Human Vulnerability Mitigation Measures

Everyone within an organization is a potential target for cyber threats through email phishing attacks, social engineering attacks, and the variety of other developing cyber threats. This makes good cybersecurity practice the responsibility of everyone within an organization. It is important to make sure that the personnel of an organization have the tools that they need to be able to meet that responsibility and this starts with proper cybersecurity education and training. This training should be an ongoing process that begins when the employee begins work at the company and continues on throughout their time with the organization as the cyber threat landscape changes.

Who Should Be Required To Go Through Training

- Cybersecurity is not just the responsibility of the employees in your organization's IT department. It is the responsibility of everyone within your organization. It is reported that 90% of data breaches are the result of human error according to a 2017 study. With that being the case it is important to make sure that everyone has the training that they need to identify cyber threats when they see them and respond accordingly. This covers everyone from the board of directors of an organization, to the department heads, to the front line employees, to the interns within an organization (NH Products. 2019).

Start Early With New Employees

- It is important to make sure that new employees are familiar with your policies. New employees may bring with them poor cyber security practices from prior places of employment and need to be brought up to speed with your policies and procedures. This can be most effectively done through the onboarding and orientation process of new employees through an engaging training process (2019. Thycotic).
- Make it clear to new employees that good cybersecurity practices are a part of the organization's culture and that each employee plays an important role in maintaining the cybersecurity of the organization. This applies to all employees, not just those with an IT job function. However, those with an IT job function should be encouraged to get some entry-level cybersecurity certification that would be appropriate for their job function (NH Products. 2019).

Ongoing Education

- Education of an organization's employees should not end with their initial orientation when joining the company. Cybersecurity education should be ongoing process given that the threats will continuously evolve over time. Cyber threats that were a major threat ten years ago may not apply today, while new threats have taken their place. It is important to keep your employees up to date about the everchanging landscape of cyber threats (The Security Awareness Company, 2017).
- Supplementary training materials, such as audiocasts, videos, screensavers, posters, factsheets, and newsletters reinforce to the adult learner that they are responsible themselves for cyber

security in their daily work. By providing on-going reinforcement of the organization's policies and best practices, these materials help create a workplace culture of awareness that will help thwart some of the most common intrusion attack methods. Jon Portzline says supplementary training aids "serve two main purposes. The first is to drive engagement, while the second is to drive learner retention. By utilizing supplemental content in conjunction to the overall training program, security awareness professionals can provide small engaging pieces of content in quick bursts that helps to reiterate to learners the proper security awareness behaviors. Making things small that remind your learners about what has already been taught, helps to build retention without disrupting the flow of a learner's normal workday" (SANS Security Awareness, 2019).

- Ongoing training is commonly done on annual basis. However, it can become important to reinforce good practice on a 90 day rotation for employees with a specialized job function. A good example of a specialized job function may include anyone who handles sensitive information such as personnel files, client records, or other potentially sensitive information that needs to be kept secure (Infosec Resources, 2016).
- In 2012 Dr. Karen Quagliata conducted research on the aspects of security awareness training that have the most significant impact on security effectiveness. Dr. Quagliata recommended that employees conduct training at least yearly. Additionally, she identified that only providing training at new employee orientation was insufficient and that when training is voluntary, it has a negative impact on the perceived security effectiveness of the organization. As an educator, Dr. Quagliata emphasized that any security awareness training program should be sustainable and repeatable, that humans learn better when they are exposed to a message repeatedly, and an organization's security awareness training program is a long-term investment in the security of the organization (Quagliata, Karen. 2012).

Topic Areas of Focus

- "Staff training is essential in raising awareness among personnel and motivating them to pay attention to cyberthreats and countermeasures-even if they are not part of their specific job responsibilities. Installing updates, ensuring that anti-malware protection is on, and managing personal passwords properly shouldn't always be at the bottom of an employee's to-do-list" (Daily English Global blogkasperskycom, 2019). There are ten key areas of focus that should be included in training for employees. Usage of removable media, bring your own device policies, safe internet habits, social networking dangers, email scams, malware, hoaxes, data management, physical security and access controls, and clean desk practices. By covering these various topics and how they are applied within their organization employers will better prepare their personnel to prevent potential cyber attacks against their organization (Infosec Resources, 2019).

References

"5 Reasons Your Security Awareness Program Needs Continuous Learning • The Security Awareness Company." 2017. The Security Awareness Company. https://www.thesecurityawarenesscompany.com/2017/07/13/5-reasons-security-awareness-program-needs-continuous-learning/ (October 22, 2019).

Administrator, NH Products. 2019. "How to Get Employees on Board With Cybersecurity Awareness Training." New Horizons Worldwide. https://www.newhorizons.com/article/how-to-get-employees-on-board-with-cyber-awareness-training (October 22, 2019).

"New Hire Onboarding Checklist: A CISO's Security Perspective." 2019. Thycotic. https://thycotic.com/company/blog/2019/03/12/new-hire-onboarding-checklist-security-perspective/ (October 22, 2019).

"The Human Factor in IT Security: How Employees Are Making Businesses Vulnerable from Within: Kaspersky Official Blog." Daily English Global blogkasperskycom. https://www.kaspersky.com/blog/the-human-factor-in-it-security/ (October 23, 2019).

Quagliata, Karen. 2012. Impact of Security Awareness Training Components on Security Effectiveness: Research Findings. March 27. https://csrc.nist.gov/CSRC/media/Presentations/Impact-of-Security-Awareness-Training-Components-o/images-media/fissea-conference-2012_quagliata.pdf

"Security Awareness Course Design Best Practices." 2016. Infosec Resources. https://resources.infosecinstitute.com/security-awareness-course-design-best-practices/ (October 22, 2019).

"Top 10 Security Awareness Training Topics for Your Employees [Updated 2019]." 2019. Infosec Resources. https://resources.infosecinstitute.com/top-10-security-awareness-training-topics-for-your-employees/ (October 22, 2019).

"The Science of Adult-Learning: Five Minutes with the SANS Director of Content, Jon Portzline." SANS Security Awareness. https://www.sans.org/security-awareness-training/blog/science-adult-learning-five-minutes-sans-director-content-jon (October 22, 2019).