International Journal of Smart Sensor and Adhoc Network

Volume 3 | Issue 3 Article 1

March 2022

A Quantitative Study of Risk Scores and the Effectiveness of AI-Based Cybersecurity Awareness Training Programs

Meraj Farheen Ansari
University of the Cumberlands, merajfarheenansari25@gmail.com

Recommended Citation

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.
DOI: 10.47893/IJSSAN.2022.1212
Available at: https://www.interscience.in/ijssan/vol3/iss3/1

A Quantitative Study of Risk Scores and the Effectiveness of AI-Based Cybersecurity Awareness Training Programs

Meraj Farheen Ansari
Cybersecurity, University of the Cumberlands
Chicago, United States, merajfarheenansari25@gmail.com

Abstract

Cybersecurity awareness training plays a dynamic role for organizations in certifying resources' accessibility. The objective of this paper is to determine the correlation between an employee's risk score and the effectiveness of AI-based security awareness training that deals with cyber threats. The research uses the Unified Theory of Acceptance and Use of Technology to update prior research, revealing that at-risk employees' behavior and information security awareness training implementation make up successful interventions. However, those studies did not discuss AI training, and so this research fills that literature gap. This study used a quantitative research design. The researcher analyzed survey responses using Pearson's Correlation and an independent t-test to determine statistically significant relationships and differences between employees' risk scores and an AI-based security awareness training programs' effectiveness. The calculations came from a sample of 200 participants from two different organizations. The Pearson product correlation of employee's risk scores and the effectiveness of the security awareness training program was statistically significant. The researcher also conducted an independent-samples t-test to compare the employees' risk scores by gender. There were no significant differences in scores. Male were higher than female ones. The mean difference was minimal. The findings herein help interpret the role of information security awareness training in the workplace, promoting behavioral changes that would impede data violations by including the users' vulnerability and the severity of intimidation, and the response to a threat in prognosticating behavior intentions.

Keywords

Behavioral intention, Cybersecurity, Information security awareness training (ISAT), Unified Theory of Acceptance and Use of Technology(UTAUT), Phishing, Performance Expectancy (PE), Risk Scores, Social engineering, Vulnerability.

1. Introduction

Cybersecurity is an area of concern for any organization. Yet, it is not computers or technology that one should fear: the human element is often the weakest link in a security chain. User errors can occur due to dangerous practices, naivete about the online world, or disagreement with security procedures. When a user exposes sensitive data to criminal third parties, either knowingly or unknowingly, those parties can steal organizational data that was not exposed initially. Due to an escalation in intense social engineering invasions, hackers target technology users who can access the information systems to infiltrate the networks. As a result, training and instructing computer users to treat security-conscious performance as an essential element in

their work will positively affect the overall information security operation. The objective of this study is to investigate the correlation between the end-users risk scores and survey results.

To strengthen the system, users must undergo training to become aware of how threats can occur. They must learn how to increase preventive safety measures to the information security system. Yet, previous studies found extensive information security awareness training incapable of adjusting behavior [7]. Another study investigated environmental constituents that could lead to such behavior, such as social norms [6]. Yet other researchers studied the overall effectiveness of training programs [16]. There was even a study that highlighted the significance of security awareness and training [14]. Researchers have urged further research into the factors that affect information security behavior intention [8] [10] [18] [14]. Therefore, this study fills a gap in the research by investigating how the employees' risk scores affect behavior. The effectiveness of the AI-based security awareness training program can alter employees' risk scores.

Hence, it is essential to understand the objective of this paper that how AI-based security awareness training effectiveness and employees' risk scores can influence behavior intention and increase security norms to prevent cyber intrusions.

2. Background

According to different research papers, organizations are not aware of the ideal methods to educate their employees about Cybersecurity protective measures. Experts suggest certain tactics to create cybersecurity awareness. An excellent example is to engage the employees during the training; organizations should remain positive and speak the employees' language [3]. However, organizations currently depend on technology and information assurance decisions, which require that managers prepare and prevent any cyber-attacks on the organizations.

Prior studies have confirmed that security awareness training is a critical and necessary element to resist attacks, and such information can emphatically influence performance [1] [2] [4] [5] [13]. Therefore, addressing security awareness training is valuable to end-users and can also be necessary to organizations. According to various articles, machine learning can be a reliable solution to cyberattacks imposed by cybercriminals. Although machine learning centers on image recognition and natural language processing, it cannot be a more effective solution than the two done by humans [12]. Currently, organizations are utilizing machine learning in security awareness. Also, the deep learning neural network evaluates the changes in risk within organizations. According to some research papers, various firms help different organizations measure how their security programs perform.

This researcher used the UTAUT to conduct this study. As technology acceptance and use have expanded, several models have aimed to demonstrate technology acceptance and adoption. The UTAUT is a model created from "reviewing and synthesizing eight theories and models of technology use" [20]. Many studies have used the TAM to foretell an end-user's agreement with various information technology systems by ascertaining the user's ease of using a particular system [19]. The UTAUT constructs are useful in measuring performance and identifying the

elements that impact behavior. Overall, the UTAUT suggests that if users' recognized ease of use and convenience is high, they will acquire and practice the system. In this research, risk scores refer to performance expectancy, and the effectiveness of the training program relates to effort expectancy.

3. Research Problem

The researcher selected a quantitative method to investigate the relationship between the employees' risk scores and the effectiveness of the security awareness training program. This quantitative method will help decide the relationship between the employees' risk score and efficacy of the security training program and the difference in risk score, particularly gender. In this study, a total of 200 participants responded to the survey. These participants are from two different organizations that are using AI-based security awareness training programs. Only the employees who received the AI-based security awareness training program were allowed to participate in the survey. Google Forms collected the survey responses.

The demographic information included employee identification, age range, gender, the length of the training period, and the type of industry in which they are employed. The majority were female participants, with 54% compared to males. 69% of employees whose training period was 1-5 years, 17.5% of employees' training period was less than one year, and only 13.5 % received training for more than five years. The majority of participants were 35-50 years from the architecture & planning industry, with 57.5%. The participants mostly used their laptops to complete the survey questionnaire.

4. An AI-based, New-School comprehensive security awareness training program

Artificial intelligence-driven security awareness operations can help conduct simulated phishing schemes on users or groups of employees to see how hackers can extract data from a tool used by the users. Smart machine learning with integrated AI can distinguish patterns and suggest where weaknesses can occur in Cybersecurity. Present training awareness simulation can only recognize which employee became a victim and which employee recognized the threat. It will not recommend any employee measures by adding selected features like a virtual risk officer. The users' risk scores with machine learning help determine several different factors. Machine learning can analyze data and detect behavioral patterns missed by the present binary system of technology and humans. Companies may add a Virtual Risk Officer (VRO), a Virtual Risk Score (VRS), and Advanced Reporting (AR) features to the security awareness training and simulated phishing platforms. The cybersecurity awareness training programs which use deep learning neural networks effectively evaluate the users' knowledge and understand how risk varies over time [9].

5. Analysis of Research Questions

RQ1: Is there a relationship between employees' risk scores and the effectiveness of the security awareness training program?

The UTAUT variables were measured to answer this research question. The performance of the employee is measured and calculated as a risk score. The effort expectancy is the ease of use and is associated with security practices (security awareness training). The participants did not address any viewpoints of security that were characterized as challenging to use [15].

The Pearson product correlation of employee's risk scores and the effectiveness of the security awareness training program had a very low positive correlation ($r = .154$, $p < .05$), and the result is statistically significant at 0.05. Hence, the research shows that H1.1 was supported.

RQ2: Are there any differences in Risk Score by Gender (Male Vs. Female)?

The UTAUT variable (PE) and moderator variable (gender) were measured to answer this research question. The performance of employees (Risk Score) is analyzed and found no significant differences in Risk Scores (PE) by gender.

Levene's Test for Equality of Variance of the Risk Score shows $F=0.39$; the significance of variances is 0.843. The t-test for equality of means displays $t=1.850$, and the degree of freedom= 198, when $p = 0.066$.

The researcher conducted an independent-samples t-test to compare the employees' risk scores for males and females. There were no significant differences ($t(198) =1.850$, $p=> 0.05$) in scores. Male scores ($M=25.074$, $SD = 5.9022$) are higher than Female ones ($M = 23.518$, $SD = 5.9522$). The mean difference (which is 1.5563. 95% CI: -.1026 to 3.2152) was minimal. Hence H2 was not supported.

RQ3: Is there a relationship between the length of the training period and employees' risk scores?

To answer this research question, the UTAUT variable (PE) Risk Score and the moderator (experience) were measured. This study suggests that the Pearson product correlation between the length of the training period (experience) and employee's risk score has no statistically significant relationship ($r = -.036$, $p >.05$) . Hence, H3 was not supported. The results show that there was a markedly low and negligible negative correlation between them.

6. Summary, Discussion and Implications

6.1 Discussion of Findings

The test conducted was Pearson Correlation to find the relationships between the employees' risk score and AI-based security programs' training effectiveness. Based on the results, we reject the null hypothesis because there is a significant relationship. In the area of length of training, we accept the null hypothesis because there is no significant relationship. An independent t-test analysis revealed that there are no differences between the risk score by gender. In that case, we accept the null hypothesis.

6.2 Practical Assessment of the Research Questions

The results of this study might urge practitioners to consolidate the UTAUT motivators within information security awareness training to enhance training strategies and techniques to resist cyber-attacks. Additionally, practitioners can incorporate all the motivators into expanding security awareness training material to augment training applications. Therefore, all the employees will be provided with an appropriate training program with considerable awareness of information security's significance.

6.3 Limitations of the Study

The study was limited by the fact that responses came from participants of two different industries, which means that finings may not apply elswhere. Moreover, the study used a survey to determine the correlation between the risk scores and the effectiveness of AI-based security awareness training. A survey's application proposes intrinsic limitations, such as participants' perception and understanding in answering the questions. The questionnaire cannot determine any outcome as it is only data accumulated based on the questions asked; there were no opportunities to ask follow up questions or observe non-verbal responses.. Another flaw was the lack of other media that could influence intention, like social connections, organizational engagement, and perseverance.

6.4 Implications for Future Study

While prior research examined the significance of security awareness training and organizational responsibility on behavior intention from a protection motivation viewpoint, the current investigation goes farther in analyzing the correlation between the UTAUT variables moderated by security awareness training and behavior intention for two different organizations [14, 18]. Researchers can apply this study's conclusions to enhance awareness of the consequences of protection motivators on behavior intention. The findings herein highlight the importance of learning the vulnerabilities an organization has and the inherent perils in employees' decision-making.

Experts should review the training approach, strategy, organizational responsibility culture, information security, and delivery methods. Overall, the outcomes showed that the AI-based security awareness training program positively affected behavioral intention within UTAUT. Further research can examine Fortune 500 and non-Fortune 500 companies' employees' behavior intention to monitor the UTAUT variables and the inherent consequences of information security awareness training. An added recommendation is to conduct pre-and post-testing after completing awareness training in diverse contexts, procedures and performing operations to measure AI-based security awareness training effectiveness more ultimately

7. Conclusion

Organizations that implement cybersecurity awareness training programs and use artificial intelligence can effectively provide awareness among their employees. Machine learning identifies patterns and shows possibilities. Deep neural networks deliver niche lessons for individual employees and those in particular areas. In today's technological world, the effective use of technology helps in protecting patient information. Every organization can improve its security by training the staff with appropriate cybersecurity awareness, implementing a robust control system, and enhancing online security. Managers should also be aware of the various cyber-attacks and how to handle them. With the best cyber practices, healthcare organizations can become immune to many, if not all, cyberattacks [11]. Information system interpreters in each organization are accountable for providing this type of cyberlearning to the employees, assuring they are mindful of the risks inherent in cyberspace and making intelligent decisions to resolve those threats for the organization's best interests [17]. Every organization has its weak link, which is the easiest target for cybercriminals.

This research intended to recognize the effectiveness of AI-based security awareness training programs and employees' risk scores relationship and how it affects behavior intention. As per the findings, the relationship between the employees' risk scores and AI-based training effectiveness is statistically significant. On the other hand, there are no differences in employees' risk scores by gender. Lastly, there is a negative correlation between the training period's length and employees' risk score. Therefore, based on the analysis, organizations should provide an appropriate training program with a considerable understanding of their employees' information security awareness. This study's practical inferences can provide businesses with the insight to implement adequate security awareness training programs.

REFERENCES

[1] F. Aloul, “The need for effective information security awareness,” Journal of Advances in Information Technology, vol. 3, pp. 176-183, 2012. Retrieved from http://www.jait.us/

[2] D. Ashenden and A. Sasse, “CISOs and organisational culture: Their own worst enemy?” Computers & Security, vol. 39, pp. 396-405, 2013. doi:10.1016/j.cose.2013.09.004

[3] M. Bada, A. M. Sasse, and J. R. Nurse, “Cybersecurity awareness campaigns: Why do they fail to change behavior?” arXiv preprint arXiv:1901.02672, 2019.

[4] K. A. Barton, G. Tejay, M. Lane, and S. Terrell, “Information system security commitment: A study of external influences on senior management,” Computers & Security, 59, 9-25. doi:10.1016/j.cose.2016.02.007, 2016.

[5] J. H. Bullée, L. Montoya, W. Pieters, M. Junger, and P. H. Hartel, “The persuasion and security awareness experiment: Reducing the success of social engineering attacks,” Journal of Experimental Criminology, vol. 11(1), pp. 97-115, 2015.

[6] L. Cheng, Y. Li, W. Li, E, Holm, and Q. Zhai, “Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security, 39, 447-459. doi:10.1016/j.cose.2013.09.009

[7] A. G. Chin, U. Etudo, and M. A. Harris, “On mobile device security practices and training efficacy: An empirical study,” Informatics in Education, vol. 15(2), pp. 235-252, 2016. doi:10.15388/infedu.2016.12

[8] B. Hanus and Y. A. Wu, “Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective,” Information Systems Management, vol. 33(1), pp. 2-16, 2016. doi:10.1080/10580530.2015.1117842

[9] W. He, et. al., “Improving employees' intellectual capacity for Cybersecurity through evidence-based malware training,” Journal of Intellectual Capital, 2019.

[10] P. Ifinedo, “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory,” Computers & Security, vol. 31(1), pp. 83-95, 2012. doi:10.1016/j.cose.2011.10.007

[11] L. Kim, “Cybersecurity awareness protecting data and patients,” Nursing Management, vol. 48(4), pp. 16–19, 2017. doi: 10.1097/01.NUMA.0000514066.30572.f3

[12] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, “Smart airport cybersecurity: Threat mitigation and cyber resilience controls,” Sensors, vol. 19(1), p. 19, 2018. doi:10.3390/s19010019

[13] O. J. Olusegun and N. B. Ithnin, “People are the answer to security: Establishing a sustainable information security awareness training (ISAT) program in organization,” International Journal of Computer Science and Information Security, vol. 11, pp. 57-64, 2013.

[14] N. S. Safa, et. al, “Information security conscious care behavior formation in organizations,” Computers & Security, vol. 53, pp. 65-78, 2015. doi:10.1016/j.cose.2015.05.012

[15] B. A. Savage, “A qualitative exploration of the security practices of registered nurses,” unpublished.

[16] P. J. Steinbart, R. L. Raschke, G. Gal, and W. N. Dilla, “SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs,” Journal of Information Systems, vol. 30(1), pp. 71-92, 2016. doi: 10.2308/isys-51257

[17] S. D. Pawlowski and J. Yoonhyuk, “Social representations of cybersecurity by university students and implications for instructional design,” Journal of Information Systems Education, vol. 26(4), pp. 281–294, 2015.

[18] C. Posey, T. L. Roberts, and P. B. Lowry, “The impact of organizational commitment on insiders' motivation to protect organizational information assets,” Journal of Management Information Systems, vol. 32, pp. 179-214, 2015. doi:10.1080/07421222.2015.1138374

[19] V. Venkatesh and F. D. Davis, “A theoretical extension of the technology acceptance model: Four longitudinal field studies,” Management Science, vol. 46(2), pp. 186-204, 2000.

[20] V. Venkatesh, J. Thong, and X. Xu, “Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology,” MIS Quarterly, vol. 36(1), pp. 57-178, 2012.