Cybersecurity Awareness Level: The Case of Saudi Arabia University Students

Wejdan Aljohni[1], Nazar Elfadil[2], Mutsam Jarajreh[3]
Computer Engineering Department
Fahad Bin Sultan University
Tabuk, Saudi Arabia

Mwahib Gasmelsied[4]
Finance and Investment Department
University of Tabuk
Tabuk, Saudi Arabia

***Abstract*—Cybersecurity plays an important role in reliance on digital equipment and programs to manage daily lives chores including the transmission and storage of personal information. Therefore, it is a global issue in our growing society, and it becomes increasingly important to measure and analyze the awareness of it. In this paper, a questionnaire has been designed to measure the current level of cybersecurity awareness (CSA) among Saudi university students. Cybersecurity students' awareness level questionnaire has been adapted from few other previous cybersecurity awareness campaigns. In this questionnaire, a total of 136 students have participated in the survey. The questionnaire was collected to measure the cybersecurity students' awareness level through their knowledge, culture, and surrounding environment or through students' behavior by thee affected factors. These are: gender, location, and study department of the students. The study findings reveal that the students' awareness is in an average has no significant difference in cybersecurity awareness level between male and female students, but females show a bit more concern about cybersecurity. However, there is a clear and high awareness of students of computer and information technology departments compared to others. Moreover, urban students outperformed students in remote areas in awareness of cybersecurity. The survey results indicate that the study model has been effective in measuring students' awareness.**

***Keywords*—Cybersecurity; awareness; protection; internet; students; higher education; security awareness; survey; APAT**

I. Introduction

The huge technological revolution in every aspect of our everyday life, such as smart devices, smart homes, and smart cities, cybersecurity has become an important component of any information system as it includes all elements of computer/network security that secure devices from unauthorized access, changes and destruction of information systems [1]. Cybersecurity vulnerabilities are the elements that put a system or network at risk of being infected with malicious software. When one recognizes that a system was influenced by an assault, this illustrated that an assault on the framework occurred and being effective. This can be assumed that the system was powerless against the assault, then the expression vulnerability can be used to refer to the peculiarities or features of the framework that causes it defenseless and helpless against all assaults [2]. Malwares are shown all over internet services to influence devices daily and carry out assaults that render devices, networks and data vulnerable. Osterman's research survey discovered that eleven million malware differences were detected by 2008 and ninety percent of the malware derived from concealed downloads from trusted and prominent sites.

Network security is a huge referent question, yet its political significance emerges from associations with the aggregate referent articles of "The State", "The Society", "The Nation" and "The Economy" [3].

A. Statement of the Problem

IT represents all the technology available from hardware, software, and all applied techniques such as communication. IT risks can be classified into three main types; they are operational risks, security risks, and risks from the organization and people living within it. With the increase in the spread and use of the internet, those risks have increased [4]. In security risks, the computer infrastructures components may predispose a device at a risk, they include software, hardware, and network. Securing these three elements or components implies accountability that is utilized to detect malicious elements and a perimeter defense system. This system is used to defend and resist the breach of infrastructure by malicious elements. It has also an access control mechanism that is used for authorization of incoming/outgoing data.

On the other hand, college students are the most groups that use a network, and they are supposed to be the most aware group of cybersecurity, also cybersecurity awareness culture should be established at an early stage [5]. University students are on this stage which is edge to enter the workforce. There is a great variety in the quality, capacity, importance, and nature of the students' data, but no one denies the importance of preserving them and not changing, falsifying, or distorting them, and preserving data even exceeds to include their formats and arrangement. It is a very sensitive nature, and any slight change may cause many problems to the users. IT systems, cyber networks need special treatment as they contain numerous data for students; they should be maintained and kept confidential, otherwise they will be exposed to many threats. All universities need to secure their students data, avoid risks, and avoid all potential associated effects or at least minimize the effects of these risks [6]. The unawareness of students about threats and risks that can face them in cyberspace, can cause successful execution of such threats. Students should establish a culture of cybersecurity awareness before entering the workforce. One of the most important steps in this way is measuring the cybersecurity awareness of university students.

B. Research Objectives

The end user is seen as a weak link [7]. Therefore, if students are not aware enough to recognize a security threat, they cannot be expected to avoid it, report it or remove it. Students are on the edge to enter the workforce, should be prepared and aware of security risks to avoid being a victim of cybercrime. They need cybersecurity awareness. The aim of this study is to evaluate the level of information security awareness among KSA university students. Online security is important to any society because it is part of the world which is viewed as a global village. Thus, it must be at the beginning of every educational system to secure the safety within cyber environments.

C. Research Questions

Identifying the research questions is the first step that must be concise and clear. In the context of this study, the research questions are stated as follows:

- RQ1. How much do KSA university students know about information security?
- RQ2. Is there an impact of gender, study department, or residential area on awareness levels?

This paper is organized in 5 sections. An introductory was clearly elaborated in section 1. While section 2 contained the related work. The research method discussed in section 3. The survey result findings were thoroughly discussed in section 4. The review concludes by discussing research limitations and conclusion.

II. Related Works

A log analyst needs good cyber situation awareness to perceive malicious activity, comprehend the impact and type of threat, and predict future consequences. The paper of [8] describes the development and validation technique to measure log analysts' situation awareness, especially when it comes to practical examples. The validation was conducted in a realistic setting by forming two questionnaires designed for the two different roles in log analysis and during an exercise involving five professionals. The results suggest that the technique can be used to evaluate cyber situation awareness for log analysts to keep track of incidents. To address the same issue, a framework was proposed [9] to help network analysts to evaluate the security situation of the network and increase their awareness from three dimensions: threat, vulnerability, and stability, and merge the results at decision level to measure the security situation of the overall network.

In [10], the security awareness of data in the Middle East area, especially in educational environments such as undergraduate students, researchers, academic staff, and employees has been studied to analyze and identify the awareness level of IS in this environment. The results revealed that there is a clear lack of knowledge of IS principles, the participants do their daily work and practical application without the requisite knowledge and understanding of the importance of IS basics. The researchers were interested in investigating the impacts associated with security risks and the lack of the security awareness in the institutions. The paper set several recommendations to reduce the harms of this situation, the important one of these recommendations was through supporting the training and awareness programs as well as adopting all the necessary safety measures by academicians and employees of the institution to enhance the security and safety of their data. Other studies [11-13] focused on the analyzing and raising the awareness of cybersecurity on college students. Researchers [14] attempted to measure the level of cybersecurity parental awareness to protect their children. A quantitative data analysis was performed using statistical software.

In [2], employees are the most vulnerable links, they need cybersecurity awareness and training to protect themselves and the company against new evolving cyber-attacks. An (Analyze-Predict-Aware-Test) APAT based Model along with Algebraic Equation has been adopted in developing a proactive approach towards enhancing the cybersecurity by making employees aware of new forms of security threats and what measures to follow when a suspicious activity is identified. Other research [15, and 16] developed and validated a model which assists in reducing big data security and privacy risk caused by employee weakness.

In the research paper [17], the researchers investigated the cybersecurity awareness of the public people in Saudi Arabia. The investigation was based on various aspects and contexts including demographics, cybercrime awareness, cybersecurity practices, and incident reporting as well as, a quantitative online survey was used to collect information related to cybersecurity awareness among Saudi nationals. The results revealed that the Saudi citizens had a good knowledge of IT, but they have limited awareness of the threats associated with cybersecurity practices, cybercrime, and the organizations and government roles in guarantee information safety across the Internet. Additionally, Internet skills influence cybersecurity practices from the end users. The study recommended to develop a model to create cybersecurity awareness in the region to reduce cybercrime.

In the same field and in the Middle East region and in a different country other than Saudi Arabia, Fadi [3] discussed the need for security education, training, and awareness programs in United Arab Emirates. The study involved and focused on the chances of the fall victims to phishing, a comprehensive wireless security survey of access points in Dubai and Sharjah and the Radio-frequency identification (RFID) security awareness. These determinants and aspects have been studied and discussed in Emirati schools, universities, and private and government organizations. Many counter measures that enhance the security awareness among students and professionals in UAE were reported. Recently, a study conducted by Moti [18] was carried out in four countries Palestine, Slovenia, Poland, and Turkey. The aim was to investigate cybersecurity awareness, beyond the differences of the respondent's country or gender.

Many researchers, such as Ashish [19, and 20] set models to measure accurately cybersecurity awareness and enhance the level of effective information security measures taken against all types of attacks. These models defined awareness as a problem not a solution, to solve this problem, one must be able to measure it and promote the awareness level according to the

measurements. Dynamic model is superior to other models set by the researchers [5, and 21] because it was designed in a stepped structure with leveling standardization, applicable to all groups/levels and capability-based approach used. After displaying most of our research-related ideas, the researcher of the current study can conclude that there is a lack of addressing some of the concepts that authors must deal with in measuring and analyzing the cybersecurity awareness of university students in KSA, such as effects of gender, study department and residential area as affected factors in awareness level of cybersecurity; also, awareness analysis and measurements through knowledge, culture and surrounding environment or through student behavior.

Authors studied in-depth survey about the awareness of cybercrime amongst the people of Bangladesh [21-23]. The survey has been carried out through responses both the online and offline questionnaires. Statistical Package for the Social Sciences (SPSS) software was accompanied for detailed analysis. Based on this study, the results shown negative results about people which were unaware of standard practices for cybersecurity and the government which was not vibrant regarding cybercrime related issues.

The information warfare and security awareness grabbed a high research attention recently and will be the on the research scope of many information security researchers in future [21, 24], and, thus of significance of this work.

III. Research Methodology

A survey is formed and carried out to gather data of evaluating students' awareness about cybersecurity threats. The target subjects of the survey are KSA universities students, students need to be educated about security issues early, the earlier they are aware of Information Security vulnerabilities, the safer they will be in the future as they will be able to pay more attention to security matters and avoid engaging in illegal behavior. The location, gender, and department are all the possible variables that may affect the security awareness level of the students. Therefore, the sample who answer the questionnaire should be students from different departments and from different areas in KSA. The data of the students' responses will be used to determine how students are aware of the information security threats. To achieve this goal, this study uses of the research methods.

A. Research Design

This research used the descriptive and quantitative method of gathering data to offer a clear view of the security awareness level of the universities students and it guarantees the validity and reliability of the research. In the quantitative design, the descriptive statistics are used to indicate the scores' distribution using a few indices. Structured of the questionnaire was distributed manually. These methods are preferred because they are fast, suitable, and economic for each questionnaire. The main steps can be listed as follows: (1) Students from different Universities, gender, location, and departments were asked to take part of this survey, (2) Students were evaluated based on their responses, (3) Survey is carried out voluntarily and randomly, (4) The questionnaire required approximately 10 to 15 minutes to be completed, and (5) Survey was distributed in a period of 2 months.

B. Data Sources

Two sources of data collection were used in this study, the first is primary data sources which is the data were collected by developing a structured questionnaire to study, analyze and discuss Saudi university students' awareness of cybersecurity and their affected factors. In the questionnaire, 136 completed samples were collected, and the second is secondary data which is the data that were collected from websites, previous scientific research, books, journals, articles, and thesis. The main objective of collecting these data is to design a suitable, structured questionnaire that accommodates all aspects of the university students' awareness of cybersecurity.

C. Questionnaire Analysis

The research depended on the structured questionnaire as the main tool for data collection, which was distributed on the research's sample to fill the required information. In the questionnaire, there are 24 questions in the Survey. This questionnaire includes two directions, they are:

- Awareness through knowledge, culture, and surrounding environment, which covered by 11 closed questions.
- Awareness through student behavior, which covered by 13 closed questions.

The answers to all the questions were closed, cast in the positive direction for each direction and designed on 4 score Likert Scale from 1 to 4 values as follows: (a) Strongly Disagree= 1, (b) Disagree =2, (c) Agree= 3, and (d) Strongly Agree= 4. After the collection of questionnaires from respondents, the data were entered into the computer and processed by using the Statistical Package for the Social Sciences (SPSS V.20). SPSS is a widely used program for statistical analysis in social science. It is also used by market researchers, health researchers, survey companies, government, education researchers, marketing organizations, data miners, and others.

IV. Survey Results and Analysis

In this study, the data from the questionnaire answered by the Saudi universities' students are used to determine how students are aware of information security threats. This chapter presents the statistical results which were collected from the questionnaire responses. Data were analyzed using SPSS to compute various statistics. The responses were collected and recorded on tables to compute the frequencies and percentages of each question. Authors selected descriptive statistic as analytical approach for analyzing the collected data from the questionnaire.

A. Quantitative and Descriptive Analysis

The questionnaire was distributed, which includes two directions, they are: 1) Awareness through knowledge, culture, and surrounding environment (covered by 11 closed questions) and 2) Awareness through student behavior (covered by 13 closed questions). There are two influencing factors that were

considered; namely: (a) student gender, (b) student department or learning background.

Nevertheless, 136 samples were collected; Table I and Fig. 1 show the details. The answers to all the questions were closed and cast in the positive direction for each direction. The Likart scale was used for their analysis, Table II collected the answer to questions and the answers were as follows.

SPSS is used to extract the quantitative and descriptive analysis of these results. The arithmetic mean clearly indicates the trend in answering each question. Of course, mean values indicate the tendency of the respondents to the questionnaire to one of the four answers, and this is evident by the appearance of the top (Maximum) of the bell curve at or near a specific value. The thinner and higher the curve, the greater the conformity of the participants 'opinion towards a specific answer. Where, the standard deviation is a measure of the amount of variation or dispersion of a set of values. A low standard deviation indicates that the values tend to be close to the mean (also called the expected value) of the set, while a high standard deviation indicates that the values are spread out over a wider range.

B. Effects of Factors and Directions

To analysis the effects of factors and directions authors use the following procedures:

- Authors set three hypothesis that have determinant factors, they are Gender, Location and department, but the expectation that department will have high, direct and clear effects so, authors will investigate the effects of the department as in dependent factor, where location and gender as dependents together with department.
- The Stem-and-leaf plots are used which it is a method for showing the frequency with which certain classes of values occur. Also, plots window will fulfill this purpose; there are three different display options for boxplots: Factor levels together, Dependents together, and none. The Factor levels together and Dependents together settings only affect analyses with two or more numeric variables.
- Calculate the Pearson Correlation, is a statistic that measures linear correlation between two variables it's suitable to measure of the strength of a linear association between our two directions.

The windows or boxplot appearing in the form of the stem-and-leaf plots each of them show how many participants are associated with one of the factors in the answers, and indicate the distribution or concentration of the values of their answers in each question, and through that, it is possible to know the effect of the parameter in each question.

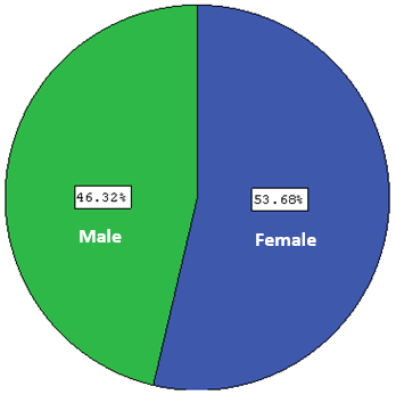
C. Answering Research Questions

This section summarizes and discusses the answers to the research questions.

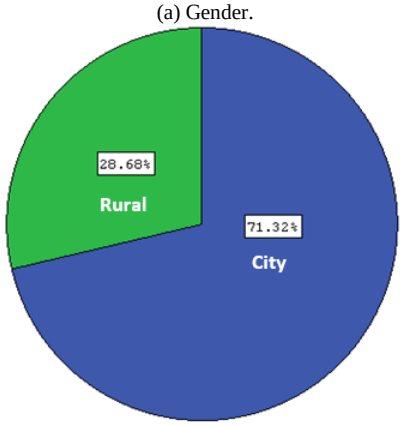
RQ1. How much do KSA students know about information security? The analysis of the collected questionnaires showed that students' awareness of urban cities about cybercrime greater than remote areas and the countryside (rural), of course, due to the availability of modern technologies.

TABLE I. FREQUENCY SAMPLES

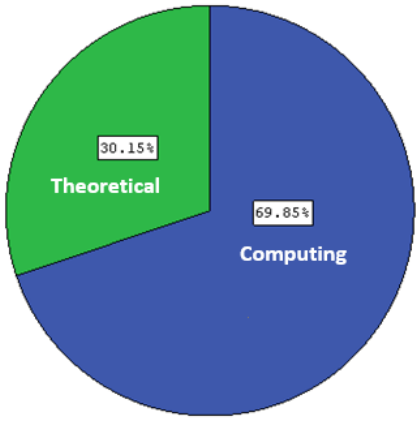
Location			***Department***			***Gender***		
Percent	***Frequency***		***Percent***	***Frequency***		***Percent***	***Frequency***	
71.3	97	***City***	69.9	95	***Computer***	53.7	73	***Female***
28.7	39	***Rural***	30.1	41	***Theory***	46.3	63	***male***
100.0	136	***Total***	100.0	136	***Total***	100.0	136	***Total***



(a) Gender.



(b) Location



(c) Department.

Fig. 1. Pie Chart of Samples, a) Gender, b) Location, and c) Department.

TABLE II. THE ANSWER OF SURVEY'S QUESTIONS

value	*1*		*2*		*3*		*4*	
	samples							
	%		*%*		*%*		*%*	
Q1	5.1	7	8.1	11	14.0	19	72.8	99
Q2	0	0	2.2	3	16.2	22	81.6	111
Q3	.7	1			2.9	4	96.3	131
Q4			4.4	6	5.1	7	90.4	123
Q5	2.9	4	6.6	9	13.2	18	77.2	105
Q6					.7	1	99.3	135
Q7							100.0	136
Q8	1.5	2	8.8	12	16.2	22	73.5	100
Q9	2.9	4	10.3	14	12.5	17	74.3	101
Q10	8.1	11	17.6	24	50.0	68	24.3	33
Q11	8.1	11	22.8	31	64.0	87	5.1	7
Q12			.7	1	20.6	28	78.7	107
Q13							100.0	136
Q14			5.1	7	66.2	90	28.7	39
Q15			80.1	109	9.6	13	10.3	14
Q16			27.2	37	4.4	6	68.4	93
Q17	3.7	5	22.8	31	16.9	23	56.6	77
Q18							100.0	136
Q19	3.7	5	12.5	17	32.4	44	51.5	70
Q20	11.0	15	11.8	16	59.6	81	17.6	24
Q21	30.9	42	61.8	84	3.7	5	3.7	5
Q22	9.6	13	51.5	70	21.3	29	17.6	24
Q23	41.2	56	31.6	43	16.2	22	11.0	15
Q24	13.2	18	35.3	48	27.2	37	24.3	33

RQ2. Is there an impact of gender, study department, or residential area on awareness levels? The female participated are more exclusive and more knowledgeable about cybercrime, and at the same time the knowledge of the computer department's affiliates increased on the theoretical departments. But, there is no clear effect of the relationship of the department with gender from the provided answers.

Nevertheless, both genders were fully agreed that increasing training will increase awareness, and the students of the computer department are more aware of the importance of training in increasing cyber.

It is worth to mention that Gender, Location, and Department have significant effects of the two (culture and behavior) direction. Students of the computer department are the most fortunate and the most knowledgeable, aware, and safe of cybercrime risks.

Finally, the Pearson correlation coefficient can take a range of values from +1 to -1. A value of 0 indicates that there is no association between the two variables. A value greater than 0 indicates a positive association; that is, as the value of one variable increases, so does the value of the other variable. A value less than 0 indicates a negative association; that is, as the value of one variable increases, the value of the other variable decreases. From SPSS the entering data give Pearson correlation coefficient between our two directions as +0.411, this mean the relation is Positive with medium strength of association.

V. CONCLUSION

The objective of this research study was to measure students' cybersecurity awareness level. The study elaborates on the literature related to cybersecurity awareness among university students. For this purpose, a questionnaire was developed. The proposed questionnaire focused on students' awareness as part of the information security concepts and intended to measure cybersecurity awareness level. Nevertheless, study findings indicate that students have had average levels of awareness regarding cybersecurity concepts. It is worth mentioning that students' awareness levels did not differ significantly in terms of gender, and student's class level, but female showed bit more concern about cybersecurity. However, there is a clear and high awareness of students of computer and information technology departments. This study recommends necessary policy measures to be taken by universities to ensure that students from all places have same level of cybersecurity awareness. The results show that urban students outperformed students in remote areas in awareness of cybersecurity.

Cybersecurity awareness is normally neglected by educational institutes. University students should be aware of the possible threats that can face them while using the internet. Therefore, a culture of awareness must be established for students to be able to identify possible threats. This culture should be establishing from an early stage. Furthermore, students should be well prepared and aware of security measures that users can apply to avoid being a victim of cybercrime.

REFERENCES

[1] N.Thakur and C. Y. Han, "An Ambient Intelligence-Based Human Behavior Monitoring Framework for Ubiquitous Environments," MDPI Information,vol.12,no.2,pp.81-107, Feb.2021.

[2] A.H.khan, P.Sawhney, S.Das, D.Pandey, "SartCybersecurity Awareness Measurement Model (APAT)," International Conference on Power Electronics &IoT Applications in Renewable Energy and its Control (PARC), February 2020. https://doi.org/10.1109/PARC49193.2020.236614.

[3] M. O'Connell " Cybersecurity without Cyberwar," Journal of Conflict and Security Law, vol. 17, pp.187-209, 2017.

[4] J. H.Pardue, P.Patidar, "Threats to Healthcare Data: A Threat Tree for Risk Assessment," Issues in Information Systems, vol XII, No. 1, pp. 106-113, 2011.

[5] S.E.Erol, S.Sagiroglu, "Awareness Qualification Level Measurement Model, " International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Dec. 2018.

[6] M.Jaber, M.Dhaini, A.Fakherddine, and R.A. Haraty. "A Novel Privacy-Preserving Healthcare Information Sharing Platform Using Blockchain," Security and Privacy Issues in IoT Devices and Sensor Networks. Advances in ubiquitous sensing applications for healthcare, pp.245-261. Elsevier, 2021.

[7] Thomason, "People -The Weak Link in Security," Global Journal of Computer Science and Technology Network, Web & Security, vol.13, Issue 11, 2013.

[8] P.Lif, M.Granasen, T.Sommestad, "Development and validation of technique to measure cyber situation awareness," International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), pp.367-379, June 2017.

[9] X.Rongrong, Y.Xiaochun, H.Zhiyu, "Framework for risk assessment in cyber situational awareness, " IET Information Security, vol. 13, Issue. 2, 2019.

[10] S.Al-Janabi, I.Al-Shourbaji, "A Study of Cybersecurity Awareness in Educational Environment in the Middle East, " Journal of Information & Knowledge Management, vol. 15, No. 1, 2016.

[11] E. B. Kim, "Information Security Awareness Status of Business College: Undergraduate Students," Information Security Journal: A Global Perspective, vol.22, pp. 529-551, 2013.

[12] M. O'Connell " Cybersecurity without Cyberwar," Journal of Conflict and Security Law, vol. 17, pp.187-209, 2017.

[13] Y.K.Peker, L.Ray, S.D.Silva, N.Gibson, C.Lamberson, "Raising Cybersecurity Awareness among College Students, "Journal of The Colloquium for Information System Security Education (CISSE), vol.4, no.1, September, 2016.

[14] N.Ahmad, U.Asma, W.F.P. Fauzi, Z.Othman, Y.Yeop, S.Noru, "Cybersecurity Situational Awareness among Parents," Cyber Resilience Conference (CRC), Nov. 2018.

[15] P.Potgieter, "The Awareness Behaviour of Students On Cybersecurity Awareness by Using Social Media Platforms: A Case Study at Central University of Technology, " Kalpa Publications in Computing vol.12, pp. 272-280, Proceedings of 4th International Conference on the Internet, Cybersecurity and Information Systems 2019.

[16] L.Hadlington, "Employees Attitude towards Cybersecurity and Risky Online Behaviours: An Empirical Assessment in the United Kingdom," International Journal of Cyber Criminology, vol. 12, Issue 1, June 2018.

[17] F.Alotaibi, S.Furnell, I.Stengel, M.Papadaki, "A survey of cyber-security awareness in Saudi Arabia," 11th International Conference for Internet Technology and Secured Transactions (ICITST), Dec. 2016.

[18] M.Zwilling, G.Klien, D.Lesjak, Ł.Wiechetek, F.Cetin, and H.N. Basim, "Cybersecurity Awareness, Knowledge and Behavior: A Comparative Study," Journal Of Computer Information Systems, vol. 60, 2020.

[19] A.Malviya, G.A. Fink, L.Sego, B.Endicott-Popovsky, "Situational Awareness as a Measure of Performance in Cybersecurity Collaborative Work," Eighth International Conference on Information Technology: New Generations, April 2011.

[20] M.Evangelopoulou, C.W. Johnson, "Empirical framework for situation awareness measurement techniques in network defense," International Conference on Cyber Situational Awareness (CyberSA), pp. 234-238, June 2015.

[21] S.Tirumala, M.R.Valluri, G.A. Babu, "A survey on cybersecurity awareness concerns, practices and conceptual measures," International Conference on Computer Communication and Informatics (ICCCI), Jan. 2019.

[22] N.Ahmed, U.Kulsum, M.I.Bin Azad, A.S.Zaforullah, M. E.Haque, M.S.Rahman, "Cybersecurity Awareness Survey: An Analysis from Bangladesh Perspective," IEEE Region 10 Humanitarian Technology Conference, Dhaka, Bangladesh, pp. 564-569, 2017. https://doi.org/10.1109/R10-HTC.2017.8289074.

[23] N.Ahmed, M.R.Islam, U.Kulsum, M. Rajibul, M. Haque, M. Rahman, "Demographic Factors of Cybersecurity Awareness in Bangladesh," 5th International Conference on Advances in Electrical Engineering (ICAEE), pp.923-928, Dhaka, Bangladesh, 2019.

[24] R.A. Haraty, "C2 Secure Database Management Systems - A Comparative Study," Proceedings of the ACM Symposium on Applied Computing. San Antonio, TX. March 1999.