David Levy

Professor Demirel

CYSE 425W

1 December 2023

Security Awareness Training

Currently, security awareness training is considered one of the main pillars for building resilient organization's shields against cyber threat issues. The necessity for instructing people in an organization on matters related to cybersecurity is critical in a period when the digital world changes frequently, coupled with numerous complex types of cyber attacks. The question of security awareness training assumes key importance in the context of this study, serving as a basis for understanding how organizations should deal with security issues while working within this complicated technological and human environment.

"Don't click: "Assessment of a Security Awareness Training: Towards an effective anti-phishing training," is a comparative literature review that seeks ways of examining the effectiveness of security awareness training, particularly on phishing attacks' mitigation. This research involves various methods that include experiments in the field, simulations, and surveys based on scenarios. For example, an assessment of the effectiveness of compulsory phishing training for at risk employees of the US healthcare system emphasizes the need for continuous learning. Further, an experimental field investigates the effect of embedded training and consciousness in spear-phishing instances. However, the evaluation goes beyond normal mechanisms utilizing such things as emotional appeal as well as user context so as to improve the training outcome. These policy assessments provide broad implications of what should be attended to. This highlights the importance of considering all aspects of human factors and thus completely changing security education in fighting phishing. This is why it is important to adapt training procedures concerning cyberspace to individual differences. A multifaceted perspective on policy frameworks in cyberspace.

In the journal article, "Moving Beyond Cyber Security Awareness Training to Engendering Security Knowledge Sharing," professionals apply pre- and post-study survey analyses to evaluate participants' improvement on cyber security related terms. Others like Alotaibi et al. (2018) address the development and assessment of interactive approaches such as mobile gaming to enhance awareness with a particular emphasis on strong password usage as well as virus protection strategies. (Safa et al. (2017) also stress that collaborative studies are rare in organizational cybersecurity including that of the latter as a significant risk mitigation practice. Policy assessment conducted in these studies not only evaluates the current security measures but also generates important policy enhancement implicatures. Intrinsic motivation is needed to curb insider threats as noted by Safa et al. (2018) who suggest a model. In this regard, the comprehensive approach deployed by these experts in promoting good practices of cybersecurity within organizations characterizes a multifaceted strategy in terms of reviewing and fortifying security awareness and policies.

The "Implementing Effective Cyber Security Training for End Users of Computer Networks" study uses a comprehensive mechanism to determine how effective security awareness training programs are. The researchers use such options as audience-based surveys, perceptual taxonomies, and simulated exercises to reveal the degree of how to inform their managers regarding the gaps in the knowledge base as well as personalized programs. This paper covers how Science and Practice are integrated and it is the main functions of a collaborative relationship between Human resources professionals. During the policy assessment, an alignment of organizational practices should be done with industry best practices to establish gaps. These assessments provide other areas of policy implications allowing the firms to tweak their strategies of cybersecurity. This iterative process allows the alignment of training objectives with current threats so that employees are equipped with skills to detect and stay ahead of cyber threats.

The method that I would use to measure the effectiveness of the security training takes a few aspects from these sources. For starters, I would have everyone take a baseline test to see the specific areas that need attention in the training. Next, I would have everyone take a survey to determine their preferred learning style and create separate programs that cater to the main learning styles. Then, training would be recurring monthly rather than just when they join the organization. Before each of the training sessions, the members would take another test to help determine whether this method of training was producing favorable results. Another method to determine effectiveness would be to hire a penetration tester and see how the employees responded to a simulated attack. I believe that his method would ensure that everyone stays vigilant and makes the organization more secure as a whole.

Conclusively, the study reviewed and pointed out that security education is multi-faceted and requires lifelong learning and personalized strategies and employing new techniques in this case, mobile games. These studies highlight how best policy review, integration and self-motivation approaches can be applied holistically in containing insiders' threats. Taking into account relevant literature, the suggested way of evaluating the efficiency of training is based on a dynamic model. Organizations can make their training program more suitable by doing baseline testing, designing programs for learning styles, continuous training, and simulating attacks so as to be strong. The aim of this holistic approach is not just to improve awareness of one individual, but to create a culture of security consciousness within the organization that matches the best practice in the industry.

Works Cited

Alahmari, Saad, et al. “Moving Beyond Cyber Security Awareness and Training to Engendering Security Knowledge Sharing.” *Information Systems and e-Business Management*, vol. 21, no. 1, Oct. 2022, pp. 123–58. https://doi.org/10.1007/s10257-022-00575-2.

Beyer, Richard, and Bradley Brummel. “Implementing Effective Cyber Security Training for End Users of Computer Networks.” *HRM-SIOP Science of HR Series*, www.shrm.org/hr-today/trends-and-forecasting/special-reports-and-expert-views/Documents/SHRM-SIOP%20Role%20of%20Human%20Resources%20in%20Cyber%20Security.pdf.

Bhaskar, Ranjit. “Better Cybersecurity Awareness Through Research.” *ISACA*, 18 May 2022, www.isaca.org/resources/isaca-journal/issues/2022/volume-3/better-cybersecurity-awareness-through-research. Accessed 1 Dec. 2023.

Jampen, Daniel, et al. “Don’t Click: Towards an Effective Anti-phishing Training. A Comparative Literature Review.” *Human-centric Computing and Information Sciences*, vol. 10, no. 1, Aug. 2020, https://doi.org/10.1186/s13673-020-00237-7.