WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Holistic Systematic Review on Methodologies of Assessing Effectiveness Cybersecurity Awareness Program

Adamu Abdullahi Garba[1], Nurdeen M. Ibrahim[2] , Joshua Abah[3], Mr. Ya'u Nuhu[4]

[1,2]Department of Cybersecurity and Data Sceince Nile University Abuja Nigeria.
[3]Computer Science & Dean of Faculty of Computing, Nile University of Nigeria
[4]Department of Computer science, Federal Polytechnic Damaturu
Email: adamu.abdullahi@nileuniversity.edu.ng

ABSTRACT—

Cyber-threat is now a global concern to all internet users, as the rate of crimes has tremendously changed from physical to virtual. Implementing awareness programs at various organization levels is required, also there is a need to know the methodologies used in measuring cybersecurity awareness program effectiveness. The paper aims to review and explore the previous methodologies applied, target organizations, and application of Machine Learning techniques in the assessment of awareness programs. Systematic literature review techniques were used to conduct the search using pre-defined keywords and published papers, the information was used in providing an answer to the research questions. The finding shows questionnaire was widely used as a method of evaluating cybersecurity awareness and also organizations implement more awareness programs, the gap found is the lack of using ML in assessing the effectiveness of design, implemented cybersecurity awareness programs.

Keywords— Cybersecurity, Security Awareness Assessment, Machine Learning

1. Introduction

The protection of critical information assets has become an organization's priority as most activities are performed online, therefore continues updating and improving the technology used to avoid cyber-threats (Dlamini et al., 2009). This has been possible as the result of the increase in high dependence on the internet, as of today there are about five billion people worldwide are using the internet. The 21century is regarded as the saturation stage of cybersecurity due to the high rate of cybercrimes. Sometimes the world cyber does not only refers to as technology but also a political idea that is cantered in the numerous technologies.

This threat has increased as the result of reliance on using smartphones device, which is particularly seen among young generation (Lau et al., 2017; Mi et al., 2020). This young generation has less knowledge on basic cybersecurity tips on how to protect themselves from any minor cyber threat. There are many smartphones available, therefore data can be easily breached and stolen (Allam et al., 2014) which increases security risk and causes a great threat to its users. Internet users' behavior when using the internet has an important role to play in either minimizing or increasing information security problems (Öłütçü et al., 2016) Cyberspace has been working as a financial marketplace, partisan background, and

also, as a social scene by utilizing the potential of the sector(Weishäupl et al., 2018). Organizations are required to adopt an optimized security measure that works within and outside the network to protect their sensitive information(Langer, 2017). Also to control access to critical infrastructure organizations need e The risk of security threats increases due to the lack of proper awareness which tends to increase security problems(Kim, 2014; Peker et al., 2016). The result of using a smartphone to access the internet and the affected people to cybercrimes keeps on increasing (EDUCAUSE, 2018). Hence, designing security awareness programs becomes crucial. Educational institutions can assist in implementing an action plan for educating students and other individuals as most were considered to be the "weakest link" in information security employees to be aware of cyber threats (Shaaban, 2014). Cybersecurity awareness programs should be a continuous process to keep updating with the new cyber threats, however, there are certain challenges associated with how to identify the effectiveness of cybersecurity awareness programs for youths.

Firstly, how to identify the acceptance of the concept of security and how to promote security culture within a workspace(Rantos et al., 2012). This challenge is often contributed to the behaviors of youth, whose cybersecurity knowledge is low but tends to ask an expert (S. Furnell, 2008).

Secondly, how to assess the message conveyed in an awareness program is enough or not? "Often one full size- fit all" is applied (Rahim et al., 2015). This can only be achieved when the program is tailored to the specific audience and to the cybersecurity knowledge required to change their mindset toward cybersecurity risk. This would help in delivering an effective cybersecurity awareness program to the intended audience. The most important aspect in delivering a cybersecurity awareness program is to change or tech certain concept which directly affects the behavior, with this, understating

the methods to identify the effectiveness of the program is significant. There are many methods available, however, selecting the appropriate one that suits the program is quite difficult and how to identify which method is frequently used. This research would review the current method in assessing the effectiveness of cybersecurity awareness programs and further see if machine learning techniques (ML) are used in assessing the effectiveness of cybersecurity awareness programs. This research would further help the researcher in applying these methods in assessing the effectiveness of cybersecurity awareness programs, also this would help other researchers to adopt the use of ML in analyzing cybersecurity awareness programs.

2. Methodology

Research Questions

The systematic literature review process was performed in obtaining selected papers, this method is widely accepting in conducted holistic review on a certain phenomenon as proposed by (Kitchenham, 2007; Kitchenham et al., 2009). This method consists of a predefined step-by-step method in conducting particular research. The steps in this method include the following:(Rahim et al., 2015).

- Step 1: Define the research question
- Step 2: Determine the data sources and search process
- Step 3: Define inclusion and exclusion criteria
- Step 4: Result of searching and data extraction
- Step 5: Discussion

Step 1: Define the research question

The review was carried out to find the answer to the following research questions.

- RQ1. What is the current method used in identifying the effectiveness of cybersecurity awareness programs?
- RQ2. What type of organizations implement cybersecurity awareness programs?
- What Machine Learning Technique is used in the assessment of the effectiveness of cybersecurity awareness programs?

Step 2: Determine the data sources and search process

The following known databases were used in searching relevant available papers in cybersecurity awareness programs and assessment methods, these databases include IEEE, Science Direct, Scopus, Emerald and Springer, and web of Science. The keyword used as search terms: “Cybersecurity assessment method”, “Security program”, Awareness education”, “Cybersecurity in ML”. The search was limited to the only article published from 2006 to date.

Step 3: Define inclusion and exclusion criteria

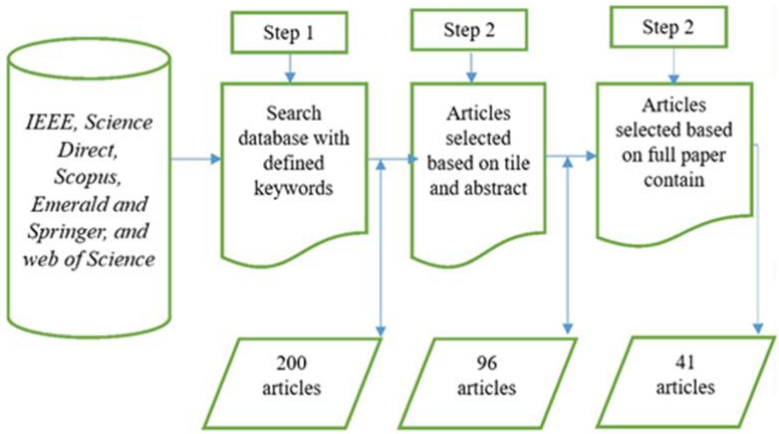
The following table 1 explains the inclusion and exclusion criteria applied in the research.

Research criteria

Included Article	**Excluded Article**
Fully available paper	Full text but not available
Year of publication from 2006 –date	Outside range of the year
focused on “cybersecurity awareness program”, “cybersecurity assessment method”	Were outside domain

Step 4: Result of Searching and Data Extraction

This section provides the search results from the database based on the search keywords. The section outline the identified articles, the table comprise of authors name, year, and tile. From the table other analyses such as identifying the current method used in identifying the effectiveness of cybersecurity awareness programs, organizations that implement cybersecurity awareness programs, and what Machine Learning Technique is used in the assessment of the effectiveness of cybersecurity awareness programs. A total of 48 articles was used based on the predefine key-words out of the many retrieve from the selected database, figure 1 below shows the processes that were followed in the data extraction phase.



Data Extraction Process

Research criteria

Au	Survey	Case Study	Questionnaire	Inter view	Focus Group	Game Tool
(Rahim et al., 2015)	✓		✓			
(Ahlan & Lubis, 2011)		✓	✓			
(Tsohou et al., 2008)		✓	✓			
(Al Shamsi, 2019)		✓		✓		
(Albrechtsen, 2006)		✓		✓		
(Albrechtsen & Hovden, 2010)	✓		✓			
(Bada & Nurse, 2019)		✓		✓		
(Charoen et al., 2008)		✓			✓	
(Charlie et al., 2006)		✓				
(Cheung et al., 2012)	✓		✓			
(Claar & Johnson, 2012)	✓		✓			
(Cone et al., 2007)	✓					✓
(D'Arcy et al., 2009)	✓		✓			
(Furman et al., 2012)		✓	✓			
(S. Furnell, 2008)	✓		✓			
(S. M. Furnell et al., 2007)	✓		✓			
(Hagen et al., 2011)	✓		✓			
(Hepp et al., 2018)			✓	✓	✓	✓
(Son et al., 2014)	✓		✓			
(Rantos et al., 2012)	✓		✓			
(Korovessis et al., 2017)	✓			✓		
(H. A. Kruger & Kearney, 2006)	✓		✓		✓	
(H. Kruger et al., 2010)		✓	✓			
(Labuschagne et al., 2011)		✓				✓
(Mani et al., 2014)	✓		✓	✓		
(McCrohan et al., 2010)		✓	✓			

(Monk et al., 2010)	✓		✓			
(Parsons et al., 2014)	✓		✓			
(Michael & Power, 2007)		✓	✓			
(Rezgui & Marks, 2008)	✓		✓	✓		
(Al-jerbie & Mohd Zalisham Jali, 2014)		✓	✓			
(Slusky & Partow-Navid, 2012)		✓	✓			
(Talib et al., 2010)	✓		✓			
(Beyer et al., 2015)		✓	✓			
(Wolf et al., 2011)		✓	✓			

Note: Au = author

Type of Organizations Implement Cybersecurity Awareness Program

AU	Organization	Home User	College	Normal user
(Ahlan & Lubis, 2011)			✓	
(Al Shamsi, 2019)			✓	
(Albrechtsen & Hovden, 2010)	✓			
(Albrechtsen, 2006)				✓
(Bada & Nurse, 2019)	✓			
(Burcu Bulgurcu, 2016)	✓			
(Drevin et al., 2007)	✓			
(Charoen et al., 2008)	✓			
(Charlie et al., 2006)	✓			
(Claar & Johnson, 2012)				✓
(Cone et al., 2007)	✓			
(D'Arcy et al., 2009)	✓			
(Eminağaoğlu et al., 2009)	✓			
(Furman et al., 2012)				✓
(S. Furnell, 2008)		✓		
(Hagen et al., 2011)	✓			
(Hepp et al., 2018)	✓			
(Caputo et al., 2014)	✓			
(Mani et al., 2014)			✓	
(Rantos et al., 2012)	✓			✓
(Korovessis et al., 2017)	✓			
(Kritzinger & Von Solms, 2010)		✓		

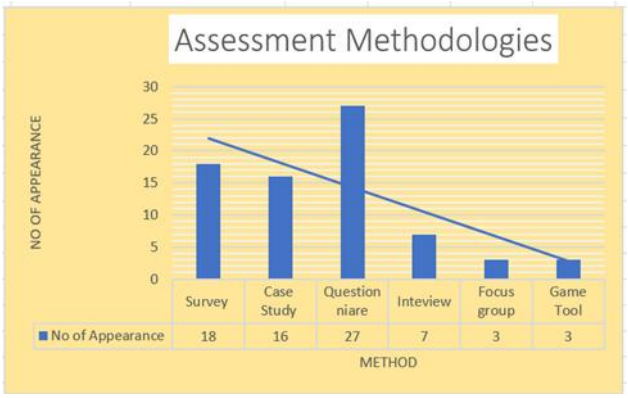
Discussion

This section clearly explains research questions formulated in this paper and discusses each question with its relevant justification.

RQ1 What is the current method used in identifying the effectiveness of cybersecurity awareness programs

The assessment of cybersecurity programs has gotten much attention from several researchers who have proposed many methodologies that are used in identifying the effectiveness of the program and how user level of understanding has increased due to the cybersecurity awareness program conducted. The currently identified method is used to know the effectiveness of an awareness program. Following the systematic review conducted and presented in table II, where it shows the identified method, authors, and year of the publication. Based on the table there are eleven independents

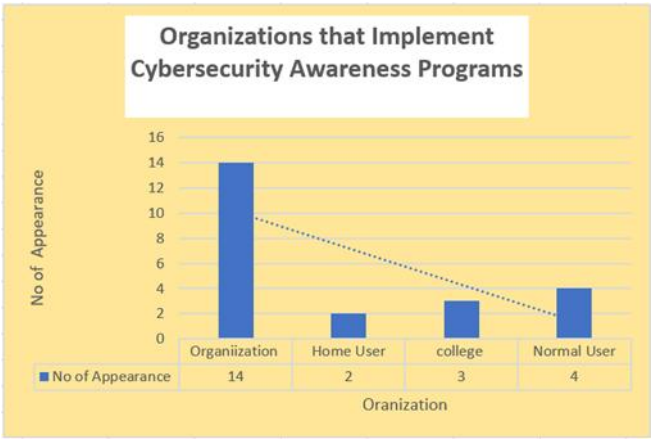
assessment methodologies by thirty-seven authors. These all identified can further be group into either qualitative or quantitative methods or approaches. Based on the table it has clearly shown the most used or trending method is the Questionnaire-based as figure 2 shows below with 27 occurrences. However, some researchers have used multiple methods to identify the effectiveness of (Ahlan & Lubis, 2011; Al Shamsi, 2019; Bada & Nurse, 2019; Burcu Bulgurcu, 2016; D'Arcy et al., 2009). This has indicated that cybersecurity awareness assessment can be obtained with the combination of more than one methodology, this would provide more non-bias, and also humans cannot be based simply on one type of method. Therefore, researchers can mix more than one method when trying to identify the effectiveness of the implement cybersecurity program as evaluating human behavior is quite complex. From the identified methods to the best of the authors' research, there are no assessments ever conducted using the program evaluation technique that follows a certain framework or guideline. Therefore, this shows no framework has been followed for designing any cybersecurity awareness program, and also no program assessments have ever been conducted during the design process before implementation. This pointed out the need for a framework that would guide researchers in designing an effective cybersecurity awareness program.



Assessment Methodologies Statistic

RO2. What type of organizations implement cybersecurity awareness programs?

This section would explain the type of organization that implemented cybersecurity awareness programs. The audience can be employees, students, or the community. This section is important as its details out where the previous studies have covered and where is left out. The research target is to find out if university students were considered in the previous research or not as they are the most vulnerable due to the high dependence on the internet(Johansson & Götestam, 2004). Figure4 has identified five major organizations that mostly implement cybersecurity awareness programs.



Assessment on an organization that implement cybersecurity awareness programs

Figure 3 Above shows the organization has the highest with 14 and the College has an only 2, this has indicated less focus on students' awareness. The objective of the research was to identify which organization has implemented the program, from the survey has indicated there are is less research in

this field. Therefore, more research is needed to be conducted for the student to be aware of cybersecurity. Few studies have covered this section (Slusky & Partow-Navid, 2012; Son et al., 2014)

RO3 What Machine Learning Technique is used in the assessment of the effectiveness of cybersecurity awareness programs

This section explains the available previous research conducted with machine learning (ML) techniques to assess the effectiveness of cybersecurity awareness programs. Machine learning has been bumming in recent times as many applications and critical systems have implemented the techniques for prediction. In the field of cybersecurity, ML is mostly used in the networking area for threat, attack, and anomaly detection(Martínez Torres et al., 2019). Also in spam detection ML is used (Fawcett, 2003). However, a published paper also explains phishing e-mails detection with ML techniques(Abu-Nimeh et al., 2007). Based on the authors' knowledge and research conducted most ML techniques used are mainly for identification or prediction of cyber-threats, however, one paper was found to have used ML to predict the level of cybersecurity awareness level using classification and regression tree CART Classifier in an educational environment in the middle east, this was used based on a

pre-designed quantitative questionnaire (Al-Janabi & Al-Shourbaji, 2016). This paper only identifies the current cybersecurity awareness knowledge of the students without

conducting any awareness program, therefore, firstly there are urgent needs to conduct an awareness program based on the cybersecurity need then a quantitative method should be used in gathering the result for prediction. The section seems to be left out as no other researcher has conducted such an experiment to the best of the authors' understanding. This has given room for more research to be conducted and ML techniques to be used in predicting the effectiveness of cybersecurity awareness programs.

Conclusion

In conclusion, this paper has provided a detailed answer to the research questions formulated, and the assessment of the effectiveness of cybersecurity awareness methodologies used has been provided based on the previous researcher, thou is not a new topic in the literature. However it was found, the application of ML in identifying the effectiveness of cybersecurity awareness programs was given much attention like in cyber-threat predictions, and this has open up an opportunity for researchers to apply more ML to predict the success of cybersecurity awareness programs. The recent methods use are good also but, applying ML would provide more accurate results than only depending on the quantitative or qualitative, or mix-method approach. Moreover, it was found from the literature there is no framework used when designing any cybersecurity awareness program as a guide. This also has opened up a new dimension for the researchers to propose frameworks peculiar to cybersecurity awareness programs that would be used as a guide when designing an awareness program, this would further make the program more effective after implementation than when the traditional method is used. Finally, based on the literature, universities/ colleges/secondary was far left behind when it comes to implementing cybersecurity awareness programs as youths are more exposed to cyber-threats due to the high dependency on the internet in their daily activities.

References

Abu-Nimeh, S., Nappa, D., Wang, X., & Nair, S. (2007). A comparison of machine learning techniques for phishing detection. *Proceedings of the Anti-Phishing Working Groups 2nd Annual ECrime Researchers Summit*, 60–69.

Ahlan, A. R., & Lubis, M. (2011). Information security awareness in university: Maintaining learnability, performance and adaptability through roles of responsibility. *Proceedings of the 2011 7th International Conference on Information Assurance and Security, IAS 2011*, 246–250. https://doi.org/10.1109/ISIAS.2011.6122827

Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information and Knowledge Management*, *15*(1). https://doi.org/10.1142/S0219649216500076

Al-jerbie, S. I., & Mohd Zalisham Jali. (2014). A Second Look at the Information Security Awareness among Secondary School Students. *International Conference on Information Security and Cyber Forensics*, 88–97.

Al Shamsi, A. A. (2019). Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE Effectiveness of Cyber Security Awareness Program for young children View project Sentiment Analysis for Arabic Dialects View project Effectiveness of Cyber Security. *International Journal of Information Technology and Language Studies (IJITLS)*, *3*(2), 8–29. http://journals.sfu.ca/ijitls

Albrechtsen, E. (2006). *A qualitative stusy of users veiws on information security*.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers and Security*, *29*(4), 432–445. https://doi.org/10.1016/j.cose.2009.12.005

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers and Security*, *42*, 56–65. https://doi.org/10.1016/j.cose.2014.01.005

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M. A., & Passingham, N. (2015). Awareness is only the first step. *Hewlett Packard Enterprise Business White Paper*, 1–12. https://riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf

Burcu Bulgurcu, H. C. and I. B. (2016). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefsand Information Security Awareness. *Management Information Systems Research Center, University of Minnesota*, *34*(3), 523–548.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security and Privacy*, *12*(1), 28–38. https://doi.org/10.1109/MSP.2013.106

Charlie, C., Shaw, R. S., & Yang, S. C. (2006). Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System. *Information Technology, Learning & Performance Journal*, *24*(1), 1–14. http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=87d7976e-feb9-4d5f-b6f2-a7f931d20b63@sessionmgr14&vid=3&hid=9

Charoen, D., Raman, M., & Olfman, L. (2008). Improving end user behaviour in password utilization: An action research initiative. *Systemic Practice and Action Research*, *21*(1), 55–72. https://doi.org/10.1007/s11213-007-9082-4

Cheung, R. S., Cohen, J. P., Lo, H. Z., Elia, F., & Carrillo-Marquez, V. (2012). Effectiveness of Cybersecurity Competitions. *Proceedings of the International Conference on Security and Management (SAM)*, *1*, 1. http://josephpcohen.com/papers/seccomp.pdf%5Cnhttp://world-comp.org/p2012/SAM6108.pdf

Claar, C. L., & Johnson, J. (2012). Analyzing home pc security adoption behavior. *Journal of Computer Information Systems*, *52*(4), 20–29. https://doi.org/10.1080/08874417.2012.11645573

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers and Security*, *26*(1), 63–72. https://doi.org/10.1016/j.cose.2006.10.005

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers and Security*, *28*(3–4), 189–198. https://doi.org/10.1016/j.cose.2008.11.007

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers and Security*, *26*(1), 36–43. https://doi.org/10.1016/j.cose.2006.10.006

EDUCAUSE. (2018). *Horizon Report 2018 Higher Education Edition*. https://library.educause.edu/~/media/files/library/2018/8/2018horizonreport.pdf

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies - A case study. *Information Security Technical Report*, *14*(4), 223–229. https://doi.org/10.1016/j.istr.2010.05.002

Fawcett, T. (2003). " In vivo" spam filtering: a challenge problem for KDD. *ACM SIGKDD Explorations Newsletter*, *5*(2), 140–148.

Furman, S., Theofanos, M. F., Choong, Y.-Y., & Stanton, B. (2012). Basing cybersecurity training on user perceptions BT - Security Training and Education. *IEEE Security and Privacy*, *10*(2), 40–49. https://doi.org/10.1109/MSP.2011.180

Furnell, S. (2008). End-user security culture: A lesson that will never be learnt? In *Computer Fraud and Security* (Vol. 2008, Issue 4, pp. 6–9). https://doi.org/10.1016/S1361-3723(08)70064-2

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers and Security*, *26*(5), 410–417. https://doi.org/10.1016/j.cose.2007.03.001

Hagen, J., Albrechtsen, E., & Ole Johnsen, S. (2011). The long-term effects of information security e-learning on organizational learning. *Information Management & Computer Security*, *19*(3), 140–154. https://doi.org/10.1108/09685221111153537

Hepp, S. L., Tarraf, R. C., Birney, A., & Arain, M. A. (2018). Evaluation of the awareness and effectiveness of IT security programs in a large publicly funded health care system. *Health Information Management Journal*, *47*(3), 116–124. https://doi.org/10.1177/1833358317722038

Johansson, A., & Götestam, K. G. (2004). Internet addiction: characteristics of a questionnaire and prevalence in Norwegian youth (12-18 years). *Scandinavian Journal of Psychology*, *45*(3), 223–229. https://doi.org/10.1111/j.1467-9450.2004.00398.x

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management and Computer Security*, *22*(1), 115–126. https://doi.org/10.1108/IMCS-01-2013-0005

Kitchenham. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering*. https://doi.org/10.1145/1134285.1134500

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering - A systematic literature review. *Information and Software Technology*, *51*(1), 7–15. https://doi.org/10.1016/j.infsof.2008.09.009

Korovessis, P., Furnell, S., Papadaki, M., & Haskell-Dowland, P. (2017). A toolkit approach to information security awareness and education. *Journal of Cybersecurity Education, Research and Practice*, *2017*(2), 5.

Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. In *Computers and Security* (Vol. 29, Issue 8, pp. 840–847). https://doi.org/10.1016/j.cose.2010.08.001

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, *18*(5), 316–327. https://doi.org/10.1108/09685221011095236

Labuschagne, W. A., Burke, I., Veerasamy, N., & Eloff, M. M. (2011). Design of cyber security awareness game utilizing a social media framework. *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*, 1–9. https://doi.org/10.1109/ISSA.2011.6027538

Langer, S. G. (2017). Cyber-Security Issues in Healthcare Information Technology. *Journal of Digital Imaging*, *30*(1), 117–125. https://doi.org/10.1007/s10278-016-9913-x

Lau, K. P., Chiu, D. K. W., Ho, K. K. W., Lo, P., & See-To, E. W. K. (2017). Educational Usage of Mobile Devices: Differences Between Postgraduate and Undergraduate Students. *Journal of Academic Librarianship*, *43*(3), 201–208. https://doi.org/10.1016/j.acalib.2017.03.004

Mani, D., Choo, K. K. R., & Mubarak, S. (2014). Information security in the South Australian real estate industry: A study of 40 real estate organisations. *Information Management and Computer Security*, *22*(1), 24–41. https://doi.org/10.1108/IMCS-10-2012-0060

Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Review: machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, *10*(10), 2823–2836. https://doi.org/10.1007/s13042-018-00906-1

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, *9*(1), 23–41. https://doi.org/10.1080/15332861.2010.487415

Mi, T., Gou, M., Zhou, G., Gan, Y., & Schwarzer, R. (2020). Effects of planning and action control on smartphone security behavior. *Computers and Security*, *97*, 101954. https://doi.org/10.1016/j.cose.2020.101954

Michael, E., & Power. (2007). Developing a culture of privacy: A case study. *IEEE Security and Privacy*, *5*(6), 58–60. https://doi.org/10.1109/MSP.2007.163

Monk, T., Van Niekerk, J., & Von Solms, R. (2010). Sweetening the medicine: Educating users about information security by means of game play. *ACM International Conference Proceeding Series*, 193–200. https://doi.org/10.1145/1899503.1899525

Öıütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers and Security*, *56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management and Computer Security*, *22*(4), 334–345. https://doi.org/10.1108/IMCS-10-2013-0078

Peker, Y. K., Ray, L., Silva, S. Da, & Gibson, N. (2016). Raising Cybersecurity Awareness among College Students. In *Journal of The Colloquium for Information System Security Education (CISSE)* (Issue September).

Rahim, N. H. A., Hamid, S., Kiah, L. M., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*(4), 606–622. https://doi.org/10.1108/K-12-2014-0283

Rantos, K., Fysarakis, K., & Manifavas, C. (2012). How Effective Is Your Security Awareness Program? An Evaluation Methodology. *Information Security Journal*, *21*(6), 328–345. https://doi.org/10.1080/19393555.2012.747234

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers and Security*, *27*(7–8), 241–253. https://doi.org/10.1016/j.cose.2008.07.008

Shaaban, H. K. (2014). Enhancing the Governance of Information Security in Developing Countries: The Case of Zanzibar. *PhD Thesis*, 2014. https://doi.org/10.1080/13678868.2012.756154

Slusky, L., & Partow-Navid, P. (2012). Students Information Security Practices and Awareness. *Journal of Information Privacy and Security*, *8*(4), 3–26. https://doi.org/10.1080/15536548.2012.10845664

Son, J., Kim, D., Hussain, R., & Oh, H. (2014). Conditional proxy re-encryption for secure big data group sharing in cloud environment. *Proceedings - IEEE INFOCOM*, 541–546. https://doi.org/10.1109/INFCOMW.2014.6849289

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*, 196–203. https://doi.org/10.1109/ARES.2010.27

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. *Information Security Journal*, *17*(5–6), 207–227. https://doi.org/10.1080/19393550802492487

Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers and Security*, *77*, 807–823. https://doi.org/10.1016/j.cose.2018.02.001

Wolf, M., Haworth, D., & Pietron, L. (2011). Measuring An Information Security Awareness Program. *Review of Business Information Systems – Third Quarter 2011*, *15*(3), 9–22. https://doi.org/10.19030/rbis.v15i3.5398