International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | April 2022 www.irjet.net p-ISSN: 2395-0072

An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy

Bibhu Dash[1], Meraj F. Ansari[2]

[1] Dept. of Computer and Information Systems, University of the Cumberlands, Williamsburg, KY USA
[2] Dept. of Computer and Information Systems, University of the Cumberlands, Williamsburg, KY USA

Abstract - *Security Education Training and Awareness plays a dynamic role for organizations in endorsing resources' thoughtfulness and accessibility. This paper determines the importance of security awareness training in dealing with cyber threats. This research uses the Technology Acceptance Model (TAM), indicating that at-risk employees' behavior and information security awareness training execution are successful interventions. Yet, those investigations did not examine Artificial Intelligence (AI) enabled training, so this study fills that literature gap. This analysis used a qualitative research design. The article examines employees' behavior and the effectiveness of AI-based security awareness training programs. The study here helps analyze information security awareness training in the workplace, encouraging behavioral transformations that would restrain data breaches by incorporating the users' exposure and the stringency of coercion and the retort to peril in prophesying behavior discretions.*

***Key Words*: Cybersecurity, Risk culture, SETA, NICE, TAM, viCyber, AI-enabled exercise, Security Awareness Training**

1.INTRODUCTION

One of the most challenging issues that come with advancements in technology is securing systems from cyber-attacks [1]. There is a clear need to implement proper infrastructure security, beginning from the grassroots and the local government. This has made cybersecurity an essential factor in the teaching of information systems with the development of hacktivist groups such as Anonymous, whose sole purpose is to cripple the information systems of different governments [2]. Information system analysts in each organization are responsible for the cyber education of the employees, ensuring they are conscious of the risks that exist in cyberspace and making informed decisions that are in the best interests of the organization's security [3].This paper will mainly focus on the programs that can be implemented to ensure information security and data vulnerability awareness. The main objectives of the research will be to ensure that the employees or staff of the organization understand the threats that exist to the organizational data and how to ensure there is security in the organizations' information systems by focusing on both the human factors and technological angles that may lead to penetration or hack. The second aim of this research will be to identify the points in a security chain that can be termed weak points in the chain. The main problem that this research will face is the rapidly changing dynamics of technology and the development of new and more secure methods of securing data.

2. THEORETICAL FRAMEWORK

In preparing this research paper, extensive analysis and research were done on peer papers and books showing conduct and dealings in cybersecurity from organizational security to government and military information security [2]. An interest was taken in peer research papers and articles that show works on cybersecurity threats to organizations and the best practices to safeguard the organization from an outside threat by fortifying the employee knowledge on the topic. The scholarly articles proved to be especially useful by providing insight into why information security is essential. Most of the papers offered an approach that seemed to be a bottom-up approach by ensuring that each employee is educated on the best security practices that are up to date. If every employee does their particular part in this security chain, the whole organization will be safe. A chain is as strong as its weakest link [4].

Naïve information security practices among current and former employees of the organization have been the leading source of cyber threats, vulnerabilities, and penetrations, with between 72% and 95% of the threats coming from these sources, according to Price Waterhouse coopers research findings [5, 6, 23]. Most attacks are performed by unsupervised use of the internet, where information systems are attacked by malware. Malware is one of the most common tools cybercriminals use to conduct attacks and exploit vulnerabilities in an order. Another significant threat that a system has is the risk of human error, known as social engineering, where humans are manipulated to give out valuable system information, such as their authentication details. Even the best-developed systems can be brought down through social engineering by utilizing methods such as phishing, vishing, and impersonation [7]. Hence, organization

employees must acquire updated cybersecurity protection skills and countermeasure awareness [8].

2.1 TECHNOLOGY ACCEPTANCE MODEL

In this paper, Technology Acceptance Model (TAM) was adopted in this study to measure the variables. In 1989, the author Davis executed the technology adoption model, and it recreated an influential role in information management. Davis et al. depict the TAM model as a framework "used to represent the determinants of computer acceptance that is prevailing, and proficient of interpreting user behavior [i.e., use] across a broad array of end-user. In TAM's initial version (see Figure 1), the term attitude has another meaning influenced by technology and use. The TAM specifies "attitude" as the stage in which the end-user has assertive (or unfavorable) perceptions of the technology or process.

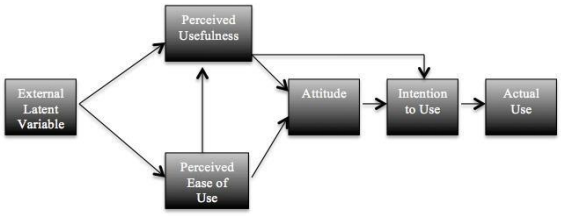

Fig -1: Technology Acceptance Model: Initial Version

2.2 TAM'S MODIFICATION

Employing the original TAM model, investigators executed many analyses. Davis et al. (1989) authenticated that perceived usefulness and ease of usage undeviatingly influence a new variable: behavioral intention [9]. Venkatesh and Davis (1996) eradicated the attitude variable and replaced it with behavior intention to develop the TAM's final version (see Figure 2) after further testing [10]. In both TAM's older and new versions, external variables are crucial in demonstrating perceived usefulness and ease of use. External variables usually entail user training, user engagement throughout the study, and execution [11].

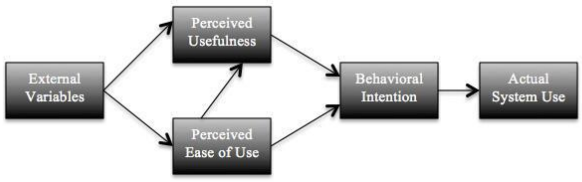

Fig -2: Technology Acceptance Model: Final Version

Cybersecurity awareness is vital in the organization. It specifies the level to which the organization is ready for any cyber-attack and how well the employees are conversant with the topic [12]. For an organization to say that they have awareness in their ranks, the employees and the organization must be subjected to the threats while being taught the cause and effects of each threat and how to prevent and counter the threat [13]. This will create a sense of responsibility among the employees and not leave the information security bulk of dealing with threats to the information system managers. Security risks in an organization require both prevention and countermeasures. The countermeasures include employee awareness, Security Education Training Awareness (SETA) programs, and computer sanctions and monitoring [14]. Therefore, now the organization needs to research the cyber threats that are most likely to face and determine their countermeasures by developing a cyber-security risk policy and computer safety document.

Unless employees protect themselves and the organization's systems, even the best intrusion detection and prevention systems will fail. The organization may have the latest technology in firewalls, intrusion detection, and intrusion prevention systems, but human factors must be considered, like awareness and skill training programs [15]. Many of the programs are the SETA hat that comes in many forms like coercing and fear tactics by showing the employees the threats in real-world situations and the adverse effects they bring [16]. Both online and real-life training should be conducted on the employees to ensure that they get to memorize every critical security measure. The delivery method of the SETA programs may be different in an organization depending on the type of employees being dealt with. Still, the essential factor is that they understand the risk that the organization may face from their actions.

For the SETA program to be effective, it must address the organization's security and risk policy topics. But some critical foundational issues have to be in place as they are familiar to most organizations, such as data security, shared risks and vulnerabilities, and password management [17]. The ISO/IEC 27002 [18] standards for IS security policy is a document that contains the necessary information security topic. Although some of the issues are not common in all organizations, it works well as a template for security policies.

3. SETA DESIGN AND ITS EFFECTIVENESS

Though the security awareness program is rising progressively in many organizations, very little data is available to measure its direct impact on work environments [19]. Security awareness training is the first step toward an organizational security strategy model. To

help organizations develop an effective SETA program, the above discussed theoretical framework should pass these 3-C tests: Constant, Complementary, and Compensatory [20]. Also, SETA programs need to be cost-effective, high in availability and benefit it gets with an optimal degree of security. Some of these programs are very complex, but at the same time, it lacks the primary step, for instance, the entire lifecycle of the phishing training program. Simple rules for a successful training program are clarity and less forceful involvement. So, the SETA training program members need to be more informative without integrating themselves more into employees' daily activities. Recently, game-based cybersecurity programs were influential in students' cyber security awareness training [21].

Some organizations are overly dependent on these SETA models, making this the core of their security culture. According to Proctor [22], the primary concern is an over-reliance on cybersecurity awareness training programs, and companies think these are the remedy for any cyber security breach. The over dependency and high expectations from the C-Suite executives of the company are not a welcome move for a healthy security climate. To get the best out of these programs, individuals react differently; they need to be designed to primarily facilitate Confidentiality, Integrity, and Availability (CIA) [23]. Any organization that follows and implements a SETA program to promote employee resilience to better cope with changing life is a successful project.

4. USE OF AI IN CYBERSECURITY TRAINING

AI and Machine Learning (ML) are a blessing to modern enterprises to educate and tackle cyber threats. AI is used as both offensive and defensive techniques to tackle cybersecurity. AI has been embedded in all information systems such that scholars have pointed out that AI failures in complex systems such as banking may face catastrophic sequences with no options of recovery [24]. A question arises here, how should we teach and blend the applications of AI in cybersecurity for better usefulness? As per scholars, the two options are: (1) approach cybersecurity the traditional way and discuss AI when relevant (2) approach cybersecurity using AI the best it can offer [25]. The first option is helpful for learners who want to understand cybersecurity holistically. The second option is available for professionals who desire an effective way to defend against all kinds of cyber threats. Considering the importance of cybersecurity education at all levels, many Massive Online Open Courses (MOOCs) have been developed recently to educate and train beginners and professionals. But all of these pieces of training lack practical usefulness to safeguard us from all forms of cyber threats, which prompts organizations to develop their training program as desirable.

4.1 NICE FRAMEWORK AND VICYBER MODEL

In an effort to design the best cybersecurity curriculum using AI tools, organizations are using the models developed by the National Institute of Standards and Technology (NIST), USA. The effective model developed by NIST is called the National Initiative for Cybersecurity Education (NICE) framework. It is a full-proof model developed by industry experts and academicians for cybersecurity education, training, and workforce development [26]. The NICE framework consists of seven categories, 31 specialty areas, and 369 Knowledge. Skills and Abilities areas (KSAs), 65 competencies, and 444 tasks under various specialty areas [27]. Hodhod et al. [27] described the detailed NICE framework as shown in Figure 3, and it has a wide acceptance in many industries.

Fig-3: NICE framework diagram

The NICE framework broadly guides curriculum development, but significant companies face difficulties using it due to the lack of domain experts who can utilize it to the fullest. The large competencies need to be considered along their relationships to develop a practical framework. To overcome this challenge, Amazon presents a cloud-based system: viCyber, an intelligent system capable of rapid cybersecurity curriculum and training development using AI and visual mappings [28]. This service can be used anytime and anywhere to develop, train, and collaborate easily when keeping the infrastructure safe from threats. The viCyber model design is governed based on the NICE framework with feedback and recommendation engine considering user perspective [27, 29]. This AI-based model has a decision support system based on the human-computer interaction to describe the building up process, which helps to modify the conceptual understanding of the user when going through the training with real-time feedback.

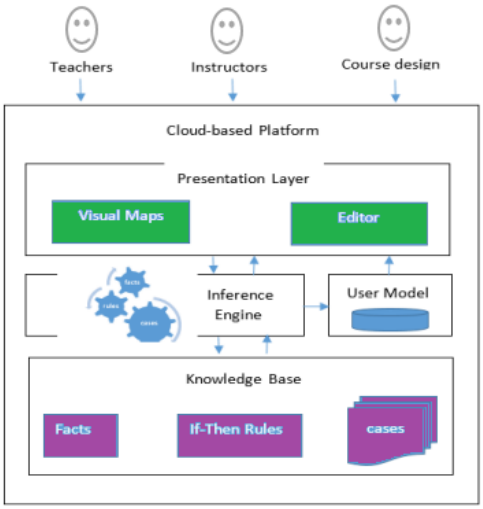

Fig-4: viCyber architecture with AI-enabled rules engine [27]

Note: Adapted from *Cybersecurity curriculum development using AI and decision support expert system*, by Hodhod, R., Wang, S., & Khan, S., 2018, International Journal of Computer Theory and Engineering, 10(4), 111. Copyright 2018 by International Journal of Computer Theory and Engineering.

4.2 USABILITY AND RELIABILITY OF VICYBER TOOL

This viCyber smart system presents a work in progress to develop cybersecurity curricula rapidly and reliably. This project contributes to changing the status of cybersecurity education by helping instructors develop the best cyber security programs. The viCyber uses a two-dimensional visual mapping technique that maps competencies with KSAs. The visual mapping connects the knowledge base with the skills and abilities of the NICE framework. The learners will select the specialty areas according to the skill levels that they should master to succeed in the cybersecurity market. Each course in viCyber is an incremental tree according to the expert level of course content. The evaluation piece in viCyber framework measures how good the curriculum design is and what level of audiences should attempt the particular training [27, 30]. Overall, the feedback with scores explains user expertise levels for further recommendations on how to make the design better. The output module in the viCyber tool gathers data from the curriculum and push to the cloud for future performance evaluation. Also, the powerful feature of this tool is its reusability to accommodate the existing curriculum as per industry needs. Users can match their behavior to fetch the highest matching curriculum using the nearest neighbor classification algorithm to match the course's tags and keywords [30]. This system can store the peer-review curriculum following the NICE framework using AI. The automatic curricula evaluation in this tool provides users with confidence to design and redesign modules as time passes.

5. SUMMARY AND CONCLUSION

The issue of cybersecurity is prime among individuals and professionals of all domains. The main aim of this research study was to figure out the best method of planning and implementing cybersecurity awareness programs among users and employees in organizations. To do this, research was conducted to answer the questions; Who or what is the weakest link in the security chain? What are the necessary components to develop positive security habits? What are the employee's responsibilities for protecting the company's assets? The results were found, and the weakest link in the security chain of any organization was determined to be the least aware employee in the organization. This employee's behavior can be defined as the measure of the strength of the information system, as a lack of awareness can bring down even the most reliable information systems. The second question in the research was determined to be by developing a SETA program that was custom to the organization. The last result was that each employee is responsible for the organization's security. By using a bottom-up approach where each employee is accountable for their section of the information system by the end of it, the whole system would be secure. The viCyber tool with the NICE framework is somehow the best workable framework in the marketplace to build a robust training and feedback system. The use of AI-enabled behavioral security training is rising in some startups and hi-tech firms that are gaining more popularity with young audiences as it studies an employee's behavior for a few days or weeks before prompting to take the training. This paper will motivate future scholars and guide them to build their SETA model integrating AI, Deep learning, and Natural language processing (NLP) for better outcomes.

REFERENCES

[1] Wei Chen Lin, & Saebeler, D. (2019). Risk-Based V. Compliance-Based Utility Cybersecurity -a False Dichotomy? Energy Law Journal, 40(2), 243–282.
[2] Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2018). Cybersecurity at the Grassroots: American Local Governments and the Challenges of Internet Security. Journal of Homeland Security & Emergency Management, 15(3), N.PAG
[3] Pawlowski, S. D., & Yoonhyuk Jung. (2015). Social Representations of Cybersecurity by University Students and Implications for Instructional Design. Journal of Information Systems Education, 26(4), 281–294.
[4] Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2019). Smart Airport Cybersecurity: Threat Mitigation

and Cyber Resilience Controls †. Sensors (14248220), 19(1), 19.

[5] D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. Communications of the ACM, 50(10), 113-117.

[6] IBM Global Technology Services. (2014). IBM security services 2014 cybersecurity intelligence index. Retrieved from http://www-03.ibm.com/security/services/2014-cyber-securityintelligence-index-infographic/

[7] Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2014). Social engineering in social networking sites: How good becomes evil. Proceedings of the Pacific Asia Conference on Information Systems, 1-10

[8] Goode, J., Levy, Y., Hovav, A., & Smith, J. (2018). Expert assessment of organizational cybersecurity programs and the development of vignettes to measure cybersecurity countermeasures awareness. Online Journal of Applied Knowledge Management, 6(1), 67–80.

[9] Davis, F. D. (1989). Perceived usefulness, perceived ease of use and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.

[10] Venkatesh, V., & Davis, F. D. (1996). A model of the antecedents of perceived ease of use: Development and test. Decision sciences, 27(3), 451-481.

[11] Ansari, M. F. (2021). The Relationship between Employees' Risk Scores and the Effectiveness of the AI-Based Security Awareness Training Program (Doctoral dissertation, University of the Cumberlands).

[12] Ansari, Meraj Farheen (2022) "A Quantitative Study of Risk Scores and the Effectiveness of AI-Based Cybersecurity Awareness Training Programs," International Journal of Smart Sensor and Adhoc Network: Vol. 3: Iss. 3, Article 1

[13] Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92-100.

[14] Choi, M. S., Levy, Y., & Hovav, A. (2013). The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. Proceedings of the Pre-International Conference of Information Systems on Information Security & Privacy, 1-19.

[15] Carlton, M., & Levy, Y. (2015). Expert assessment of the top platform-independent cybersecurity skills of non-IT professionals. Proceedings of the IEEE Southeast Conference, 1-6. doi:10.1109/SECON.2015.7132932.

[16] Kranz, J., & Haeussinger, F. (2014). Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior. International Conference on Information Systems, Auckland, Australia.

[17] 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.

[18] ISO/IEC. (2013). ISO/IEC 27002. 2013 Information technology- Security techniques - Code of practice for information security controls. Retrieved from https://www.iso.org/obp/ui/ #iso: std:iso-iec:27002: ed-2:v1:en

[19] 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.

[20] PricewaterhouseCoopers. (2016). The global state of information security survey 2016. Retrieved from http://www.pwc.com/gx/en/issues/cyber-security/information-securitysurvey.html

[21] 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.

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

[23] 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.

[24] R. V. Yampolskiy and M. Spellchecker, "Artificial intelligence safety and cybersecurity: A timeline of ai failures," arXiv preprint arXiv:1610.07997, 2016.

[25] S. Laato, A. Farooq, H. Tenhunen, T. Pitkamaki, A. Hakkala and A. Airola, "AI in Cybersecurity Education- A Systematic Literature Review of Studies on Cybersecurity MOOCs," *2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)*, 2020, pp. 6-10, doi: 10.1109/ICALT49669.2020.00009.

[26] NIST. (April 8, 2017). [Online]. Available: https://www.nist.gov/

[27] Hodhod, R., Wang, S., & Khan, S. (2018). Cybersecurity curriculum development using AI and decision support expert system. *International Journal of Computer Theory and Engineering*, *10*(4), 111.

[28] P. Wang and W. Kelly, "A novel threat analysis and risk mitigation approach to prevent cyber intrusions," Colloquium for Information System Security Education (CISSE), vol. 3, pp. 157-174, 2015.

[29] A. H. M. Ragab, K. A. Fakeeh, and M. I. Roushdy, "A medical multimedia expert system for heart diseases diagnosis & training," in Proc. the 2nd Saudi Science Conf., 2004, pp. 31-45.
[30] D. Benyon and D. Murray, "Applying user modeling to human-computer interaction design," Artificial Intelligence Review, vol. 7, no. 3, pp. 199-225, 1993.

BIOGRAPHIES

Description: Mr. Bibhu Dash is a Ph.D scholar (IT) at University of the Cumberlands, KY USA. Bibhu has 17 years of experience in IT with different insurance and financial domains. Bibhu's interest areas are Big Data, AI, ML, Deep Learning, NLP and IoT.

Description: Dr. Meraj Farheen Ansari completed her Ph.D. (IT) from the Graduate School of Information Technology, University of the Cumberlands. She also completed her MBA with a Specialization in Management Information Systems from Concordia University, Milwaukee, WI, USA. Her research interests include awareness of cybersecurity, eliminating Cyber Threats, & ML. Her current research involves how to aware organizational employees of cyber security threats using AI awareness programs. Currently, she is working as a Security Analyst in Northern Trust Bank, Chicago, IL, USA.