Technological
Communication

BBRC
Bioscience Biotechnology
Research Communications

Biosc.Biotech.Res.Comm. Vol 13 No (4) Oct-Nov-Dec 2020 Pp 2271-2276

A Suggested Model to Raise Awareness of Cybersecurity Among Computer Teachers in Public Education: An Analytical Study on Education Department in Jeddah Governorate

Misbah Ahmed Al-Sahafi and Abdullah Mohammed Al-yateem*
Ministry of Education Riyadh Kingdom of Saudi Arabia

ABSTRACT

The study aimed at presenting a proposed model to raise awareness of cybersecurity among computer teachers in public education based on a set of previous studies, the most important of which was carried out by the researcher. The descriptive analytical approach was used to achieve the goal of the study, based on the nature of the study and its questions. The study concluded in its results that enhancing cyber awareness is based on educational training through identifying training needs related to cybersecurity and building and implementing training programs. In addition, the continuous training of the staff on duty is fruitful in raising awareness of cybersecurity hand in hand with holding effective partnerships in the field of information culture and information and cyber security. The study also identified a set of axes that contribute to raising awareness of cybersecurity through an analysis of existing and potential risks as well as indicating intended and unintended information crimes and measures that can be executed about them, and how to prevent and manage crises related to cybersecurity. Moreover, the study presented a set of ways and procedures through which to preserve cybersecurity through a set of basic security elements and means of awareness and digital culture, and finally establishing measures to build policies and legislation that guarantee the preservation of cyber security. The study recommends building educational specializations to teach information and cyber security, building curricula related to information and cyber security, and a continuous updating of the expected risks that may occur on cybersecurity and the development of plans facing them and crisis management and prevention plans. The study presented a suggested model based on its results and through reviewing previous studies aimed at raising awareness of cybersecurity among computer teachers in public education.

KEY WORDS: CYBER SECURITY, PUBLIC EDUCATION, COMPUTER, INFORMATION SECURITY, A SUGGESTED MODEL.

ARTICLE INFORMATION

*Corresponding Author: aalyateem@hotmail.com
Received 30th Oct 2020 Accepted after revision 17th Dec 2020
Print ISSN: 0974-6455 Online ISSN: 2321-4007 CODEN: BBRCBA

Thomson Reuters ISI Web of Science Clarivate Analytics USA and Crossref Indexed Journal

NAAS Journal Score 2020 (4.31) SJIF: 2020 (7.728)
A Society of Science and Nature Publication,
Bhopal India 2020. All rights reserved
Online Contents Available at: http//www.bbrc.in/
DOI: http://dx.doi.org/10.21786/bbrc/13.4/97

INTRODUCTION

Cyber security is among the main challenges that has emerged with the accelerating development and progress of technology. By definition, it means that we must protect the conduct of cyber operations, protect data and applications, and preserve and maintain national information for individuals and the state. That is, to prevent any unauthorized entry or any tampering with data. Therefore, it is necessary to build a strong system that

protects these services and information that this beautiful technology provide us with through the cyberspace. As well, we should work on teachers' awareness, especially computer teachers. Indeed, cybersecurity has become the talk of the whole world, and has even become a political part of any other security, economic or political policies, as decision makers in various countries have put cybersecurity issues as a priority in their policy (Al-Otaibi, 2017).

As the cybersecurity becomes a subject of increasing public interest and research efforts, more and more studies that examine the roles of male and female teachers in particular have been conducted. These studies treat different subjects such as setting rules in the curriculum and classes to understand cybersecurity clearly, empowering students with problem-solving skills, providing peer counseling, and educating parents about cyber security through parent meetings and newsletters. However, cybersecurity is a very recent research topic in the Arab world that has not received enough attention at the level of scientific research. Nevertheless, it is not possible to neglect some of the few efforts, especially in the educational field and among teachers since it is one of the most important competencies for computer teachers. So, the current study is interested in finding a model to raise awareness of cyber security among secondary stage computer teachers in Jeddah.

The study issue: Through the experience of the researcher in the field of computers and based on his knowledge of previous studies, and based on his previous published study (Alsahafi, 2019) about the level of cybersecurity awareness among computer teachers in the education department of Jeddah and its results and recommendations according to the application of its curriculum and answering its questions and checking the validity of its hypotheses, the researcher decided to take advantage of these previous data to build a proposed model aiming at raising awareness of cybersecurity among computer teachers in public education by analyzing the results of his previous studies and inferring from previous studies and literature. The study seeks to answer the following question: "What is the suggested model for raising awareness of cybersecurity among female computer teachers in the Education Department in Jeddah Governorate?"

Previous Studies: Alsahafi's study aimed at identifying the level of cybersecurity awareness among secondary stage computer teachers in the city of Jeddah. The study community consisted of all computer teachers of the secondary stage in Jeddah for the academic year 1440 AH-2019 CE and their number was (352) teachers according to Jeddah Education Department statistics. The study sample consisted of (106) Female teachers. The quantitative method was used according to the study issue, questions, and nature. A questionnaire was used as a data collection tool. The study found in its results that there are weaknesses and limitations among computer teachers both in awareness of concepts of cyber security and in awareness of the level of cybersecurity. In addition, there is an absence of statistically significant differences between average responses of study sample individuals at the level of significance (≥ 0, 05) in the degree of cyber security awareness of computer teachers. This was due to the current study variables (years of experience - educational qualifications - training courses). The study recommended mainly:

1. The provision of free in-depth training programs in cybersecurity for computer teachers on top of work.
2. Attaching female teachers to diplomas in cybersecurity to raise their level of understanding, awareness and application.
3. The integration of cyber security in local educational programs.
4. Issuing and distributing circulars related to regulations and legislations developed for cybersecurity to all schools.
5. Integrating regulations and legislations within the code of career behavior.
6. Paying more institutional attention to educational seminars and training workshops that highlight the importance of developing cybersecurity.
7. The use of the Ministry of Education experts to develop cybersecurity tools in various educational institutions.

The study of Al-Ghadian et al., (2018) also aimed at revealing the most important forms of electronic blackmail crimes, their motives and their psychological effects from the viewpoint of teachers, Authority members and psychological counselors. The sample of the study consisted of (523) members divided into three groups: The first comprised the (48) members of the authority for the Promotion of Virtue and Prevention of Vice. The second consisted of (48) psychological counselors. The third was formed by (368) randomly chosen male and female teachers. To achieve the study objectives the researchers used three self-prepared criteria including the criterion of electronic crime images, the criterion of electronic crime motives, and the criterion of psychological effects of electronic blackmail after checking their psychometric characteristics.

The results indicated that there are statistically significant differences in the physical, emotional, and entertainment motives among the psychological counselors and the teachers in favor of the teachers, and between the teachers and the authority members in favor of the teachers. As for the differences in sexual motives, they were between the teachers and the authority members in favor of the authority members. Finally, the results of the study showed that there are statistically significant differences

in the degree of estimating the psychological effects of crimes of electronic blackmail due to the difference in the respondent category (male and female teachers and psychological counselors), and the differences were between psychological counselors and teachers in favor of psychological counselors.

Abdel Majid (2018) studied Cyber security is an urgent necessity for community security: The Safe Family Proposal for Educating the Arab Gulf Society in Information Security for Both Students and Parents aimed at revealing the role of parents in protecting their children from the threat of hacking and electronic blackmail. This study made a comparison between many families, parents and children, who had the opportunity to be properly qualified to use these technologies, and those families who were not trained to do so. This comparison was in order to identify the role of parents in protecting their children from electronic hacks.

The study found that there is a very important role for parents in protecting their children from electronic threats, including cases where children have an adequate level of education in dealing with this new technology. Therefore, the researcher has put forward a qualifying proposal for preserving the electronic privacy of male and female students, which includes all categories of public and private education, in addition to a program for qualifying both parents. This program seeks to contribute to the raising of the society security culture and the protection of children against this urgent danger.

Al-Shammari (2015) carried out a study on strategic vision to protect the cyberspace of the Kingdom of Saudi Arabia which aimed at: a) Clarifying the concept of cyberspace, its limits and its characteristics. b) Defining the electronic gap. c) Reviewing the reality of cyberspace in the Kingdom of Saudi Arabia. d) Explaining the dangers of cyberspace. e) Clarifying the awareness of those responsible for information security. f) Clarifying the obstacles that hinder the Kingdom's ability from confronting the dangers of cyberspace. The researcher used the descriptive analytical approach and Content analysis in addition to the deductive inductive approach. The study found that there are some risks that threaten the cyberspace of the Kingdom of Saudi Arabia. In addition, there are limits of the awareness of those responsible for information security in the Kingdom of these risks. It also found that there are many obstacles hindering the Kingdom's ability to confront those risks.

Recently, Nakama and Paullet (2018) aimed at teaching students at all university academic levels how to face cyber-attacks. The study indicated that there is another important set of key skills in the dynamics of online courses in the first university stages to overcome their contextual limitations: (1) Learn how to navigate the learning management system. (2) Send and receive messages effectively between students and faculty members. The study contributed to the students 'acquisition of online learning strategies because students may feel that they are unable to complete academic assignments without assistance, which can threaten their self-value. As a result, many college students fail to seek the needed help, considering it as embarrassing, accepting defeat, and something that can be avoided whenever possible. Through the success of the program, the study contributed to develop cybersecurity among university students among all academic levels.

Goran (2017) studied "Cyber Security Risks in Public secondary" which was aimed at analyzing cybersecurity problems in a public secondary school and suggest practical solutions. A sample of secondary schools was used through the case study methodology. The result of this paper was a case study on an urban secondary school and its weaknesses in front of various electronic attacks through clarifying the dangers of electronic attacks and how to prevent them.

METHODOLOGY

Based on the nature of the study, its issue, and its goals, the analytical method was used to analyze the data of previous studies and the study previously conducted by the researcher on the topic of cybersecurity awareness among computer teachers in the Education Department in Jeddah Governorate. It also used the focus groups method in order to amend and validate the proposed model presented by the study through a group of seven experts in the field of computer, information and cyber security.

RESULTS AND DISCUSSION

Through his previous study (Alsahafi, 2019) reached a set of statistical results that need to be enhanced in the proposed model because of their low application level through the previous study method:

First: Computer teachers' awareness of the concept of cyber security in Jeddah.

Table 1. The level of awareness of the Cyber security among computer teachers in Jeddah education department

Paragraph No	Paragraph Text	SMA	Standard Deviation	Response level
1	I know the risks of opening links and email attachments.	2.53	1.21	Medium
2	I have a solid knowledge of the concept of social engineering.	2.48	1.35	Medium
3	I know the risks of smart phone viruses.	2.34	1.14	Medium
4	I have an understanding of the concept of phishing (fraud) online.	2.21	1.08	Medium

Other phrases like: (I have full knowledge of the concept of social engineering - I have knowledge of the risks of smart phone viruses - I have knowledge of the concept of phishing (electronic fraud) got lower degrees in their average due to the lack of coverage of those concepts at the school community and by public media in contrast to other common concepts and terms that teachers know, although, without a precise definition of their dimensions.

Second: Computer teachers' awareness of ways to preserve cyber security systems in the city of Jeddah:

Table 2. Computer teachers' awareness of ways to preserve cyber security systems in the city of Jeddah

Paragraph No	Paragraph Text	SMA	Standard Deviation	Response level
1	I am aware of the features needed to create a good password when entering websites.	2.34	1.14	Medium
2	I use the same password for all social media and email.	2.18	1.48	Medium
3	Use the same password for the websites I need to conduct financial operations like bank websites and online shopping websites.	2.20	1.35	Medium
4	I know the danger of sending a password via e-mail.	2.11	1.44	Medium
5	I change the password regularly.	2.02	1.39	Medium
6	I read user agreements of free software before pressing "I agree".	1.95	1.14	Low
7	There is a separate law for cybercrime in Saudi Arabia.	1.87	1.48	Low
8	There are laws and regulations for cyber security in Saudi Arabia.	1.74	1.35	Low

The phrases (I read user agreements for a free program before pressing "I agree" - there is a separate law for cyber crime in Saudi Arabia - there are laws and regulations for cyber security in Saudi Arabia) got a low degree. This may be due to the fact that computer teachers perform many procedures and processes related to dealing with Software and computer applications, which leads them not to read the agreements and conditions of each program that they download and install on their devices. In addition, there was a lack of knowledge of the classifications of laws and legislations related to cybercrime. The result was expected, as it is common in societies and not limited to computer teachers who should be keen to understand the terms of the agreements.

3- A suggested model for raising awareness of cybersecurity among computer teachers in public education:

Preface: Based on the application of the study methodology, the results and recommendations that were presented, and through an analysis of the results of the previous study related to the topic that the researcher previously performed, and what was seen from previous studies that discussed the study topic, the researcher reached the following model, which was reviewed by experts who were chosen to discuss and amend it so as to reach its final wording as follows:

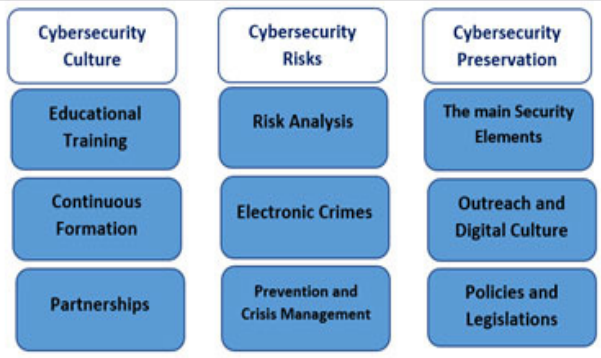
Vision: Reaching a public awareness that helps in achieving and enhancing cybersecurity, and clarifying some practical solutions through which information and cyberspace can be protected in relation to the growing threats and risks facing this vital field.

The objectives of the proposed model: The goals of the proposed model are:

1. Raising awareness of cyber security among computer teachers
2. Raising awareness of the importance of cybersecurity
3. Cybersecurity continuous training and formation
4. Identify partnerships related to raising awareness of cybersecurity
5. Factors affecting cyber security
6. The dangers of poor cybersecurity
7. Methods of preserving cyber security

The suggested model for raising awareness of cybersecurity for computer teachers in public education:

Figure 1



The first chapter: Cybersecurity culture

Educational training: It includes the following procedures: Analysis of training needs in the field of cybersecurity Determine minimum skills in cybersecurity Building training programs related to cybersecurity

2. Continuous Formation:

It includes the following procedures: Identify appropriate educational and specialized needs for cybersecurity Preparing internal and external scholarship plans and programs Identify continuous formation specializations related to cybersecurity Building systems and procedures that regulate continuous formation in a way that motivates female teachers Prepare training plans, select trainers, and schedule programs

3. Partnerships:
It includes the following procedures: Identify areas for partnerships in spreading a cybersecurity culture Identify cybersecurity relevant agencies and partners Build educational and training partnerships according to existing needs Build cooperation with relevant expertise agencies

The second chapter: cybersecurity risks:1. Risk analysis:
It includes the following procedures: Identify constant ongoing cybersecurity problems, and develop, remedy and update prevention plans Identify intended and unintended threats related to the internal and external misuse Identify and update global threats to cybersecurity Continuous perusal of security gaps revealed from time to time and keeping vigilant to dealing with them on time

2. Electronic crimes:
It includes the following procedures: Identify electronic crimes related to cybersecurity according to the legislation within the educational system or according to the system of electronic crimes related to cyber security Define procedures for dealing with electronic crimes according to their levels, whether dealing with them internally or externally as crimes that need the intervention of the competent authorities Issue sanctions against electronic crimes related to cybersecurity and circulate them to employees and affiliates Continuous monitoring, technically and administratively, of everything that poses a threat with regard to electronic crimes.

3. Prevention and crisis management:
It includes the following procedures: Spreading digital culture and raising awareness regarding the risks related to cybersecurity periodically for employees and affiliates Continuous updating of ways to prevent cyber security threats through casual situations or others' experiences Preparing predictive studies related to cybersecurity threats in the areas of administration, technology, legislation, laws and policies Preparing crisis response and management plans as an anticipation for every emergency in the field of cyber security threats.

The third chapter: Cyber security Preservation: 1. The main security elements:
The main elements include: Confidentiality and security: it means ensuring that the information is neither disclosed nor viewed by persons who are not authorized to do so.

Integrity and content safety: It is to ensure that the information content is correct and has not been modified, and in particular, it has not been destroyed, altered, or tampered with at any stage of processing or exchange, whether in the stage of internal dealing with the information or by unlawful interference. Constant availability of information or service: It must ensure that the information system continues to operate and the ability to interact with information and provide service to informational sites, and that the user will not be subjected to use or access prevention to the system. Do not deny the information-related behavior of the operator: It is intended to ensure that the person connected to the information or its sites cannot deny that he has acted, so that the ability to prove this behavior is available and that a person at a certain time has performed it, as well as the inability of the recipient of a specific message to deny receiving this message.

2. Outreach and digital culture: Digital citizenship: It includes The following units:

Respect which includes the following three criteria: Digital Access: It means working towards providing equal digital rights and supporting electronic access. Digital Etiquette: standards for behavior and procedures through the use of technology Digital Law: It means digital responsibility for actions and deedsEducation:It includes three criteria as follows:

Digital Communication: Everyone now has the opportunity to communicate and collaborate with anyone else in any part of the world at any time.

Digital Literacy: Digital citizenship is based on teaching and educating individuals in a new way - taking into account the need of these individuals for a very high level of information literacy skills. Digital Commerce: It means that the citizen is aware of how to buy and sell electronically, financial transactions through the Internet, and knowledge of e-shopping behavior.

Protection: It includes three criteria as follows: Digital Rights & Responsibilities: it means the available laws and regulations in the use of technology. Digital Health & Wellness: which means mental and physical health in the world of digital technology. Digital Security (self-protection): It means procedures for ensuring electronic safety and protection Digital security education and awareness:

- Contributing to citizens' strong Islamic education according to the Islamic faith.- Enhancing national affiliation.- Enhancing security awareness among students regarding their safety from falling into security-related crimes, establishing the principle of social responsibility and deepening the concept of comprehensive security.- Giving the individual the skill of objective and critical thinking to distinguish between correct and wrong ideas.

- Enhancing the importance of order and legal culture for citizens so as they know their rights and duties and achieve preventive security.

3. Policies and legislation: The main elements include: Identifying the sources and references of policies related to cybersecurity Preparing the main chapters of cyber security legislation and policies Building policies and legislations related to cyber security based on the main elements previously prepared and stemming from references and sources related to information and cyber security. Preparing administrative and technical regulations related to the implementation of cybersecurity policies and legislation

8- Findings and recommendations: Based on the aim of the study and the application of its methodology, the study concluded in its results that enhancing cyber awareness is based on educational training by identifying training needs related to cybersecurity and building and implementing training programs. Moreover, continuous formation on top of work is fruitful in raising awareness of cybersecurity in addition to establishing effective partnerships in the field of information culture, information and cyber security. The study also identified in its results a set of principles that contribute to raising awareness of cybersecurity through an analysis of existing and potential risks as well as indicating intended and unintended information crimes and the measurements that can be implemented about them, and how to prevent and manage crises related to cybersecurity.

The study also introduced a set of ways and procedures through which to preserve cybersecurity by presenting a set of basic security elements and means of digital culture awareness, and finally establishing measures to build policies and legislations that guarantee the preservation of cyber security. The study recommends building curricula related to information and cyber security, and before that building educational specializations to teach information and cyber security, in addition to the continuous updating of the expected risks that may occur on cybersecurity and the development of plans to face them and crisis management and prevention plans.

REFERENCES

Alsahafi, Mesbah Ahmed (2019). The level of cybersecurity awareness for female teachers of secondary stage in Jeddah. Journal of Scientific Research in Education No. 20 c 10. 2019 m.

Al-Ghadian, Sulaiman Bin Abdul-Razzaq, Yahya Bin Mubarak Khatatba, and Ezzeddine Abdullah Awad Al-Nuaimi (2018). Pictures of cyber blackmail crimes, their motives and their psychological effects from the viewpoint of teachers, authority members and psychological counselors. Security Research Magazine: King Fahd Security College - Center for Research and Studies No. 27, p. 69: 157 - 227.

Al-Otaibi, Abdul Rahman Bajad (2017). The role of cybersecurity in enhancing human security. A master research that is not published. Naif Arab University for Security Sciences. Al Riyadh, Saudi Arabia.

Abdul Majeed, Nabih Tariq (2018). Cyber security is an urgent necessity for community security: a safe family proposal to educate the Arab Gulf community on information security for both students and parents. International Arab Journal of Informatics. Volume 6. Number (11). 2018 m.

Al-Shammari, Hamid Quneidh (2015) A strategic vision to protect the electronic space of the Kingdom of Saudi Arabia. A master research that is not published. Naif Arab University for Security Sciences. Al Riyadh, Saudi Arabia.

Nakama, Debra & Paullet, Karen (2018). Broadening Participation In Cybersecurity Education: Using An Intersectionality Lens To Uncover New Perspectives. Issues in Information Systems Volume 20, Issue 3, pp. 47-56, 2019.

Goran, Ion, (2017). Cyber Security Risks in Public High Schools.Student Theses. CUNY Academic Works. . http://academicworks.cuny.edu/jj_etds/5