DOI: http://dx.doi.org/10.26483/ijarcs.v10i5.6476

Volume 10, No. 5, September-October 2019

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A REVIEW OF THE IMPACT OF TRAINING ON CYBERSECURITY AWARENESS

Ahmed Alruwaili
Deakin University
Melbourne, Australia

Abstract: This study aimed to review the studies carried out on the impact of training on cybersecurity awareness. Various databases were searched for keywords 'cybersecurity & training', 'cybersecurity & training & impact' and 'cybersecurity awareness & training.' These studies were also shortlisted as per the year of publication. The review found that during recent years, the increasing use of the Internet in professional and private spheres has led to an explosion in the rate of cybercrime across the world. Training on cybersecurity awareness has seen a mixed impact, with some studies claiming that such training has limited results. Some authors have talked about customization of training programs for effective cybersecurity awareness generation.

Keywords: Review; Cybersecurity; Training; Awareness; Impact.

I. INTRODUCTION

Across the world, businesses, governments, and private organizations make extensive use of Information and Communications Technologies (ICT), and as a result, their security is of utmost importance. The people working in these organizations need to be made aware of the security aspect of using these technologies. Similarly, people using the Internet at home also need to be aware of the concept of cybersecurity, so that their information, as well as their finances, can be kept safe.

According to Alotaibi, Furnell, Stengel, Papadaki (2016), around the world, cybercrimes have exploded in number. Their study says that the Business Email Compromise (BEC) scams worldwide were estimated to be more than USD 3 billion. According to Alotaibi, Furnell, Stengel, Papadaki (2016), the effect of cybercrime is not just measured solely "in terms of costs incurred, but also in terms of breach of data privacy which can affect many consumers." This study says that by 2019, the projected losses due to cybercrime are estimated to be around USD 2 trillion. The authors say that in substantial companies, the number of cyberattacks has been decreasing, but in medium and small-sized companies, it is increasing (Alotaibi, Furnell, Stengel, Papadaki, 2016). "Due to a minimally regulated digital infrastructure, the exploitation of cyberspace with malicious intent threatens the rights of individuals, privacy of individuals, assets of private enterprises, and even the security of nations" (Paulsen, McDuffie, Newhouse, & Toth, 2012 – as cited in Nilsen, Levy, Terrell, Beyer, 2017)

Although cybersecurity is a concern across the world, it is of more significant concern for the government and the business world. According to Jin, Tu, Kim, Heffron, & White (2018), "cybersecurity is a shared mission between government and industry because a large portion of the national cybersecurity infrastructure is in the private sectors".

Hence, in order to study the impact of cybersecurity awareness programs, we will review the studies which have been carried out on the subject.

II. METHODOLOGY

In this paper, I will review some of the research studies which have been carried out on the subject of cybersecurity in Saudi Arabia. Towards this end, specific search terms were used in the Scholarly search engines, such as 'cybersecurity & training', 'cybersecurity & training & impact' and 'cybersecurity awareness & training.' The search yielded over 16,110 results, out of which thirteen were chosen for this review. The results of these searches were shortlisted as per the year of publication. For this study, only studies published after 2010 were used in order to review the studies on cybersecurity in Saudi Arabia.

III. RESULTS AND DISCUSSION

With the rise in the spread of the Internet, the incidence of cybercrimes has also increased. According to Bada, Sasse, & Nurse (2014), it has been seen that governments around the world encourage citizens to carry out transactions online and also provide advice on how to go about it in a secure fashion. Despite this, major cybersecurity attacks continue to occur. The authors say that one likely reason for this could be the fact that the people carrying out such attacks are becoming more skilled.

It is also true that sometimes, technology acts as a challenge for the practice of cybersecurity. Bada, Sasse, & Nurse are of the opinion that many times, security interfaces are too complicated for the layman to use. As per the literature on the subject, people often know the correct answers to cybersecurity awareness questions, but do not practice it in real life. Bada, Sasse, & Nurse (2014) propose that it is essential for security and privacy practices to be designed into a system from the very beginning. Also, any system which is too difficult to use will ultimately lead to users making mistakes and even avoiding security altogether (Bada, Sasse, & Nurse, 2014).

According to Aloul (2012), the increase in the number of cyberattacks across the world is mainly due to:

(1) increase in electronic data
(2) increase in mobile devices
(3) increase of organized cybercrime groups
(4) increase of intelligent external and internal IT security threats

(5) the difficulty of tracing the attackers
(6) limited cybercrime laws, and
(7) limited IT security knowledge among internet users.

According to Bada, Sasse, & Nurse (2014), the primary goal of cyber security-awareness campaigns in large government and private organizations is to influence the adoption of secure behaviour online. However, in order for such campaigns to be effective, it needs more than only informing people about what they should or should not do. They also need to accept that the information is pertinent. People also need to know how to respond and be willing to do this in the face of many other demands (Bada, Sasse, & Nurse, 2014).

A. Security Awareness

Security awareness has been defined by various authors, and most definitions have inferred from the required characteristics of security awareness.

According to Bada, Sasse, & Nurse (2014), security awareness is defined in NIST Special Publication as follows: "Awareness is not training. The purpose of awareness presentations is to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly". This clearly accentuates where the main weight on awareness should be. As per the authors, alongside being aware of possible cyber risks, people also need to behave accordingly (Bada, Sasse, & Nurse, 2014).

According to Al-Daeef, Basir & Saudi (2017), awareness is a "crucial part of any information security program either at a personal or organizational level. Individuals' lack of awareness may include but not limited to; browsing and hence disclosing personal information to untrusted sites, installing critical applications, and sharing personal information with others". Security awareness programs must be articulated to inspire users' behavior and understanding levels.

As per Al-Daeef, Basir & Saudi (2017), according to Information Security Forum (ISF), "security awareness is a continual process of learning by which, trainees realize the importance of information security issues, the security level required by the organization, and individuals' security duties".

Many times, security awareness is ignored in organizations. According to Aloul (2012), security awareness is "an often-overlooked factor in an information security program. While organizations expand their use of advanced security technology and continuously train their security professionals, very little is used to increase the security awareness among the normal users, making them the weakest link in any organization".

B. Cybersecurity Awareness Campaigns

According to Bada, Sasse, & Nurse (2014), an awareness and training program is vital, as it is the source for spreading information that all users (employees, consumers, and citizens, including managers) need. The authors say that in the case of an Information Technology (IT) security program, it is the most common method used to communicate security requirements and appropriate behaviour. For an awareness and training program to be effective, the material has to be interesting, current, and simple enough to be followed. As per Bada, Sasse, & Nurse (2014), "any presentation that 'feels' impersonal and too general as to apply to the intended audience, will be treated by users as just another obligatory session".

According to Bada, Sasse, & Nurse (2014), Past and current efforts to improve information- security practices and promote a sustainable society have not had the desired impact. It is essential, therefore to critically reflect on the challenges involved in improving information- security behaviours for citizens, consumers, and employees. In particular, our work considers these challenges from a Psychology perspective, as we believe that understanding how people perceive risks is critical to creating effective awareness campaigns. Changing behaviour requires more than providing information about risks and reactive behaviours – firstly, people must be able to understand and apply the advice, and secondly, they must be motivated and willing to do so – and the latter requires changes to attitudes and intentions. These antecedents of behaviour change are identified in several psychological models of behaviour. We review the suitability of persuasion techniques, including the widely used 'fear appeals'. From this range of literature, we extract essential components for an awareness campaign as well as factors that can lead to a campaign's success or failure (Bada, Sasse, & Nurse, 2014).

According to Al-Daeef, Basir & Saudi (2017), a "Security Education, Training and Awareness (SETA) was defined as an educational program that aims to reduce security breaches caused because of the lack of employees' security awareness. SETA was designed to educate employees on how to focus on security issues to protect themselves and their organization's data and network". SETA program integrates security in all tasks that employees do; from locking computer screens when they move away from their desks; to report unusual activities regarding emails, files and staff (Al-Daeef, Basir & Saudi, 2017).

According to Al-Daeef, Basir & Saudi (2017), apart from the training methods which have been implemented, "the main goal of security training programs is to raise trainees' awareness level and thus, influence their security behavior". Traditionally, information security has been viewed as a sort of service which has to be provided, instead of something which influences people. Due to this, researchers have always focused on the technical aspects of information security.

According to Al-Daeef, Basir & Saudi (2017), there have been claims that training on information security does not work, but there is evidence that well-designed user training methods can effectively enhance awareness and security behavior. In their study, the authors say that technology-related mistakes made by users cannot be resolved by adding more technology; instead, awareness-based training programs can be the perfect choice to lessen the limitations of technical-based security solutions. According to Al-Daeef, Basir & Saudi (2017), many researchers believe that security is usually viewed as users as a secondary goal, and therefore, they feel like they don't need to be trained to be more aware and know how to recognize and react against the different forms of fraudulent activities (Al-Daeef, Basir & Saudi, 2017).

C. Impact of Cybersecurity Awareness Training

According to Ghazvini & Shukur (2016), even though the number of information security awareness training programs is rising progressively, "there is inadequate evidence to verify their effectiveness and impact on daily activities in a work environment." As per the literature on the subject, a few of the information security awareness training programs are not sufficient enough. "For instance, number of awareness training programs tends to be more informative without integrating into employees' daily activities that leads to disciplinary actions. Some other awareness training programs are only provided as one-time session that cannot truly change users' behavior toward information system" (Ghazvini, & Shukur, 2016). The

authors say that awareness training programs should be a regular activity and need to be reinforced periodically.

According to Michalsky (2013), in his paper on cybersecurity awareness training programs in the healthcare industry, criticisms related to cybersecurity awareness training programs "usually run along the lines of a company becoming complacent or overly dependent on such a program, that employees are human and will continue to fall prey to determined network intruders or that employees should be focused on their healthcare missions—not on cyber security".

According to Proctor (2016), the primary concern is that there is over-reliance on cybersecurity awareness training programs and that companies think these are the panacea for any cyber security breach. The author says, "When there are failures in the architecture of cyber systems leading to breaches the focal point of failure becomes the user not the system design because executives are led to believe that cybersecurity awareness training programs will eliminate all breaches" (Proctor, 2016).

There has been evidence that such training programs do bring about a change in employees' cybersecurity practices. According to Muhirwe & White (2016), cybersecurity awareness significantly impacts one's cybersecurity practice.

Sometimes, companies do not make the most of cybersecurity awareness training programs ultimately. According to Miranda (2018), "users and the organization may be failing to fully benefit from a phishing training exercise due to lack of a comprehensive program that addresses the entire lifecycle of phishing awareness training."

There is evidence that game-based cybersecurity awareness training programs are effective in generating cybersecurity awareness, especially amongst high school students. According to Jin, Tu, Kim, Heffron, & White (2018), game-based learning for cybersecurity education was very effective in cybersecurity awareness training.

IV. Recommendations from Studies

One of the main recommendations from studies carried out on cybersecurity awareness training is that individuals react differently to the same conditions. Hence, according to McBride, Carter & Warkentin (2012), the approach taken for cybersecurity awareness training must also differentiate between individual personality types of employees. According to the authors, there is "need for future research to develop customized training protocols that incorporate the interrelations between the Big Five personality factors and individual perceptions of security threats and organizational sanctions".

According to Ghazvini & Shukur (2016), research is insufficient for effective information security awareness delivery methods. Hence, it is essential that an effective awareness training delivery method is selected, designed, and implemented to ensure proper protection of the organizational assets.

According to Landress, Parrish, & Terrell (2017), if cybersecurity trainers try to improve resilience, in addition to traditional security awareness training, the rates of attacks by cybercriminals will decrease in both number and severity. "When facilitating concepts of confidentiality, integrity, and availability (CIA), the training program should be augmented by employing the resiliency characteristics of Richardson's (2002) second wave, which describes people who learn resilient behaviors to cope with life" (Landress, Parrish, & Terrell, 2017).

V. Conclusion

In this paper, reviewed papers written on the subject of the impact of training on cybersecurity awareness. Studies have present that the spread of the Internet has led to companies and homes being subject to cybercrimes. The issue of cybersecurity is prime both amongst professionals and individuals. The authors have talked about the limited effectiveness of cybersecurity awareness training programs. Some have written about what it takes for such programs to be successful.

VI. References

[1] Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A Review of Using Gaming Technology for Cyber-Security Awareness. International Journal of Information Security Research (IJISR), 6(2), 660-666.

[2] Aloul, F.A. (2012). The Need for Effective Information Security Awareness. Journal of Advances in Information Technology, 3(3), 176-183.

[3] Al-Daeef, M.M., Basir, N., & Saudi, M.M. (2017). Security Awareness Training: A Review. In Proceedings of the World Congress on Engineering. London, U.K.

[4] Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. *arXiv preprint arXiv:1901.02672*.

[5] Ghazvini, A., & Shukur, Z. (2016). Awareness Training Transfer and Information Security Content Development for Healthcare Industry. (IJACSA) International Journal of Advanced Computer Science and Applications, 7(5), 361-370.

[6] Jin, G., Tu, M., Kim, T-H., Heffron, J., & White, J. (2018). Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. Journal of Education and Learning (EduLearn), 12(1), 150-158.

[7] Landress, A.D., Parrish, J., & Terrell, S. (2017). Resiliency as an Outcome of SETA Programs. In Twenty-third Americas Conference on Information Systems. Boston, MA.

[8] McBride, M., Carter, L., & Warkentin, M. (2012). One Size Doesn't Fit All: Cybersecurity Training Should Be Customized. Institute for Homeland Security Solutions. Retrieved from https://sites.duke.edu/ihss/files/2011/12/CyberSecurity_2page-summary_mcbride- 2012.pdf

[9] Michalsky, R.J. (2013). Raising Cyber Security Awareness for Healthcare Professionals. Retrieved from http://www.njvc.com/sites/default/files/white%20papers/Cyber_Security_Awareness_in_ Healthcare.pdf

[10] Miranda, M.J.A. (2018). Enhancing Cybersecurity Awareness Training: A Comprehensive Phishing Exercise Approach. International Management Review, 14(2), 5-10.

[11] Muhirwe, J. & White, N. (2016). Cybersecurity Awareness and Practice of Next Generation Corporate Technology Users. Issues in Information Systems, 17(II), 183-192.

[12] Nilsen, R., Levy, Y., Terrell, S., & Beyer, D. (2017). A Developmental Study on Assessing the Cybersecurity Competency of Organizational Information System Users.

[13] Proctor, W.R. (2016). Investigating the Efficacy of Cybersecurity Awareness Training Programs (Unpublished master's thesis). Utica College, New York.