Cybersecurity Awareness in Students Depending on Knowledge and Background

Introduction

Cybersecurity awareness is an essential scope of study which requires understanding the factors due to which potential risks towards information security is increasing dynamically. The users of the internet must be made aware of potential threats and risks due to which human behavior is significantly impacted (Peker, Ray & Silva, 2018). The technological advancements have increased rapidly over the years which is maturing the amount of information being shared electronically. This is increasing the vulnerability of information being shared over the internet enhancing the exposure to risk (Peker, Ray, Silva, Gibson & Lamberson, 2016). The category of cybersecurity based instances has increased in magnitude over the years maturing the controls and processes. The critical infrastructure and systems developed for securing the control processes are sought to exploit human behavior or breach corporate contracts (Slusky & Goodrich, 2016). The assessment of awareness of the threats in the individuals is essential for understanding the threat and develop countermeasures.

Cybersecurity is a dynamic problem which is significantly impacting on individuals and businesses. The core objective of this research is to understand the awareness of the students against this potential threat based on which the countermeasures to cope with the cyber threat landscape can be designed (Jin, Tu, Kim, Heffron & White, 2018). The awareness factors of the students as an assessment is critically important as it enables understanding remedial aspects which are applied for coping with the challenges. The critical goals of cybersecurity awareness are understanding the aspects through which opportunities and challenges as in the threat landscape can be used to manage the potential risk and remedies (Muhirwe & White, 2016). All these attributes enable enhancing and securing the organizational cultures or enabling the individuals to protect their personal information over personal computers and shared units.

Problems Associated with Cybersecurity Risk

Cybersecurity risks and attacks are becoming highly prevalent with the advancing scope of technology. It is critical to understand the impact of this challenge on the day to day lives of the individuals (Chattopadhyay, Christian, Ulman & Petty, 2018). The awareness of cybersecurity is an important element which protects the people and systems. The critical objective of this study is to understand the awareness levels of cybersecurity in the students which shall enable understanding knowledge and backgrounds required to craft remedial

alternates (Yan et al., 2018). The awareness of the students towards cybersecurity knowledge, self-perceptions of cybersecurity skills, actual cybersecurity skills and behavior and attitudes of the people coping with the threats is critical to be understood. The cybercriminals are progressing the attempts of a security breach which is expected to increase at a multiplying pace over the years (Liu & Murphy, 2016). The individuals and businesses across the globe are dedicating enhanced revenue towards hiring the security professional which are equipped to maintain customer privacy and avoiding ransomware attacks (Whitman, 2016).

Interesting Facts about Cybersecurity Threats

Over the years cybersecurity threats have increased dramatically which includes the evolution of ransomware through corrupting data which is being used in the organizations. AI Expansion is critically important and requires an understanding of the future development of Artificial Intelligence (Giannakas, Kambourakis & Gritzalis, 2015). The use of technological devices is increasing significantly over the period of time which is enhancing the risk of the security professionals making prepared the integrating requirements which include assessment of password requirements, user verification, time-out sessions and two-factor authentication including security protocols (Pusey, Gondree & Peterson, 2016). The further contribution of the threats is increasing with the revolution of Blockchain technology linking with the popularity of cryptocurrencies namely Bitcoins and Ethereum. This technology is a huge revolution which differs from the traditional integration of currency (Dunn & Merkle, 2018). The introduction of serverless applications is increasing vulnerability as they invite cyber-attacks. The customer information, in this case, is highly vulnerable impacting on the scope of technology (Chandarman & Niekerk, 2017).

Background

Literature Review

The role of cybersecurity and the introduction of digital forensics is increasing dramatically over the years. The awareness towards cybercrimes and computer-assisted crime is increasing dramatically (Er, Cheah, Moses, Chong & Ang, 2017). There are numerous tools which have been developed over the years for understanding the future threats and risks pertaining to the topic. Estimates show that the number of cybercrime damages is increasing over the years which shall cost $6 Trillion annually as damage by 2021 (Croasdell, Elste & Hill,

2018). The researchers have evaluated this essential factor through which the volume of data including the data stored in hard drives and stacked in databases can be protected. The technology platforms and systems exist within the personal lives of all the individuals which include tablets, mobile phones, systems, and cloud computing efforts (Whitman, Mattord & Hollingsworth, 2016). The evaluation shows that very little efforts have been taken towards spreading awareness amongst individuals at a personal level. Around 91% of attacks are estimated to start from phishing emails. The advanced scope and challenges require identifying the scope of the future and making the individuals aware of the potential threats against cybersecurity (Katerattanakul & Kam, 2019). There are numerous challenges which are required to be remedied for coping with the technical challenges which include understanding the different media formats, encryption, and anti-forensics and live acquisition and analysis (Peker et al., 2018). In the year 2017, the Ransomware attacks increased by 36% and so the individuals must be made aware of the security measures which are required to be coped and understand the legal challenges and resource challenges which pertain to this segment of assessing forensic media (Peker et al., 2016).

The scope and foundations of the study are numerous which cannot be consolidated in a limited aspect of the study. The assessment of study aims at understanding the level of precautions which are adequate for the students to protect their cybersecurity and other related issues (Slusky & Goodrich, 2016). The cybersecurity awareness is linked with the knowledge, experience, and backgrounds of the study which requires aiming at the extent to which the individual level of cybersecurity is dependent.

Research Question

The research questions which pertain to the study are the following:

- *Do Students take adequate precautions to protect their cybersecurity?*
- *To what extent does an individual's level of cybersecurity depend on their knowledge, experience, and background?*

The focus of this research shall be towards evaluating the scope of the students and understanding the precautions which are taken for protecting the elements of cybersecurity. The role of individuals in coping with cybersecurity is critically important as it depends mainly on

the knowledge, experience, and backgrounds of the individuals (Jin et al., 2018). The assessment of these factors is essential for understanding the awareness of cybersecurity in individuals.

Methodology

The qualitative and quantitative techniques shall both be used for the assessment of this study. It is critical that primary and secondary data of research are both aligned with the information of the research (Muhirwe & White, 2016). It is essential that the pragmatic approach of the study which is the mixed approach of the study shall be applied to this research. The data of this research shall be acquired using a structured questionnaire which comprises of open-ended and close-ended questions (Chattopadhyay et al., 2018). The study is developed based on the scope of participation through which adequate selection of information is highly critical and crucial. The collection of data is highly important for understanding the awareness level of the students through which knowledge and background of the students are assessed along with awareness of cybersecurity (Yan et al., 2018). The data and information collected using research instruments and assessing the information on the basis of worksheet analysis shall provide an evaluation of the scope of the study. The participants of the study shall be the students who are attending the schools and colleges (Liu & Murphy, 2016). Through this evaluation of the questionnaire, the adherence levels of the students shall be assessed. The selection of data is critical for the study as it shall craft the results of the study.

Privacy and Ethical Issues

The consideration of ethical aspects is primarily important while considering privacy based ethical issues of the society. It is essential that critical aspects pertaining to cybersecurity are assessed through which problems relating to cybersecurity can be remedied (Whitman, 2016). The ethical and moral aspects of cybersecurity are critical which provides an understanding of aspects of national security, morality of hacking and computer crime. These aspects allow amendments in the control of cyberterrorism and information warfare which allows controlling the moral responsibilities of information security professionals and understand the significance of privacy (Giannakas et al., 2015).

References

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *African Journal of Information and Communication*, *20*, 133-155.

Chattopadhyay, A., Christian, D., Ulman, A., & Petty, S. (2018, September). Towards A Novel Visual Privacy Themed Educational Tool for Cybersecurity Awareness and K-12 Outreach. In *Proceedings of the 19th Annual SIG Conference on Information Technology Education* (pp. 159-159). International World Wide Web Conferences Steering Committee.

Croasdell, D., Elste, J., & Hill, A. (2018). Cyber Clinics: Re-imagining Cyber Security Awareness.

Dunn, M. H., & Merkle, L. D. (2018, February). Assessing the Impact of a National Cybersecurity Competition on Students' Career Interests. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (pp. 62-67). ACM.

Er, P. H., Cheah, P. K., Moses, P., Chong, C. K., & Ang, B. H. (2017). Awareness of Safe and Responsible Use of ICT Among Students in a Malaysian University. In *Empowering 21st Century Learners Through Holistic and Enterprising Learning* (pp. 41-48). Springer, Singapore.

Giannakas, F., Kambourakis, G., & Gritzalis, S. (2015, November). CyberAware: A mobile game-based app for cybersecurity education and awareness. In *2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)* (pp. 54-58). IEEE.

Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018, February). Game based cybersecurity training for high school students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (pp. 68-73). ACM.

Katerattanakul, P., & Kam, H. J. (2019). Enhancing Student Learning in Cybersecurity Education using an Out-of-class Learning Approach. *Journal of Information Technology Education: Innovations in Practice*, *18*(1), 29-47.

Liu, X., & Murphy, D. (2016, September). Engaging females in cybersecurity: K through Gray. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 255-260). IEEE.

Muhirwe, J., & White, N. (2016). CYBERSECURITY AWARENESS AND PRACTICE OF NEXT GENERATION CORPORATE TECHNOLOGY USERS. *Issues in Information Systems*, *17*(2).

Peker, Y. K., Ray, L., Da Silva, S., Gibson, N., & Lamberson, C. (2016, October). Raising Cybersecurity Awareness among College Students. In *Journal of The Colloquium for Information System Security Education* (Vol. 4, No. 1, pp. 17-17).

Peker, Y., Ray, L., & da Silva, S. (2018, June). Online Cybersecurity Awareness Modules for College and High School Students. In *2018 National Cyber Summit (NCS)* (pp. 24-33). IEEE.

Pusey, P., Gondree, M., & Peterson, Z. (2016). The outcomes of cybersecurity competitions and implications for underrepresented populations. *IEEE Security & Privacy*, *14*(6), 90-95.

Slusky, L., & Goodrich, J. A. (2016, June). Human Factors of Cybersecurity Awareness. In *EdMedia+ Innovate Learning*(pp. 436-444). Association for the Advancement of Computing in Education (AACE).

Whitman, M. E. (2016, October). NSF-Sponsored Student Paper Proceedings of the 2017 Conference on Cybersecurity Education, Research and Practice. In *Conference on Cybersecurity Education, Research and Practice* (Vol. 2016).

Whitman, M., Mattord, H., & Hollingsworth, C. (2016, October). 2017 Proceedings of the Conference on Cybersecurity Education, Research and Practice-NSF Sponsored Graduate Student Workshop section. In *Proceedings of the 2017 Conference on Cybersecurity Education, Research and Practice* (Vol. 2016, No. 1).

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?. *Computers in Human Behavior*, *84*, 375-382.