and amounted to (22) which equals 5.12%. The largest percentage

TABLE I
Cronbach's Alpha Coefficient to Measure Reliability

Study axes	Number of statements	Cronbach's Alpha
1. What are the effects of applying the concept of information security awareness of employees on the cybersecurity department?	6	0.844
2. How do employees at the Ministry of Health evaluate the cybersecurity department?	6	0.836
3. Do employees understand the correlation between information security awareness and cybersecurity?	6	0.861
4. What aspects of information security awareness affect cybersecurity department the most?	6	0.823
Reliability coefficient General	24	0.877

TABLE II
Personal Data of The Study Sample

Gender	N	%
Male	318	74.0
Female	112	26.0
Total	**430**	**100%**
Age	**N**	**%**
18-25	22	5.12
35 – 26	119	27.67
45 – 36	234	54.42
60 – 46	55	12.79
Total	**430**	**100%**
Nationality	**N**	**%**
Saudi	416	96.7
Non Saudi	14	3.3
Total	**430**	**100%**
Educational Qualification	**N**	**%**
Secondary or equivalent	16	3.72
Diploma	94	21.86
Bachelor	223	51.86
Postgraduate	97	22.56
Total	**430**	**100%**
Job category	**N**	**%**
Physician	25	5.81
Nursing	64	14.88
Administrative	118	27.44
Pharmacists	41	9.53
Health allied professionals	126	29.30
Other	56	13.02
Total	**430**	**100%**
Years of Experience	**N**	**%**
Less than 5 years	62	14.42
From 5 to less than 10 years	87	20.23
From 10 to less than 15 years	136	31.63
years and more 15	145	33.72
Total	**430**	**100%**

in nationality was the Saudi and amounted to (416) which equals 96.7% and the lowest percentage was Non-Saudi and amounted to (14) which equals 3.3%. As for the educational qualification, the largest percentage was bachelor and amounted to (223) which equals 51.86% and lowest was secondary or equivalent and amounted to (16) which equals 3.72%. in the job category, the largest percentage was health allied professionals and amounted to (126) which equals 29.30% and lowest was physician and amounted to (25) which equals 5.81. With reference to years of experience, the largest percentage was (15 years and more) and amounted to (145) which equals 33.72% and the lowest was (less than 5 years) and amounted to (62) which equals 14.42%.

The following tables shows the demographic characteristics of the study sample.

TABLE III
Distribution of Study Sample According Gender

Gender	N	%
Male	318	74.0
Female	112	26.0
Total	430	100%

The above table shows distribution of the study sample according to gender shows that the largest percentage were the male and they numbered (318) by an equal 74.0% and the lowest percentage were female and their number (112) by an equal 26.0%. Fig. 1 shows these ratios.

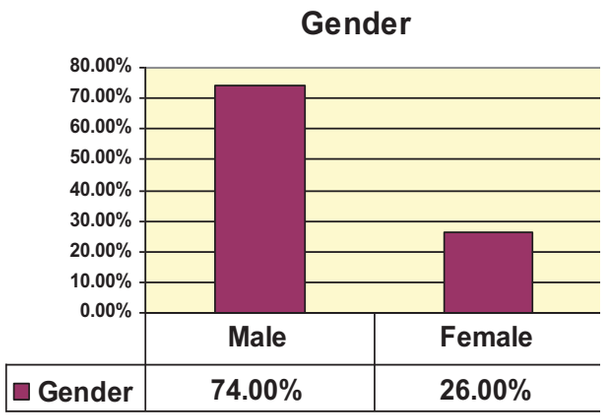

Fig. 1 Distribution of study sample according to gender.

TABLE IV
DISTRIBUTION OF STUDY SAMPLE ACCORDING TO AGE

Age	N	%
18-25	22	5.12
35 – 26	119	27.67
45 – 36	234	54.42
60 - 46	55	12.79
Total	430	100%

The above table shows distribution of the study sample according to age shows that the largest percentage were age category 36-45 years and they numbered (234) by an equal 54.42% followed age category 26-35 years and they numbered (119) by an equal 27.67% followed age category 46-60 years and they numbered (55) by an equal 12.79%. and lowest were age category 18-25 and they numbered (22) by an equal 5.12%. Fig. 2 shows these ratios.

TABLE V
DISTRIBUTION OF STUDY SAMPLE ACCORDING TO NATIONALITY

Nationality	N	%
Saudi	416	96.7
Non-Saudi	14	3.3
Total	430	100%

The above table shows distribution of the study sample according to nationality shows that the largest percentage were the Saudi and they numbered (416) by an equal 96.7% and the lowest percentage were Non-Saudi and their number (14) by an equal 3.3%. Fig. 3 shows these ratios.

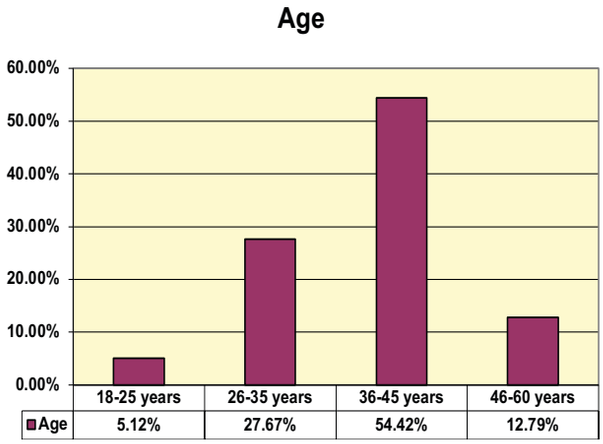

Fig. 2 Distribution of study sample according Age.

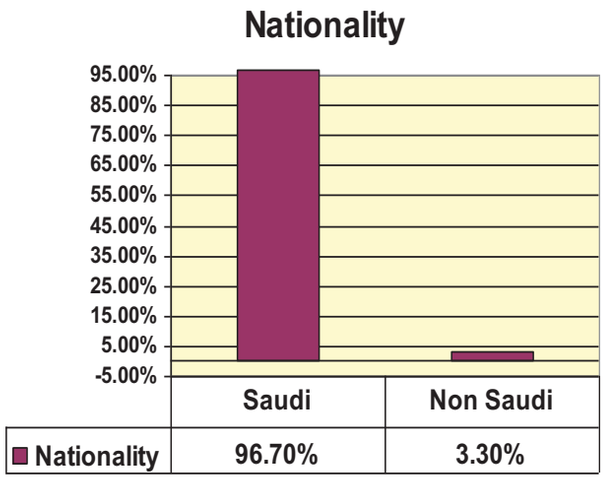

Fig. 3 Distribution of study sample according to Nationality.

TABLE VI
DISTRIBUTION OF STUDY SAMPLE ACCORDING QUALIFICATION

Qualification	N	%
Secondary or equivalent	16	3.72
Diploma	94	21.86
.Bachelor	223	51.86
Postgraduate	97	22.56
Total	430	100%

The above table shows distribution of the study sample according to Qualification shows that the largest percentage were Bachelor and they numbered (223) by an equal 51.86% followed Postgraduate and they numbered (97) by an equal 22.56% followed Diploma and they numbered (94) by an equal 21.86%. and lowest were Secondary or equivalent and they numbered (16) by an equal 3.72%. Fig. 4 shows these ratios.

TABLE VII
DISTRIBUTION OF STUDY SAMPLE ACCORDING JOB CATEGORY;

Job category	N	%
Physician	25	5.81
Nursing	64	14.88
Administrative	118	27.44
Pharmacists	41	9.53
Health allied professional	126	29.30
Other	56	13.02
Total	430	100%

The above table shows distribution of the study sample according to job category shows that the largest percentage were Health allied professional and they numbered (126) by an equal 29.30% followed Administrative and they numbered (118) by an equal 27.44% followed Nursing and they numbered (64) by an equal 14.88%.followed other jobs and they numbered (64) by an equal 14.88%. followed Pharmacists and they numbered (41) by an equal 9.53%.and lowest were Physician and they numbered (25) by an equal 5.81 Fig. 5 shows these ratios.

TABLE VIII
DISTRIBUTION OF STUDY SAMPLE ACCORDING TO YEARS OF EXPERIENCE;

Years of Experience	N	%
Less than 5 years	62	14.42
From 5 to less than 10 years	87	20.23
From 10 to less than 15 years	136	31.63
years and more 15	145	33.72
Total	430	100%

The above table shows distribution of the study sample according Years of Experience shows that the largest percentage were (15 years and more) and they numbered (145) by an equal 33.72% followed (From 5 to less than 10 years) and they numbered (136) by an equal 31.63% followed (From 5 to less than 10 years) and they numbered (87) by an equal 20.23%..and lowest were)Less than 5 years) and they numbered (62) by an equal 14.42 Fig. 6 shows these ratios.

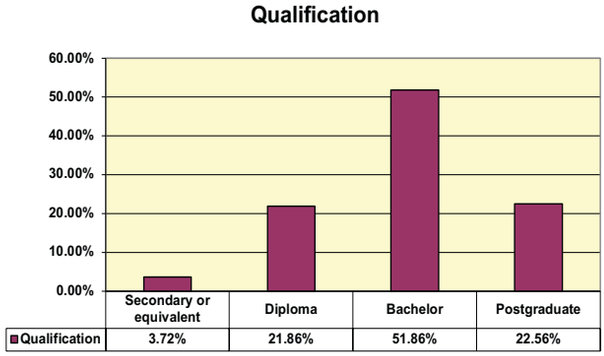

Fig. 4 Distribution of study sample according to Qualification.

Statistical Analysis of Study Questions

First question (What are the effects of applying the concept of information security awareness of employees on the cybersecurity department?)

Table IX shows the first question phrases, it turns out that the overall mean of all statements is (4.32) and this value according to the relative weight criterion indicates a very high degree, which means very high level of agreement by the majority of the study sample individuals on the determinants to first question, and the results show that there is a discrepancy in the sample study members agreement of the statements related to the first question, and the overall mean indicates a very high level of agreement on the study instrument.

It is clear from the answers to the first question of the study the importance of applying the concept of information security awareness among employees and the extent of its positive impact on the cybersecurity department. This effect is illustrated

TABLE IX
STATISTICAL ANALYSIS OF THE FIRST QUESTION PHRASES

S	Statements	Mean	Std. deviation
6	Enhance employee awareness regarding the dangers of unknown links when browsing websites on the internet	4.56	0.799
5	Unintentionally downloading malware leads to information security breaches	4.55	0.749
1	I always check every email I receive, especially those that contain links or attached files	4.46	0.803
3	I am careful about posting any personal information about myself on social media	4.46	0.846
4	I am interested in learning everything related to information security through continuous reading	4.08	0.972
2	Employees are always keen to reporting any information hacking incidents	3.83	1.329
	Overall Mean	4.32	

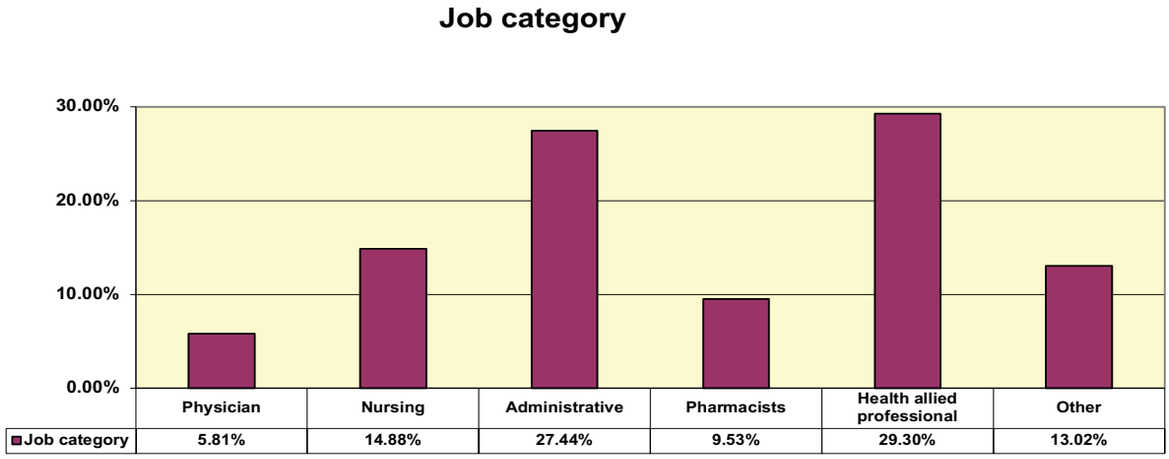

Fig. 5 Distribution of study sample according Job category.

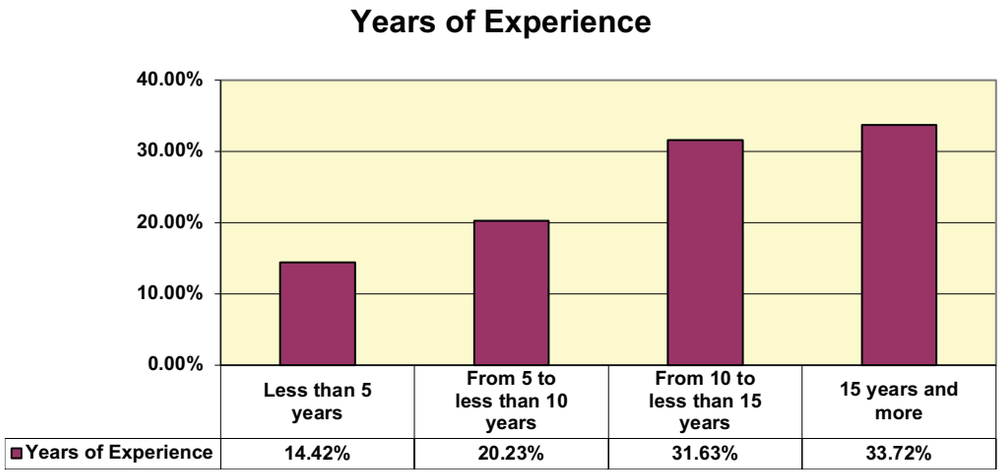

Fig. 6 Distribution of study sample according to Years of Experience.

by the role played by the cybersecurity department in promoting awareness among employees, and this interpretation is supported by the fact that the majority of the study sample are highly aware of the importance of caution when browsing on websites, avoiding anonymous links, and checking email messages well, especially if they contain attached files, and not post any personal information on social media.

Second question (How do cybersecurity department view the MOH facility in question?)

Table X shows the Second question phrases. It turns out that the overall mean of all statements is (3.48) and this value according to the relative weight criterion indicates a high degree, which means high level of agreement by the majority of the study sample individuals on the determinants to second question, and the results show that there is a discrepancy in the sample study members agreement of the statements related to the second question, and the overall mean indicates a high level of agreement on the study instrument.

It is clear from the answer to the second question of the study that the view of the majority of the study sample towards the cybersecurity department is that it achieves three basic elements of cybersecurity, which are:

The technical component, represented in the existence of database protection systems that prevent unauthorized persons from entering the systems.

The human element, it is represented in the

TABLE X
STATISTICAL ANALYSIS OF THE SECOND QUESTION PHRASES

S	Statements	Mean	Std. deviation
7	The cybersecurity department sets instructions for the use of e-mail to reduce the occurrence of security breaches	3.74	1.315
9	has database protection systems that prevent unauthorized persons The Ministry entering the systems from	3.57	1.291
8	The Ministry uses the latest technologies in security programs to prevent any information security breaches	3.56	1.310
12	In the past, data breach occurred due to staff misuse	3.42	1.181
11	The cybersecurity department is keen to provide employees with knowledge about the safe use of modern technological devices, especially those related to information security breaches	3.42	1.319
10	The Ministry has database protection systems that prevent unauthorized persons from entering the systems	3.17	1.336
	Overall Mean	3.48	

TABLE XI
STATISTICAL ANALYSIS OF THE THIRD QUESTION PHRASES

S	Statements	Mean	Std. deviation
17	Getting the information to the wrong person this could lead to leakage of this information	4.51	0.682
13	The employee's lack of understanding of information security contributes to the penetration of the information systems in the ministry	4.47	0.832
16	I am careful about not to open any anonymous emails	4.46	0.761
14	Be careful not to send any personal data through text messages or email	4.34	0.899
15	Employees access to social media during office hours increases the occurrence of information security breaches	4.01	1.051
18	The majority of employees have sufficient awareness of the importance of cybersecurity	3.24	1.322
	Overall Mean	4.17	

keenness of the cybersecurity department to provide employees with knowledge about the safe use of modern technological devices, especially those devices that are related to information security penetration.

The procedural component, the cybersecurity department determines the rules for the use of e-mail.

Third question (Do employees understand the relationship between information security awareness and cybersecurity?)

Table XI shows the third question phrases. It turns out that the overall mean of all statements is (4.17) and this value according to the relative weight criterion indicates a high degree, which means high level of agreement by the majority of the study sample individuals on the determinants to third question, and the results show that there is a discrepancy in the sample study members agreement of the statements related to third question, and the overall mean indicates a high level of agreement on the study instrument.

It is clear from the answer to the third question of the study that the viewpoint of the majority of the study sample individuals towards the employees' awareness of information security and cybersecurity is in of high degree, and the most important indicators of this are: the realization of the majority of the study sample individuals that granting information access to the wrong person can lead to the leakage of this information, also the lack of

TABLE XII
STATISTICAL ANALYSIS OF THE FOURTH QUESTION PHRASES

S	Statements	Mean	Std. deviation
22	Awareness of employees about the dangers of anonymous links as they constitute a threat of breach of information security	4.57	0.699
20	Educate employees about some of the risks resulting from information security breach	4.54	0.694
23	Reviewing and evaluating awareness activities every period of time in line with the development in information security penetration methods	4.53	0.711
21	Awareness of how to distinguish between safe and unsafe applications	4.48	0.810
19	Training on how to safe browsing on the internet	4.42	0.803
24	Motivating employees to collect new information in the field of information security	4.42	0.843
	Overall Mean	4.49	

employee's understanding of information security contributes to the occurrence of a penetration of information systems, and it was also found that the majority of the study sample individuals are aware of the danger of opening any anonymous e-mails, as this may result in a penetration of information systems. Despite these indicators that show a high degree of employee knowledge of information security, the previous results also indicate a medium degree towards the degree of employee awareness of the importance of cybersecurity. The researcher concludes that the degree of awareness is high, yet the majority of employees have less awareness of the importance of cybersecurity.

Fourth question (What aspects of information security awareness affect the cybersecurity department the most?)

Table XII shows the fourth question phrases. It turns out that the overall mean of all statements is (4.49) and this value according to the relative weight criterion indicates a very high degree, which means very high level of agreement by the majority of the study sample individuals on the determinants to fourth question, and the results show that there is a discrepancy in the sample study members agreement of the statements related to fourth question, and the overall mean indicates a very high level of agreement on the study instrument.

It is clear from the answer to the fourth question of the study that the viewpoint of the majority of the study sample individuals towards the most important aspects of information security awareness that have the most impact on the cybersecurity department are the awareness of the dangers of anonymous links, awareness of the negative effects resulting from information security penetration, continuous updating of awareness activities in proportion to continuous updating for information security penetration methods, provision of training on the safe use of the internet, and motivating employees to increase their knowledge regarding information security. The researcher concludes from the previous results that cybersecurity practices are applied at a good level, and they also contribute to increasing awareness of cybersecurity and realizing the importance of the information they deal with and their responsibility towards protecting it.

In order to determine the extent of the difference in the attitudes of the study sample individuals towards the study questions according to the differences in their personal and functional variables, T-test and ANOVA were performed, as shown in the following tables.

It is clear from Table XIII that there are statistically significant differences towards the first question, and the differences are in favor of the male category versus the female category.

It is clear from Table XIV that the (F) value was statistically significant towards the second question, and the differences were in favor of the age group (18-25) versus the age group (36-45), which means that the age group (18-25) was the most agreeable to cybersecurity department, and in contrast the age group (36-45) was least agreeable.

It is clear from Table XV that there are statistically significant differences towards the third question, and the differences are in favor of the Saudis category

TABLE XIII
THE RESULTS OF THE T-TEST TO FIND THE DIFFERENCES IN THE ANSWERS OF THE STUDY SAMPLE INDIVIDUALS ABOUT THE STUDY QUESTIONS ACCORDING TO THE GENDER VARIABLE

Study Questions	Gender	N	Mean	Std. Deviation	T value	Sig.
Q1: What are the effects of applying the concept of information security awareness of employees on the cybersecurity department?	Male	330	4.37	0.535	2.940	0.006
	Female	318	4.18	0.703		
Q2: How do employees at the Ministry of Health evaluate the cybersecurity department?	Male	112	3.58	1.001	3.258	0.011
	Female	318	3.21	1.123		
Q3: Do employees understand the relationship between information security awareness and cybersecurity?	Male	112	4.18	0.560	0.329	0.598
	Female	318	4.16	0.580		
Q4: What aspects of information security awareness affect the cybersecurity department the most?	Male	112	4.49	0.613	0.160	0.129
	Female	318	4.50	0.642		

TABLE XIV
THE RESULTS OF THE (ANOVA) TEST TO FIND THE DIFFERENCES IN THE ANSWERS OF THE STUDY SAMPLE INDIVIDUALS ABOUT THE STUDY QUESTIONS ACCORDING TO THE AGE VARIABLE

Study Questions	Age	N	Mean	Std. Deviation	F value	Sig.
Q1: What are the effects of applying the concept of information security awareness of employees on the cybersecurity department?	18-25	22	4.34	0.697	0.404	0.750
	26 – 35	119	4.36	0.515		
	36 – 45	234	4.31	0.600		
	46 - 60	55	4.26	0.649		
	Total	430	4.32	0.589		
Q2: How do employees at the Ministry of Health evaluate the cybersecurity department?	18-25	22	4.10	0.686	7.975	0.001
	26 – 35	119	3.75	0.937		
	36 – 45	234	3.30	1.098		
	46 - 60	55	3.45	0.963		
	Total	430	3.48	1.046		
Q3: Do employees understand the relationship between information security awareness and cybersecurity?	18-25	22	4.26	0.503	1.115	0.343
	26 – 35	119	4.21	0.511		
	36 – 45	234	4.17	0.589		
	46 - 60	55	4.06	0.589		
	Total	430	4.17	0.565		
Q4: What aspects of information security awareness affect the cybersecurity department the most?	18-25	22	4.40	0.623	1.782	0.150
	26 – 35	119	4.44	0.650		
	36 – 45	234	4.55	0.593		
	46 - 60	55	4.39	0.648		
	Total	430	4.49	0.620		

TABLE XV
THE RESULTS OF THE T-TEST TO FIND THE DIFFERENCES IN THE ANSWERS OF THE STUDY SAMPLE INDIVIDUALS ABOUT THE STUDY QUESTIONS ACCORDING TO THE NATIONALITY VARIABLE

Study Questions	Nationality	N	Mean	Std. Deviation	T value	Sig.
Q1: What are the effects of applying the concept of information security awareness of employees on the cybersecurity department??	Saudi	416	4.32	0.584	0.926	0.148
	Non Saudi	14	4.46	0.726		
Q2: How do employees at the Ministry of Health evaluate the cybersecurity department?	Saudi	416	3.46	1.052	1.933	0.067
	Non Saudi	14	4.01	0.658		
Q3: Do employees understand the relationship between information security awareness and cybersecurity?	Saudi	416	4.17	0.559	0.362	0.047
	Non Saudi	14	4.12	0.744		
Q4: What aspects of information security awareness ?affect the cybersecurity department the most	Saudi	416	4.50	0.611	0.398	0.129
	Non Saudi	14	4.43	0.867		

TABLE XVI
THE RESULTS OF THE (ANOVA) TEST TO FIND THE DIFFERENCES IN THE ANSWERS OF THE STUDY SAMPLE INDIVIDUALS ABOUT THE STUDY QUESTIONS ACCORDING TO THE EDUCATIONAL QUALIFICATION VARIABLE

Study Questions	Educational Qualification	N	Mean	Std. Deviation	F value	Sig.
Q1: What are the effects of applying the concept of information security awareness of employees on the cybersecurity department?	Secondary or equivalent	16	4.26	1.016	4.586	0.004
	Diploma	94	4.40	0.508		
	Bachelor	223	4.37	0.541		
	Postgraduate	97	4.13	0.640		
	Total	430	4.32	0.589		
Q2: How do employees at the Ministry of Health evaluate the cybersecurity department?	Secondary or equivalent	16	4.16	0.879	3.990	0.008
	Diploma	94	3.62	0.992		
	Bachelor	223	3.46	1.052		
	Postgraduate	97	3.29	1.057		
	Total	430	3.48	1.046		
Q3: Do employees understand the relationship between information security awareness and cybersecurity?	Secondary or equivalent	16	4.40	0.614	3.177	0.024
	Diploma	94	4.17	0.519		
	Bachelor	223	4.22	0.511		
	Postgraduate	97	4.04	0.687		
	Total	430	4.17	0.565		
Q4: What aspects of information security awareness affect the cybersecurity department the most?	Secondary or equivalent	16	4.44	0.755	1.843	0.139
	Diploma	94	4.46	0.623		
	Bachelor	223	4.56	0.571		
	Postgraduate	97	4.39	0.690		
	Total	430	4.49	0.620		

versus the non-Saudis. This is an indication that the Saudis category was the most accepting of employees' understanding of the relationship between information security awareness and cybersecurity, and in contrast the non-Saudis were the least agreeable.

It is clear from Table XVI that the (F) value was statistically significant towards the first, second, and third questions, and the differences were in favor of secondary or equivalent versus postgraduate, meaning that the category of secondary or equivalent was the most agreeable towards the three questions, and the postgraduate category was the least agreeable.

TABLE XVII
THE RESULTS OF THE (ANOVA) TEST TO FIND THE DIFFERENCES IN THE ANSWERS OF THE STUDY SAMPLE INDIVIDUALS ABOUT THE STUDY QUESTIONS ACCORDING TO THE JOB CATEGORY VARIABLE

Study Questions	Job category	N	Mean	Std. Deviation	F value	Sig.
Q1: What are the effects of applying the concept of information security awareness of employees on the cybersecurity department?	Physician	25	4.15	0.628	4.549	0.001
	Nursing	64	4.13	0.639		
	Administrative	118	4.45	0.464		
	Pharmacists	41	4.33	0.683		
	Health allied professional	126	4.25	0.594		
	Other	56	4.49	0.569		
	Total	430	4.32	0.589		
Q2: How do employees at the Ministry of Health evaluate the cybersecurity department?	Physician	25	3.17	1.016	10.270	0.001
	Nursing	64	3.13	1.057		
	Administrative	118	3.78	0.867		
	Pharmacists	41	3.31	1.269		
	Health allied professional	126	3.23	1.057		
	Other	56	4.10	0.754		
	Total	430	3.48	1.046		
Q3: Do employees understand the relationship between information security awareness and cybersecurity?	Physician	25	4.08	0.553	2.482	0.031
	Nursing	64	4.07	0.563		
	Administrative	118	4.24	0.547		
	Pharmacists	41	4.23	0.595		
	Health allied professional	126	4.09	0.584		
	Other	56	4.33	0.502		
	Total	430	4.17	0.565		
Q4: What aspects of information security awareness affect the cybersecurity department the most?	Physician	25	4.45	0.621	0.148	0.981
	Nursing	64	4.45	0.631		
	Administrative	118	4.51	0.562		
	Pharmacists	41	4.48	0.713		
	Health allied professional	126	4.50	0.670		
	Other	56	4.53	0.552		
	Total	430	4.49	0.620		

TABLE XVIII
THE RESULTS OF THE (ANOVA) TEST TO FIND THE DIFFERENCES IN THE ANSWERS OF THE STUDY SAMPLE INDIVIDUALS ABOUT THE STUDY QUESTIONS ACCORDING TO THE YEARS OF EXPERIENCE VARIABLE

Study Questions	Years of Experience	N	Mean	Std. Deviation	F value	Sig.
Q1: What are the effects of applying the concept of information security awareness of employees on the cybersecurity department?	Less than 5 years	62	4.45	0.614	2.476	0.061
	From 5 to less than 10 years	87	4.19	0.640		
	From 10 to less than 15 years	136	4.34	0.501		
	15 years and more	145	4.32	0.612		
	Total	430	4.32	0.589		
Q2: How do employees at the Ministry of Health evaluate the cybersecurity department?	Less than 5 years	62	4.03	0.911	8.725	0.001
	From 5 to less than 10 years	87	3.42	1.016		
	From 10 to less than 15 years	136	3.24	1.139		
	15 years and more	145	3.51	0.941		
	Total	430	3.48	1.046		
Q3: Do employees understand the relationship between information security awareness and cybersecurity?	Less than 5 years	62	4.32	0.555	3.980	0.008
	From 5 to less than 10 years	87	4.08	0.560		
	From 10 to less than 15 years	136	4.25	0.477		
	15 years and more	145	4.09	0.627		
	Total	430	4.17	0.565		
Q4: What aspects of information security awareness affect the cybersecurity department the most?	Less than 5 years	62	4.47	0.647	1.937	0.123
	From 5 to less than 10 years	87	4.42	0.613		
	From 10 to less than 15 years	136	4.60	0.580		
	15 years and more	145	4.45	0.641		
	Total	430	4.49	0.620		

It is clear from Table XVII that the (F) value was statistically significant towards the first, second, and third questions, and the differences were in favor of other jobs versus nursing, meaning that the category of other jobs was the most agreeable towards the three questions, and the nursing category was the least agreeable.

It is clear from Table XVIII that the (F) value was statistically significant towards the second question, and the differences were in favor of years of experience (less than 5 years) versus years of experience (from 10 to less than 15 years) meaning that the category of years of experience (less than 5 years) was the most agreeable towards the second question, and the category years of experience (from 10 to less than 15 years) was the least agreeable.

Also in the third question, the differences were in favor of years of experience (less than 5 years) versus years of experience (from 5 to less than 10 years) meaning that the category of years of experience (less than 5 years) was the most agreeable towards the third question, and the category years of experience (from 5 to less than 10 years) was the least agreeable.

V. RESULTS AND DISCUSSION

The results showed a high level of agreement from the majority of the study sample individuals

regarding the importance of applying the concept of information security awareness among employees and the extent of its positive impact on the cybersecurity department, and this is achieved through avoiding anonymous links, and checking email messages well, especially if they contain attached files, and avoid posting any personal information on social media. This is consistent with [21]which indicated the importance of having clear work rules for all employees to improve employees' awareness and understanding of the importance of information security. The researcher believes that the majority of the Ministry's employees have a high degree of awareness of the importance of information security, and this is evident through their behavior in the use of the internet.

The results showed a high level of agreement from the majority of the study sample individuals on the positive role played by the cybersecurity department, as cybersecurity was achieved through three basic elements. The technical component: represented in the existence of database protection systems that prevent unauthorized persons from entering the system. The human element: it is represented in the keenness of the cybersecurity department to provide employees with knowledge about the safe use of modern technological devices, especially those devices that are related to information security penetration. The procedural component: the cybersecurity department determines the rules for the use of e-mail. These results are consistent with the study [15] which showed that some individuals have sufficient awareness of cyber threats, they may not adequately apply preventive measures.

The researcher believes that the cybersecurity department plays an important role in promoting information security awareness for the Ministry's employees.

The results showed a high level of agreement from the majority of the study sample individuals towards the level of employees' awareness of information security and cybersecurity. The most important indicators of are the realization of the majority of the study sample individuals that granting information access to the wrong person can lead to the leakage of this information, also the lack of the employee's understanding of information security contributes to the occurrence of a penetration of information systems. It was also found that the majority of the study sample individuals are aware of the danger of opening any anonymous e-mails, as this may result in a penetration of information systems. Despite these indicators that show a high level of employees knowledge of information security, the previous results also indicate a medium level towards employees awareness of the importance of cybersecurity. The researcher concludes that the level of awareness is high, yet the majority of employees have less awareness of the importance of cybersecurity.

These results are consistent with a study [17] which recommends establishing a cybersecurity policy, cybersecurity risk assessment, and ongoing monitoring to users activities.

The researcher believes that there is a category of employees who have less awareness of the importance of cybersecurity.

The results showed a high level of agreement from the majority of the study sample individuals on aspects of information security awareness that have the greatest impact on the cybersecurity department. The researcher concludes that cybersecurity practices are applied at a good level, and also contribute to increasing awareness of cybersecurity and realizing the importance of the information they deal with and their responsibility towards protecting it.

This is consistent with the study [22] which indicated that individuals must be trained to acquire and master the skills necessary to exchange knowledge and benefit from information systems.

The researcher believes that the majority of employees understand the importance of aspects related to information security.

There are statistically significant differences in the first and second questions according to the gender variable. The differences were in favor of the male group versus the female group.

There are statistically significant differences in the first question according to the age variable. The differences were in favor of the age group (18-25) versus the age group (36-45) .

There are statistically significant differences in the third question according to the nationality variable. The differences were in favor of the Saudis category versus the non-Saudis.

There are statistically significant differences towards the first, second, and third questions according to the educational qualification variable and the differences were in favor of secondary or equivalent versus postgraduate.

There are statistically significant differences towards the first, second, and third questions according to the job category variable and the differences were in favor of other jobs versus nursing.

There are statistically significant differences towards the second and third questions according to the years of experience variable and the differences were in favor of years of experience (less than 5 years) versus years of experience (from 10 to less than 15 years) and (from 5 to less than 10 years).

VII. Recommendations

1. Spreading the culture of awareness of the importance of personal information and appreciating its importance as the most effective way to reduce cybersecurity risks, and this is done by organizing workshops at the Ministry in which focus is placed on information that should not be disclosed, whether through social media, over the phone, or personally.
2. The cybersecurity department is keen to develop guidelines to be followed by employees that include methods and cognitive strategies in order to limit personal information that is shared, whether on the internet or on social media.
3. Information security department should not only protect information through protection and anti-virus software, firewall and other software, but also should give sufficient importance to the human element by making it aware of the tricks that cybercriminals use to obtain information.
4. The cybersecurity department is keen to create an electronic archive that includes detailed cybersecurity incidents which occurred in various countries of the world, and to encourage employees to view this archive and consider it as a means of exchanging knowledge and awareness to keep pace with the rapid development in the methods of cybercriminals.
5. To seek the help of bodies with expertise in information security, for example, colleges specialized in information systems, in order to design awareness programs for workers on how to properly use the internet and the importance of avoiding suspicious sites.
6. Attention should be given to the provision of advanced technical training directed to employees to keep pace with the rapid development in methods and techniques of cybercrime. This can be achieved through the National Cybersecurity Authority, in order to educate trainees about the importance of cybersecurity.

Recommendations of the Cyber Security Program to Education and Awareness:

1. Individuals are the largest group in terms of being victims of cybercrime, as most of them lack sufficient knowledge of the importance of cybersecurity. Therefore, the proposed model in the current study is directed to the Ministry's employees to provide them with knowledge and information that leads indirectly to achieving cybersecurity.
2. There is a need to establish a department under the name (Information Security). A link on the internet should be provided to reach this department and an introductory message should be placed in this website that includes a definition of the objectives of this department, and how to exchange knowledge regarding cybersecurity.
3. This department shall be supervised by the cybersecurity department personnel at the Ministry, and they shall respond to the inquiries of site users and provide them with all knowledge and information related to cybersecurity.
4. Therefore, the proposed model in the current study aims to involve users in the exchange

of knowledge, as well as the use of a different methods for knowledge exchange, the basic idea of which is based on the exchange of knowledge between users and specialists in the cybersecurity department.

5. Choosing social media to be the framework for exchanging knowledge in cybersecurity as it allows the ease of expressing opinions and trends, communicating with friends both far and near, increasing knowledge and learning new information.
6. The expected objectives of applying this model are to increase the knowledge and information of employees in various aspects, for example, information security, cybercrime, how to secure the computer from harmful viruses, and how to discover and identify suspicious sites.

VIII. Conclusion

Awareness needs to be major concern in large foundations such as the Ministry of Health. Based on this study, the results showed a high degree about the impact of applying the concept of information security awareness of employees on the cybersecurity department. Results showed a high level of agreement on the efficiency of the cybersecurity department at the Ministry of Health from the employees' point of view. Also, the results showed a high level of agreement on the level of employees' understanding of the relationship between awareness and cybersecurity. Finally, the results of the study showed a high level of agreement on impact on the aspects of information security awareness on the cybersecurity department from the employees' point of view. The study also provided a description of an awareness program that can be implemented to educate employees about cybersecurity.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Authors declare that they have no conflict of interest.

References

[1] N. S. Safa, C. Maple, T. Watson, and R. Solms, "Motivation and opportunity based model to reduce information security insider threats in organisations," *J. Inf. Secur. Appl.*, vol. 40, pp. 247-257, 2018, doi: 10.1016/j.jisa.2017.11.001.

[2] J. Torous, K. Myrick, N. Rauseo-ricupero, and J. Firth, "Digital Mental Health and COVID - 19 : Using Technology Today to Accelerate the Curve on Access and Quality Tomorrow," *JMIR Ment. Health*, vol. 7, no. 3, Art. no. e18848, 2020, doi: 10.2196/18848.

[3] M. Thangavelu, V. Krishnaswamy, and M. Sharma, "Impact of Comprehensive Information Security Awareness and Cognitive Characteristics on Security Incident Management – An empirical study," *Comput. Secur.*, vol. 109, p. 102401, Oct. 2021, doi: 10.1016/j.cose.2021.102401.

[4] Ministry of Health, "Health Statistics Annual Book."

[5] C. A. Sanders, "Social Engineering Knowledge Measured as a Security Countermeasure," M. S. thesis, Coll. Eng. Comput., Univ. South Carolina, South Carolina, USA, 2018.

[6] J.-L. Vez and U. Damachi, "Guidance on Public- Private Information Sharing against Cybercrime," Jan 2017. [Online]. Available: https://www3.weforum.org/docs/WEF_Guidance_Cybercrime_report_2017.pdf

[7] K. A. Alshare, P. L. Lane, and M. R. Lane, "Information security policy compliance : a higher education case study," *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 91-108, 2018, doi: 10.1108/ICS-09-2016-0073.

[8] P. Schaab, K. Beckers, and S. Pape, "Social Engineering Defence Mechanisms and counteracting Training Strategies," *Inf. Comput. Secur.*, vol. 25, no. 2, pp. 206-222, 2017, doi: 10.1108/ICS-04-2017-0022.

[9] M. Yar, "Oxford Research Encyclopedia of Criminology" May 2017. [Online]. Available: https://www.shortcutstv.com/blog/wp-content/uploads/2020/02/Online_Crime._In_Oxford_Research_Encyclo.pdf

[10] M. Whitman and H. Mattord, *Principles of Information Security*, 4th ed., Boston, MA, USA: Course Technology, 2011.

[11] V. P. Talimonchik, "Legal Aspects of International

Information Security," in *Security and Privacy From a Legal, Ethical, and Technical Perspective, London*, United Kingdom: IntechOpen, 2019, ch. 1.

[12] A. Serkov, V. Kravets, O. Kasilov, B. Lazurenko, and A. Mickus, "THE CONCEPT OF INFORMATION SECURITY IN THE IOT SYSTEM," *Adv. Inf. Syst.*, vol. 3, no. 1, pp. 136-139, 2019, doi: 10.20998/2522-9052.2019.1.23.

[13] K. Prislan, A. Mihelič, and I. Bernik, "A real-world information security performance assessment using a multidimensional socio-technical approach," *Plos One*, vol. 15, no. 9, Art. no. e0238739, 2020, doi: 10.1371/journal.pone.0238739.

[14] A. Mousa, M. Karabatak, and T. Mustafa, "Database Security Threats and Challenges," in *2020 8th Int. Symp. Digit. Forensics Secur*. (ISDFS), 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116436.

[15] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness , Knowledge and Behavior : A Comparative Study," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 1–16, 2022, doi: 10.1080/08874417.2020.1712269.

[16] S. H. Jore, "The Conceptual and Scientific Demarcation of Security in Contrast to Safety," Eur. *J. Secur. Res.*, vol. 4, no. 1, pp. 157–174, 2019, doi: 10.1007/s41125-017-0021-9.

[17] S. Grades et al., "Study of Baseline Cyber Security for Various Application Domains," *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 1099, p. 012051, 2021, doi: 10.1088/1757-899X/1099/1/012051.

[18] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, "Prevention is better than cure ! Designing information security awareness programs to overcome users ' non-compliance with information security policies in banks," *Comput. Secur.*, vol. 68, pp. 145–159, 2017, doi: 10.1016/j.cose.2017.04.009.

[19] B. Hanus and Y. Wu, "Impact of Users ' Security Awareness on Desktop Security Behavior : A Protection Motivation Theory Perspective," *Inf. Syst. Manag.*, vol. 33, no. 1, 2016, doi: 10.1080/10580530.2015.1117842.

[20] J. P. Adhikari, A. Sharma, and "An introduction to cyber crimes and role of cyber- security in information technology," *Int. J. IT & Eng.*, vol. 05, no. 04, pp. 13–20, 2017.

[21] P. Dolan, M. Hallsworth, D. Halpern, D. King, and I. Vlaev, "Influencing behaviour through public policy," 2010.

[22] S. Ziam, P.-E. Arduin, and D. Vieru, "Strategies to Reduce Knowledge Leakage: A Knowledge Absorptive Capacity-Based Framework," in *19th Euro. Conf. Knowledge Manag.*, Italy, 2018, pp. 1186-1189.

[23] G. Hofstede, G. J. Hofstede, and M. Minkov, *Cultures and Organizations*. USA: McGraw-Hill, 2010.

[24] M. Bada and A. Sasse, "Cyber Security Awareness Campaigns Why do they fail to change behaviour ?," 2014. [Online]. Available: https://discovery.ucl.ac.uk/id/eprint/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf

[25] B. Khan, K. S. Alghathbar, S. I. Nabi, and M. K. Khan, "Effectiveness of information security awareness methods based on psychological theories," *Afr. J. Bus. Manag.*, vol. 5, no. 26, pp. 10862–10868, 2011, doi: 10.5897/AJBM11.067.