An Approach To Weigh Cybersecurity Awareness Questions In Academic Institutions Based On Principle Component Analysis: A Case Study Of Saudi Arabia

Adamu Abdullahi Garba, Fathe Jeribi, Ibrahim Al-Shourbaji, Mohammed Alhameed, Faheem Reegu, Sophia Alim

Abstract: Cybersecurity knowledge is among the essential elements for both public and private organizations and individuals due to the advent of online activities that pose a threat to critical organizational information. Researchers have conducted much research to provide a solution on how to increase the level of cybersecurity awareness. The methods used by various researchers include qualitative, quantitative, or mixed-methods approaches to determine the level of cybersecurity awareness. This paper aims to identify the most critical questions asked using the quantitative approach as it is the most commonly used method. The paper examines a dataset used in the work of Al-Janabi and Al-Shourbaji using an unsupervised machine learning technique known as Principal Component Analysis (PCA) to identify the most critical questions. The result from the analysis indicates that only the first six PCs have eigenvalues greater than 1, which means that these components (i.e., questions) are the most crucial to be used in identifying the most accurate level of cybersecurity awareness. Furthermore, the result provides a new dimension of questions to be used in determining the awareness level as it has been verified using the PCA technique. The paper also gives further recommendations on how to increase the level of cybersecurity awareness among both the public and private sectors.

Index Terms: Cybersecurity awareness, Principal Component Analysis, Unsupervised machine learning, Quantitative analysis.

1 INTRODUCTION

The world has become globalized where Information and Communications Technology (ICT) plays a crucial role in the daily activities of an individual and has made our lives convenient and more comfortable [1]. Technology has become an integral part of human life, and its benefits are clear, e.g. allowing one to keep in touch with their distant relatives and friends through social platforms like Facebook. Communication has also become faster as platforms such as Twitter allow discussion of the most current and trending topics in real time. Another benefit of technology is online education, which enables the acquisition of knowledge at your own convenient time and place. However, people keep their private information on digital media such as social media, which could lead to a threat to such information.

In this situation, ensuring that the data is kept safe and cannot be accessed by any unauthorized person is vitally important. Unfortunately, most people are not aware of the importance of cybersecurity aspects, thus they keep their private information on such media channels without any hesitation. In addition, there are other ways in which the confidential information of an individual can be accessed, e.g. the official websites of businesses where people shop online and give their contact details. Several developments and training programs were established in an attempt to contain the impact of breaches or attacks. The National Initiative for Cybersecurity Education (NICE) was created to improve the long-term cybersecurity posture of the USA [2], where the NICE aimed to address awareness, formal education, professional training, and workforce structure. In the UK, enhancing cybersecurity education and skills is one of the four main components of the 2011 national program to secure cyberspace [3, 4]. UK cyber policy has incorporated cybersecurity at all levels of education, starting from the age of 11 years. In Saudi Arabia, the National Cybersecurity Authority (NCA) was established in 2017 to centralize cybersecurity controls. Concurrent with this, the National Cyber Security Center (NCSC) was established to serve as the arm for the technical and operational component of the NCA. The NCSC monitors supervisory control and data acquisition (SCADA) systems among government entities, specifically in the sectors of energy and industry [3]. With the increase of cyber incidents in the education sectors, the importance of cybersecurity has been revealed, as academic institutions are now a sensitive target for hackers. Due to financial loss and lack of security in data, cyber hacks are becoming common in the education sector. According to the key findings of the cybersecurity survey in the UK, the organizations within the educational sector have become the most prominent targets in terms of identified successful data breaches or attacks in 2020, as shown in Figure 1 [4]. Therefore, it is essential to specify the importance of cybersecurity awareness in an effort to help others to understand network security training and protection measures in academic institutions [5].

- *Adamu Abdullahi Garba: Department of Computer Science, Yobe State University Damaturu, Nigeria; adamugaidam@gmail.com*
- *Fathe Jeribi: Department of Information Technology and Security, Jazan University, 82822-6649 Jazan, Kingdom of Saudi Arabia, fjeribi@jazanu.edu.sa*
- *Ibrahim Al-Shourbaji and Faheem Reegu: Department of computer and network engineering, Jazan University, 82822-6649 Jazan, Kingdom of Saudi Arabia ;ialshourbaji, and freegu @jazanu,edu,sa*
- *Mohammed Alhameed: Department of computer science, Jazan University, 82822-6649 Jazan, Kingdom of Saudi Arabia; malhameed@jazanu.edu.sa*
- *Sophia Alim: Independent researcher, Bradford, UK; sophiaalim66@gmail.com*

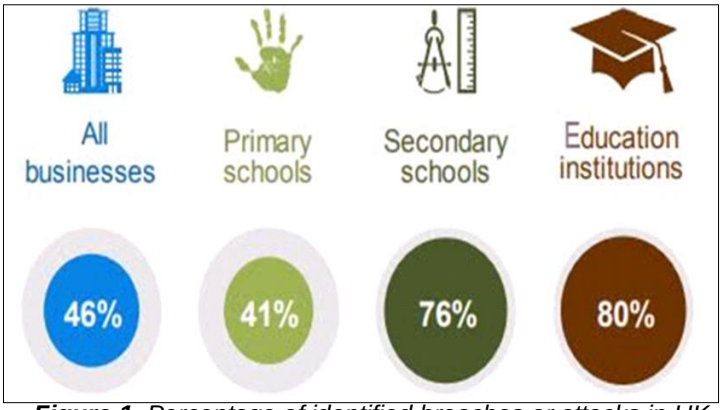


Figure 1. *Percentage of identified breaches or attacks in UK organizations.*

To understand the importance of cybersecurity awareness, King Abdullah Center for Science and Technology (KACST's), National Center for Cybersecurity Technology (C4C), as well as the Prince Mohammed bin Salman College for cybersecurity, artificial intelligence, and advanced technologies are educational institutions that were established encourage technology innovation and provide professional development to Saudi Arabia nationals [6]. These initiatives and investments helped improve cybersecurity capacity in academic sectors. The purpose of this paper is to assess the rate of cybersecurity awareness by implementing the concept of PCA to identify the most critical questions in respect to information security awareness in academic institutions within Saudi Arabia as a case study, as previous work has used the questions without implementing the PCA[7]. Although other researchers have adopted the questions, such as [8, 9,10], all these have directed, applied and interpreted the questions in their research without examining the most critical questions that fully represent information security awareness of the case studies. However, according to the knowledge of the researchers at the point of concluding the research, the PCA has only been applied in a study that identified Factors Related to Cyber Security Behavior by [11]. This research will help new researchers in cybersecurity to identify the level of cybersecurity awareness by applying the most significant questions of their academic staff, students and employees. The paper is organized as follows; In Section II, to familiarize the readers with the subject, we will cover the relationship between cybersecurity and educational instruction. In Section III, we will detail the methodology used to carry out this survey. In Section IV, we provide the experimental empirical result to determine the most critical questions in the dataset. Finally, in Section V, we will further elaborate discussion of the findings from the analysis, and then conclude the paper.

2 Background

In the current digital age, cybersecurity issues are one of the real problems having specific risks and threats. Despite the usual security threats, cyber-attacks are found to be a source of risk for students whose young and inquisitive minds often lead them to pursue information through improper online conduct. The consequences of cyber-attack may lead to adverse effects [12]. The importance of cybersecurity awareness within educational institutions can be notified by understanding the secure information carried out by computer systems such as student's personal information, identifiable information, and other policies. The author in [13] discussed that educational institutions have personal data of students such as medical records, biometrics, birth certificate, social security numbers, and any other important information that needs to be protected. Apart from this, educational institutions deal with credit cards and transactions that must follow security standards. In such a case, cyber-attacks will lead to privacy loss and breach of the laws and regulations of educational institutions [14]. According to S. Hina et al. (2020), security awareness helps to protect law enforcement and offers protection awareness for the student to access the system and resources securely. The educational sector, like any other sector, has witnessed the emergence of negative issues with the use of the internet. This is mainly due to the lack of awareness and low self-mechanism criteria. For this to improve, the author in [15] determined some measures to see how knowledge spreads in young children of South Africa. Fundamental cybersecurity life skills should be taught at primary school, delivered to all pupils, ensuring that awareness is raised in all genders equally. Cybersecurity awareness and resilience are too crucial for any government to leave to chance. On the other hand, in[16], the authors discussed the importance of cybersecurity education as the issue of cybersecurity which can help to protect against the illegal use of electronic data. It has been determined that educational sectors are under threat, and they are frequently a target for Ransomware. Because of this, some cases have been experienced related to data breaching [17]. Therefore, the educational sectors need to review their systems and adopt secure strategies for the improvement in data protection techniques and privacy policies. In the view of Venter et al. [18], the human error also leads to cyber-attack consequences; therefore, maintaining the staff and student privacy is the crucial requirement in the threat landscape, referring to cyber issues in the academic institutions of Saudi Arabia. In [19], the authors presented some cybersecurity measures that help to understand the management system and ways to secure the data by offering multi-pronged solutions. Considering the sense of security, the importance of data security for the specific demand of the educational practices such as campus wireless networking, online curriculum system, and student management system has been emphasized. With the help of data security, there might be less chance of facing data loss and risk disruption situations within academic institutions. On observing the threats observed in the educational sector, there is a need to provide strategic advice by applying practical approaches to security. Other than this, the management or educational authorities also help to align the security goals with the academic policies used in respective institutions. According to [20], the cybersecurity practices for the education sector help to assist risk management and direct the education sector to combat cyber threats. The work of [21] includes security awareness training by involving everyone in the network environment because students, teachers, and other staff are responsible for decreasing the risk rates. Over the years, cybersecurity awareness has been widely investigated in educational institutions. Since their systems need to be protected from a vast number of threats, which have become more sophisticated and aggressive than ever before, it is essential to regularly educate students/employees to adapt to the changes in technology and threats as well to meet the new requirements in the cyberspace. [22] confirmed that educating

people regarding cybersecurity has become a need in the current world to create cybersecurity experts. The authors in [7] conducted a study on cybersecurity awareness in the educational environment in the Middle East. This study focused on the need for such awareness by highlighting that although students are already using almost all social and digital media channels, they still have no clue on how to protect their data from getting hacked. The study made the need very clear by reflecting many cases of data being hacked. It also mentioned that employees entering the industry have no idea as to how they can take care of their company data from getting hacked, resulting in significant economic pain and suffering endured by these companies. The role of cybersecurity in Information Technology (IT) education was assessed [23], and it was found that this role has become crucial in IT education since hacking activities have increased over time. On the other hand, experts in IT must know how to protect such data from such hackers. IT education is becoming more focused because of the increased use of ICT in the organizations as well as in households. Businesses cannot survive without ICT, and they expand their businesses using official websites and social media accounts to reach a geographically spread audience. Therefore, it is more important to save their own and customers' data. A study on cybersecurity awareness among students was conducted [24] and it was found that such awareness helps ensure that the data is safe. It followed a quantitative approach, and they concluded that most of the students in their collected samples are not aware of how to secure their data. Information security awareness among undergraduate students in Kenya using a quantitative survey was evaluated [25]. Results demonstrated that despite the increased use of information technology in educational institutions, there is very little awareness regarding information security awareness among students in developing nations. It was found that students do not possess a sufficient understanding of information security, and there is a need to enhance such awareness. Hence, universities have to include such programs within their coursework. The authors' in [26] researched strengthening the students' learning on cybersecurity and found that the out-of-class learning strategy is a feasible pedagogical mechanism, which can result in various learning outcomes such as linking the learning to real-life with cybersecurity aspects. It has been known that educational institutions depend on technologies and computer networks to facilitate students through academics, courses, news, academic courses, and relevant information that is stored in the computer system[27]. Therefore, these computer systems and data storage devices need to be protected against several cyber threats. For this, there is a need to measure the awareness level of how much users are responsive towards computer viruses and cybersecurity bugs. For example, even if they have heard about phishing, some users are not sure how to recognize the problem or react appropriately. Research conducted by the Pew Research Center finds that many Americans are unclear about some key cybersecurity topics, terms and concepts. The 13 questions in the survey, a substantial majority of online adults were able to correctly answer only two of the manly 54% of the respondents correctly identified phishing attacks [28]. According to the Ponemon Institute report, human carelessness was the cause of 78% of cyber-attacks [29]. Parson et al. stated that naïve behaviour and accidental mistakes of computer users are the most frequent reasons for cybersecurity incidents [30]. Unaware employees may share sensitive information with unauthorized persons or inadvertently install malware, create weak passwords, or be the victim of the phishing attack. The Central Intelligence Agency (CIA) discovered that 47 government agencies had been compromised, and hackers had gained access to over 21 million government employee accounts [31]. Knowing the significance of information security awareness, training and education objectives are considered mandatory for the users, which covers all disciplines to reduce the risk of cyber-attack. Moreover, cybersecurity awareness in academic institutions prevents potential cybersecurity attacks and leads the students to recognize the threat.

3 RESEARCH MATERIAL AND METHOD

3.1 Material

In this work, the data from the study by-Janabi and Al-Shourbaji will be used. The authors used a questionnaire to obtain the level of cybersecurity awareness for the participants within a university located in the Kingdom of Saudi Arabia. The dataset consists of 26 questions where their answers were limited to "Yes" or "No". In terms of responses, 760 completed responses were collected. This dataset will be used for subsequent data analysis and assessments of this work.

3.1 PCA

PCA is a widely used method for identifying patterns in data of high dimensions [32]. It converts a set of p-associated variables into a smaller group called Principal Components (PCs). These PCs can be used to find the existing associations among variables in a compact manner. PCA removes unimportant information from the variables and keeps the variation present in the dataset.

The PCA model can be represented by:

$$\boldsymbol{U}_{m\times 1} = \boldsymbol{W}_{m\times d}\,\boldsymbol{X}_{d\times 1} \qquad (1)$$

Where u is an m-dimensional vector, which is a projection of x; the original d-dimensional data vector (m << d).

In the PCA method, the orthogonal basis can be calculated by finding the eigenvalues and eigenvectors, the eigenvectors $e_1, e_2 \cdots, e_m$ and the corresponding eigenvalues are $\lambda_1, \lambda_2, \cdots, \lambda_m$.

Let (S) denote a dataset w (of dimensions dxn) as a matrix, and each column in the matrix represents one dataset. N represents the number of data; d is the dimension for each record, and the covariance matrix (S) can be formulated as:

$$S = \frac{1}{n-1}\sum_{i=1}^{n}(x-\mu)(x-\mu)^T \qquad (2)$$

Where the mean vector of x is μ and T represents the transpose of the matrix x. The eigenvectors e_i can be found by solving the set of equations as

$$(S-\lambda_i I)_{e_i} = 0 \qquad (i = 1,2,3,\ldots,d) \qquad (3)$$

Where the eigenvalues of S are λ_i,. After calculating the

eigenvectors, they are sorted by the magnitude of the corresponding eigenvalues, the m vectors with the largest eigenvalues are selected, and the projection matrix is calculated based on:

$$W = E^T \quad (4)$$

Where E contains the eigenvectors as its columns and W is a $m \times n$ matrix.

PCA technique was widely employed for identifying inferences about the population and also in statistics and data mining series [33], [34]. Similarly, in the medical field, it has been used in lithofacies clustering [35] due to its capability in exploring and reducing high dimensional data in questionnaires and surveys [36]–[41]. PCA is used to determine the optimal set of questions, which in turn allow to explicitly identify the questions that provide full information for a specified number of questions and therefore, it will help in reducing the number of questions for data analysis.

4 EMPIRICAL RESULTS

The experiments have been carried out using SPSS 17.0 statistical software package. The PCA was employed to determine the most critical questions in the dataset, as shown in Figure 1. The scree plot can be used to show the variation between each PC. In the scree plot, the x-axis presents the component number (i.e., the question number) and the y-axis represents eigenvalues (i.e., the amount of variation).

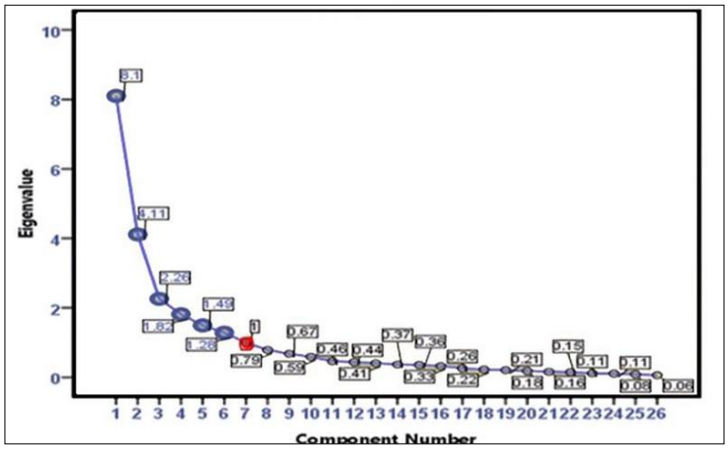
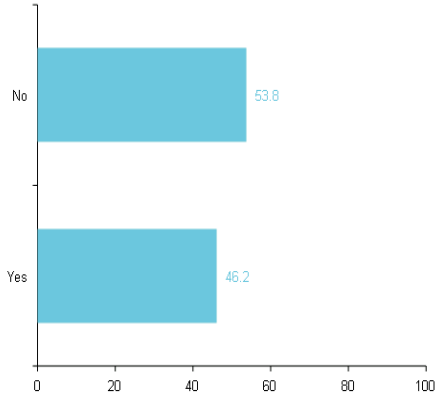
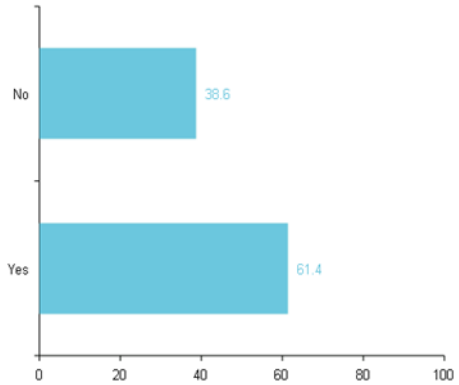


***Figure 2**. Scree plot for all questions used in the dataset*

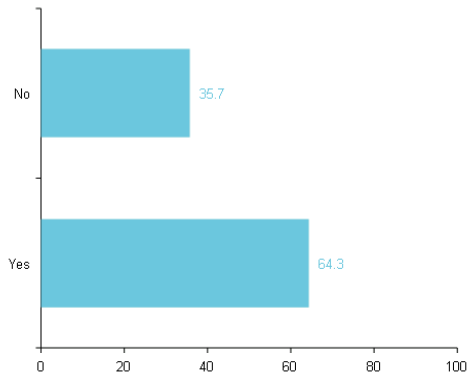
It can be seen that the first six PCs have eigenvalues greater than 1, which means that these components (i.e., questions) are the most crucial ones and they can be returned and used for further data analysis. These selected questions are summarized in Table 1, and the participants' responses to those questions are shown in Figure 3. The selected questions based on the PCA are provided in appendix A.



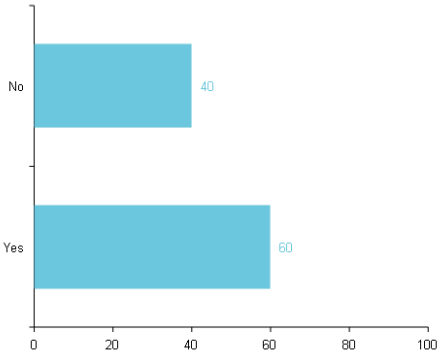
The number of respondents for question 1



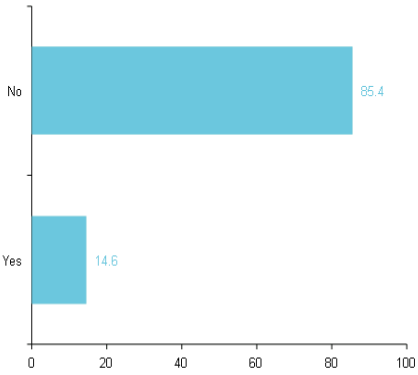
The number of respondents for question 2



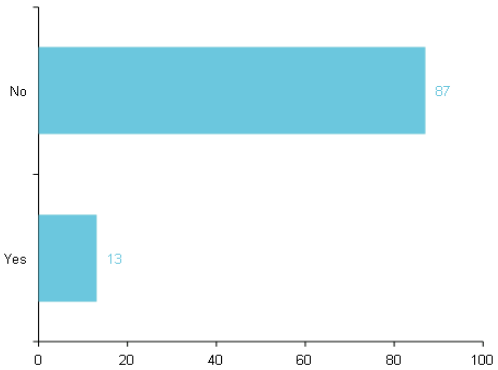
The number of respondents for question 3



The number of respondents for question 4



The number of respondents for question 5



The number of respondents for question 6

Figure 3. Participants' responses to the selected questions.

5 Discussion

This section elaborates more on the findings from the above analysis. As the objective of the research is to study the cybersecurity awareness level in an academic institution, PCA technique was implemented on the distributed questionnaire, where the target is to identify patterns in data of high dimension and also to better understand the dependency that exists between questions (variables).

The result illustrated in Figure 2 shows out of twenty-six questions, the PCA technique identified only six questions as the most important questions to be used in determining the information security awareness of a particular control group. These findings indicate that not all questions are relevant in identifying the cybersecurity awareness level. However, with the use of unsupervised machine PCA, researchers can specify the most relevant questions to be used in data analysis as it reduces the number of unwanted data by filtering the noisy data. The empirical result shows participants' understanding is more of a preventive approach.

The first question is related to cybersecurity in an academic institution because they faced some trouble in handling data in schools and colleges. Due to this, the respondents for cybersecurity awareness were asked questions related to the utilization of the encryption method or encryption software for the protection of sensitive information. In response to the question, “Did you try to use an encryption method or encryption software to protect your sensitive information?” 46.2% of respondents said "yes". It means they have used encryption software for data protection, and they have a little bit of knowledge about cybersecurity. Meanwhile, the remaining 53.8% of respondents are those who have not used any encryption software for data protection. This shows that fewer than one in two respondents have awareness about cybersecurity in the academic institution.

The next question is related to cybersecurity in an academic institution because, in academic institution, many teachers and other staff are involved in using debit cards and credit card for an outdoor payment. Due to this, the data of their cards can be used by hackers. In response to the question, “Do you use debit or credit card at an outdoor payment machine?” 61.4% of respondents said yes, they have use debit or credit cards for their outdoor payment. Still, 38.6% of respondents are unfamiliar with the utilization of the credit and debit card for their online payment. It represents that many respondents are unaware of the cybersecurity information along with the utilization of the debit or credit card. The third question of this study is related to cybersecurity in an academic institution because these institutions are struggling with different hacking problems. Moreover, a small number of people are aware of cybersecurity issues. There is a desire to learn about the various security perspectives. In response to the question, “Do you desire to learn more about security?” 35.7 % of respondents said "No" they did not want to learn about the security. Meanwhile, the remaining 64.3% responded "Yes", which means they are keen to learn about the security perspectives to protect their information. It shows awareness

of cybersecurity is necessary for educational institutes [42].The fourth question is related to cybersecurity in an academic institution because, in an academic institution, there are relatively low numbers of information security officers at present. In response to the question, “In your opinion, is it important that academic institutions have an information security officer?”, only 40% of respondents said that no there is no need for a high number of information security officers in the academic institution, mean the remaining 60% suggested that there must be an information security officer in the academic institution for the protection of data. It shows at there is a need for information security officers in academic institutions. These results are similar to the study of [43].

The fifth question is related to cybersecurity in an academic institution because there is a need to distribute credential information properly. This type of information will be sent through the mail, and many members of academic institutions are not involved in transmitting such data to the higher authorities. In response to the question “When receiving an e-mail which requires your credential information such as name, date of birth, age, your credit card number, do you respond to it?”, 85.4% of respondents said "No" they do not send their credential information when receiving an e-mail, leaving only 14.6 % of respondents who send their credential information with receiving e-mail. Most of the respondents are conscious about sharing their data with others.

The last question is related to cybersecurity in an academic institution because there is a need for complete information about this problem. If parents and teachers that are connected with academic institutions are not aware of cybersecurity, then they will face difficulties in the future. In response to the question “In case of receiving a phone call from an individual who says he/she is a student's father asking for his son or daughter’s marks, is it correct to provide that information to him?”, 87% of respondents indicated that it is not correct to provide information about the student's results and academic career as this information must remain confidential. Meanwhile, only 13% of respondents said that information regarding marks could be shared. All of these reviews of the respondent's show that is it is essential that the academic institution be aware of cybersecurity issues because the information must be kept confidential and not disclosed [44].

However, these questions can also serve as a new dimension on how to identify the level of cybersecurity awareness of any organization. Below are some recommendations to be taken into consideration when improving the cybersecurity awareness level of specific people or employees within educational organizations.

1. Identifying the target audience (organization)
2. Policy Creation and implementation of cybersecurity for the organization to follow.
3. Involve critical organizational stakeholders, such as executive-level management, and other departments during the planning process.
4. Identify and use free resources for awareness programs
5. Create or continue exercise programs that address cybersecurity issues and respond option
6. Create posters, newsletters, e-mail tips, blogs and reminders as different individuals learn differently
7. Deliberate cyber information sharing issues from the organizational level to state and national level for assistance response.

Academic institutions need to take a step toward a better level of awareness to ensure acceptance of such awareness program within their environments, which will help in mitigating the escalation of the cybersecurity risks. It is also essential that the academic institution have a clear vision and goals on addressing the safety measures with the coordination with standard bodies, governments and industry.

The COVID-19 pandemic has changed our daily routines and pushed organizations and individuals to embrace a new practice such as remote working which means people are spending more periods of time online. In turn, the number of un-employed people has also increased, meaning more people are sitting at home online. It is possible that some of these people will turn to cybercrime to support themselves, and the rate of cybersecurity will increase. Therefore, introducing and implementing a succession planning system under these circumstances became a paramount need for the universities as they can educate their students, employers and staff about the benefits of effective succession planning using a series of good content and tutor interaction and virtualized exercises for hands-on interplay.

6 CONCLUSION

The increased collection of digital data has dramatically changed the way organizations, companies, and industry sectors work, and it has a direct effect on our lifestyle. These data cannot be safeguarded easily, as the attack surface is continuously increasing and dynamically changing its attack form, while the security of the deployed primitives is not always retained. The work presented in this paper is a step towards understanding the level of cybersecurity awareness in academic institutions using a survey dataset used in one of the published works in the literature. PCA is used as a statistical data reduction technique to explore and identify linear relationships among the questions in the dataset. The result provides a new dimension of questions to be used in determining the awareness level as it has been verified using the PCA technique. The paper also provides some recommendations on how the level of cybersecurity awareness can be increased in both the public and private sectors.

Appendices

The selected questions based on the PCA analysis are provided in the following table.

Question number	Questions
1.	Did you try to use an encryption method or encryption software to protect your sensitive information?
2.	Do you use debit or credit card at an outdoor payment machine?
3.	Do you desire to learn more about security?
4.	In your opinion, is it important that academic institutions have an information security officer?

5. When receiving an e-mail which requires your credential information such as name, date of birth, age, your credit card number, do you respond to it?

6. In case of receiving a phone call from an individual who says he/she is a student's father asking for his son or daughter's marks, is it correct to provide that information to him?

REFERENCES

[1] R. Müller and C. H. Antoni, "Individual perceptions of shared mental models of information and communication technology (ICT) and virtual team coordination and performance-the moderating role of flexibility in ICT use,"Gr. Dyn., vol. 24, no. 3, pp. 186–200, Sep. 2020, doi: 10.1037/gdn0000130.

[2] "Cyber Security Breaches Survey 2020 - GOV.UK," 2020. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020. [Accessed: 10-Oct-2020].

[3] D. Upadhyay and S. Sampalli, "SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations,"Comput. Secur., vol. 89, p. 101666, Feb. 2020, doi: 10.1016/j.cose.2019.101666.

[4] "Critical security concerns for the education industry," 2020. [Online]. Available: https://resources.infosecinstitute.com/critical-security-concerns-for-the-education-industry/. [Accessed: 21-Oct-2020].

[5] S. Hina and P. D. D. Dominic, "Information security policies' compliance: a perspective for higher education institutions,"Journal of Computer Information Systems, vol. 60, no. 3. Taylor and Francis Inc., pp. 201–211, 03-May-2020, doi: 10.1080/08874417.2018.1432996.

[6] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, "A survey of cyber-security awareness in Saudi Arabia," in 2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016, 2017, pp. 154–158, doi: 10.1109/ICITST.2016.7856687.

[7] S. Al-Janabi and I. Al-Shourbaji, "A Study of Cyber Security Awareness in Educational Environment in the Middle East,"J. Inf. Knowl. Manag., vol. 15, no. 1, Mar. 2016, doi: 10.1142/S0219649216500076.

[8] A. A. Garba, M. M. Siraj, S. H. Othman, and M. A. Musa, "A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach,"Int. J. Emerg. Technol., vol. 11, no. 5, pp. 41–49, 2020.

[9] A. A. Gabra, M. B. Sirat, S. Hajar, and I. B. Dauda, "Cyber security awareness among university students: A case study,"J. Crit. Rev., vol. 7, no. 16, 2020, doi: 10.31838/jcr.07.16.108.

[10] A. Moallem, Cybersecurity Awareness Among Students and Faculty, vol. 2. Springer International Publishing, 2019.

[11] A. Kovacevic, N. Putnik, and O. Toskovic, "Factors Related to Cyber Security Behavior,"IEEE Access, vol. 8, pp. 125140–125148, 2020, doi: 10.1109/ACCESS.2020.3007867.

[12] F. E. Catota, M. Granger Morgan, and D. C. Sicker, "Cybersecurity education in a developing nation: The Ecuadorian environment,"J. Cybersecurity, vol. 5, no. 1, Jan. 2019, doi: 10.1093/cybsec/tyz001.

[13] M. S. Hermogeno, "Assessment on the Cybersecurity Awareness in Academic Institutions," 2019.

[14] H. Aldawood and G. Skinner, "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review," in Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, TALE 2018, 2019, pp. 62–68, doi: 10.1109/TALE.2018.8615162.

[15] M. Zwilling, D. Lesjak, S. Natek, and P. Anussornnitisarn, "HOW TO DEAL WITH THE AWARENESS OF CYBER HAZARDS AND SECURITY IN (HIGHER) EDUCATION?," 2019.

[16] A. Parrish et al., "Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-discipline," p. 19, 2018, doi: 10.1145/3293881.3295778.

[17] "How safe is your data? Cyber-security in higher education - HEPI," 2020. [Online]. Available: https://www.hepi.ac.uk/2019/04/04/how-safe-is-your-data-cyber-security-in-higher-education/. [Accessed: 21-Oct-2020].

[18] I. M. Venter, R. J. Blignaut, K. Renaud, and M. A. Venter, "Cyber security education is as essential as 'the three R's,'" Heliyon, vol. 5, no. 12, p. e02855, Dec. 2019, doi: 10.1016/j.heliyon.2019.e02855.

[19] J. Ricci, F. Breitinger, and I. Baggili, "Survey results on adults and cybersecurity education," Educ. Inf. Technol., vol. 24, no. 1, pp. 231–249, Jan. 2019, doi: 10.1007/s10639-018-9765-8.

[20] A. Irons, "Delivering Cybersecurity Education Effectively," 2019, pp. 135–157.

[21] N. Rahim, Z. Othman, F. Zakimi Hamid, O. Yeop Abdullah, U. Sintok, and T. Puteri Intan, "Cyber Security and the Higher Education Literature: A Bibliometric Analysis," 2020.

[22] J. Blair, A. Hall, E. Sobiesk, J. R. S. Blair, A. O. Hall, and E. Sobiesk, "Educating Future Multidisciplinary Cybersecurity Teams," Computer (Long. Beach. Calif)., vol. 52, no. 3, pp. 58–66, 2019, doi: 10.1109/MC.2018.2884190.

[23] D. C. Rowe, B. M. Lunt, and J. J. Ekstrom, "The role of cyber-security in information technology education," in SIGITE'11 - Proceedings of the 2011 ACM Special Interest Group for Information Technology Education Conference, 2011, pp. 113–121, doi: 10.1145/2047594.2047628.

[24] "International Journal on Emerging Technologies | Scopus Indexed - IJET | Research Trend," 2020. [Online]. Available: https://www.researchtrend.net/ijet/current_issue_ijet.php?taxonomy-id=82. [Accessed: 21-Oct-2020].

[25] J. Ndiege and G. Okello, "Information security awareness amongst students joining higher academic institutions in developing countries: Evidence from Kenya," African J. Inf. Syst., vol. 10, no. 3, May 2018.

[26] H.-J. Kam and P. Katerattanakul, "Enhancing student learning in cybersecurity education using an out-of-class learning approach," J. Inf. Technol. Educ. Innov. Pract., vol. 18, pp. 29–47, 2019, doi: 10.28945/4200.

[27] M. Plachkinova and T. Pittz, "Assessing the Awareness of Cybersecurity Within Entrepreneurship Students: The Cyberpreneurship Project," Entrep. Educ. Pedagog., p. 251512742091305, Mar. 2020, doi:

10.1177/2515127420913056.
[28] Aaron Smith, "What Americans Knows About Cybersecurity | Pew Research Center," 2017. [Online]. Available: https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/. [Accessed: 03-Nov-2020].
[29] Craig Mcdonalds, "A whopping 78% of small businesses are being targeted by cyber criminals: Here's how to stay ahead - SmartCompany," 2019. [Online]. Available: https://www.smartcompany.com.au/finance/fraud/cyber-crime-stay-ahead/. [Accessed: 03-Nov-2020].
[30] K. M. Parsons, E. Young, M. A. Butavicius, A. McCormac, M. R. Pattinson, and C. Jerram, "The influence of organizational information security culture on information security decision making," J. Cogn. Eng. Decis. Mak., vol. 9, no. 2, pp. 117–129, Jun. 2015, doi: 10.1177/1555343415575152.
[31] Julie Hirschfeld davis, "Hacking of Government Computers Exposed 21.5 Million People - The New York Times," 2015. [Online]. Available: https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html. [Accessed: 03-Nov-2020].
[32] H. Hotelling, "Analysis of a complex of statistical variables into principal components," J. Educ. Psychol., vol. 24, no. 6, pp. 417–441, Sep. 1933, doi: 10.1037/h0071325.
[33] D.J. Bartholomew, "Principal Component Analysis - an overview | ScienceDirect Topics," 2010. [Online]. Available: https://www.sciencedirect.com/topics/medicine-and-dentistry/principal-component-analysis. [Accessed: 03-Nov-2020].
[34] Jolliffe, "Principal Component Analysis | I.T. Jolliffe | Springer," 2010. [Online]. Available: https://www.springer.com/gp/book/9780387954424. [Accessed: 03-Nov-2020].
[35] Y. Z. Ma, "Lithofacies clustering using principal component analysis and neural network: Applications to wireline logs," Math. Geosci., vol. 43, no. 4, pp. 401–419, May 2011, doi: 10.1007/s11004-011-9335-8.
[36] J. Shlens, "A Tutorial on Principal Component Analysis," Apr. 2014.
[37] S. Vyas and L. Kumaranayake, "Constructing socio-economic status indices: How to use principal components analysis," Health Policy Plan., vol. 21, no. 6, pp. 459–468, Nov. 2006, doi: 10.1093/heapol/czl029.
[38] J. A. Barry, S. Mollan, M. A. Burdon, M. Jenkins, and A. K. Denniston, "Development and validation of a questionnaire assessing the quality of life impact of Colour Blindness (CBQoL)," BMC Ophthalmol., vol. 17, no. 1, Oct. 2017, doi: 10.1186/s12886-017-0579-z.
[39] K. Brosnan, B. Grün, and S. Dolnicar, "Identifying superfluous survey items," J. Retail. Consum. Serv., vol. 43, pp. 39–45, Jul. 2018, doi: 10.1016/j.jretconser.2018.02.007.
[40] M. Calamia, "Practical considerations for evaluating reliability in ambulatory assessment studies," Psychol. Assess., vol. 31, no. 3, pp. 285–291, Mar. 2019, doi: 10.1037/pas0000599.
[41] T. Lundgren and T. Parling, "Swedish Acceptance and Action Questionnaire (SAAQ): a psychometric evaluation," Cogn. Behav. Ther., vol. 46, no. 4, pp. 315–326, Jul. 2017, doi: 10.1080/16506073.2016.1250228.
[42] R. Chandarman, B. V. N.-A. J. of I. and, and undefined 2017, "Students' cybersecurity awareness at a private tertiary educational institution," scielo.org.za, 2017.
[43] E. Pavlova, "Enhancing the Organisational Culture related to Cyber Security during the University Digital Transformation," Inf. Secur. An Int. J., vol. 46, no. 3, pp. 239–249, 2020, doi: 10.11610/isij.4617.
[44] S. Burd, … C. U. T. C.-N. I. of, and undefined 2006, "Teh impact of information security in academic institutions on public safety and security: Assessing teh impact and developing solutions for policy and practice," ncjrs.gov, 2006.