A Study of the Impact of Digital Ownership & Responsibility in Cyber Awareness & Training

CSIS 462

Professor Bansley

James Riley Dorough

Liberty University

March 22nd, 2022

**Introduction**

Threats to infrastructure and organization have always existed. With the advent of modern computing and the creation of a centralized networking standard; threats have taken on yet a new form. Digital threats have exploded to prevalence over the last couple decades. The sophistication of *cyber security threats* has increased exponentially paralleling the sophistication, complexity, and capacity of defensive entities in the cyber security industry. Continuous conflicts in the digital domain at varying levels of impact to organization, corporation, and effectively non-combatants in scope of attacks have fueled the development of numerous policies. Governments and authoritative bodies have drafted revision after revision of evolving policy, doctrine, best practices, and security recommendations. Additional vendors and third parties have thrown their preverbal hats in the ring to bolster such digital security regulation with their own experience. These third-party entities can be accessed with a few strokes of a keyboard providing quick and applicable security recommendations or policy as both a security vendor and free. Metrics for any time range and documentation of trends in security reporting metrics can be found to include future predictions. However, even with a mountain of resources for cyber defense; organizations are still suffering attacks, breaches, and data leaks at incredible rates. One might wonder why with all this support from the *good guys*, why are organizations at such risk still. Employees in an organization who are not directly responsible for implementing cyber security controls and maintaining good security posture may not even be aware of the severity and magnitude of digital threats. Adversaries to an organization have many vulnerabilities to exploit to reach their goals. One of the most commonly exploited vulnerabilities is human weakness. It can often be agreed upon that human are the weakest link in any system, especially digital ones. Humans are prone to mistakes and if not properly trained may open the door for attackers to gain easy access to infrastructure. Many controls are available to minimize threats to human involvement in organizational operation. Yet, you can never fully remove the risk that humans pose to security unless humans are fully removed from this domain. Since that is impossible and most likely will remain the case for many years to come, security focused individuals must develop methods of lowering this risk to more acceptable levels. This paper delves into various attacks that are implemented against humans in organizations, researching and analyzing current mitigation controls to combat these threats, and will explore cyber awareness training and responsibility as a potential option to thwart attempted cyber-attacks.

**The Underlying Threat to Cyber Security**

Because humans remain the weakest link in security infrastructure, Tactics, Techniques, and Procedures (TTPs) have been developed to assist in minimizing the amount of risk posed by human fault (He & Zhang, 2019). Of these TTPs some focus on instruction of the nature of cyber threats, others choose to train members of organizations to recognize and manage threats, and yet more are tailored to those already aware of threats but must remain up to date on the current evolution and activity of cyber threats. The cyber security industry has, on average, admitted to a shortage of quality security engineers or workers to stand up against the increasing frequency and sophistication of cyber threats (Kam et al., 2021). This overlaps into risk for an organization as not only is there a current perceived shortage of cyber security employees, but untrained and unaware non cyber focused employees have less material or personal dedicated to training them in cyber topics. Where applicable, organizations should rely on existing cyber awareness training TTPs. Many larger organizations and those working with the Department of Defense (DOD) have implemented effective training and evaluation utilities for keeping their workforce in tune to current threat vectors.

**Attack Vectors & Their Impact on Human Negligence**

All industry is vulnerable to specific attacks. Most notably are attack vectors which prey on the weakness of human involvement in an organization. There exist a large variety of these types of attacks. Due to the vulnerability of employees with minimal awareness of cyber security concepts or threats, attackers often look for holes in security left open by these employees. There is no need to struggle to break into digital systems and remain hidden from intrusion detection systems (IDS) when simply sending an attack to an unaware worker with legit system access is much quieter and easier. The methods for these attack vectors are often social engineering, phishing to include spear phishing and whaling, man in the middle (MitM), and possibly physical attacks though intrusion into an office or workspace or even dumpster diving for data. These attacks pose major risks to organizations as cyber forensics and incident response will have a much more of a challenge to find a trail of information when intrusions begin with completely analog methods. Therefore, social engineering is often a go to for malicious actors. Organizations need to be aware of the framework that social engineering attacks rely on to assist in planning cyber training programs for their workforces. The effectiveness of social engineering attacks is supported by a foundation of psychologically proven attributes (Mouton et al., 2016). These attributes are consistently boiled down to friendship, familiarity, and comfort to improve likelihood of information leakage (2016). Commitment and consistency which fosters a sense of trust beyond simple familiarity. Scarcity invokes a sense of urgency and can interrupt a victims decision making cycle. Reciprocity which requires prior trust to be exploited. Social validation among the culture of the target’s workforce. Lastly, abusing perceived authority can undermine many security procedures in an organization with poor adherence to such policy (2016). When the framework that attacks are understood and how they impact an organization’s workforce, training methods can be generated or evolved to fit ever changing attack methodology. Today, many organization currently implement security awareness training with a wide breadth of topics for employees of varying competency and permissions.

**Mitigation Policy, Methodology, & Operations**

Every organization can gain differing value from various implementations of cyber training curricula. However, simply instating a workforce Security Education, Training, and Awareness (SETA) program without proper oversight and management, and feedback throughout the process can simply waste the resources of the investing organization. Many SETA programs fail at meeting the expected level of retention in participants due to its methodology being rote and not often requiring participants to actively apply security concepts to solve problems beyond simple binary pass-fail response (Cone et al., 2007). Some major contributing factors to poor reception of SETA efforts are that most non-Cyber and non-IT employees would rather have their teeth puled than sit through monotonous death by PowerPoint, required study and testing, or nitpicking cyber professionals simply calling out employee failures to comply with security standards. It has been recorded that even with a rise in number of available SETA programs, the results only show a limited rate of success; far less than appropriate to dampen the impact of malicious cyber actors (Reeves et al., 2021). As an example, in context of mobile security, employees were recorded to have far worse performance and awareness when receiving frequent training (2021). This can be attributed to a mixture of poor training delivery, ill-fitting or non-applicable topics, overly frequent training which distracts from the normal flow of operations, and existing corporate culture.

Directly, SETA materials, TTPs, and existing training policy are not the issue with the lack of effect post training results or improvement in security. In fact, for a receptive workforce or a well-structured curriculum with opportunity for application; awareness training can be fully worth the effort. Organizations that nail proper incorporation and feedback for SETA can expect a drastic decline in failed evaluations or tests. Many modern organizations have begun to make solid progress toward effective SETA programming over the last decade. The majority of larger organizations, consulting firms, and organizations with ties to the United States Department of Defense (DOD) have somewhat recently shifted to change the culture around digital security and place due importance on its upkeep and evolution. Industry now even recognizes the entire month of October as “cyber security awareness month”. This improved effort in cyber security isn’t without reason, however. The aforementioned increase in frequency and complexity of successful cyber-attacks and the inclusion of large targets such as government, DOD, healthcare, banks, and critical infrastructure has caused major organizations to take another look at the importance of having capable staff in the cyber security field. Hiring qualified and experienced cyber security staff is critical. However, as touched on, ensuring that all remaining staff are aware of current security issues and which issues affect them is just as important. These organizations which have implemented SETA programs often do so with a separate team designated to conduct training sessions, testing, and feedback.

Efforts can be found to include various types of training and evaluation methods which can be broadly classified. Many third-party companies already exist which focus on implementing this Training as a Service (TasS). Some companies also offer Security as a Service (SaaS) to help take the effort off their clients. Even though SaaS does help make security easier for a company, it does not replace the need for effective training of non cyber security staff. Some of the tools in the arsenal of cyber security trainers include passive computer-based training (CBT) or web based training (WBT), interactive versions of training and interactive labs or simulations, strategic placement of physical awareness supporting material (signs, posters, handouts), and both local and distant cyber training seminars or training sessions which allow for question and answer sessions (Cone et al., 2007). In addition to these, testing or assessments can show employees grasp of the awareness and proficiency programs (*34 Resources for Employee Cybersecurity Training*, 2021). This list is highly abstracted from all the actual practices and utilities that exist today. However, using a properly constructed cycle of observing, planning, constructing, executing, assessing, feedback gathering, and adapting SETA responsible employees can build a training framework that fits the needs of specific organizations. There may be an additional layer that can prove much more effective than previous sets of beating cyber security into the minds of those who express no interest or poor understanding of the topic.

**Responsibility Training & Ownership as a Mitigation Concept**

The concept of responsibility is often understood to be a key motivation for many people in important, high risk, or public service positions. If you consider your own actions and focus on what you believe you have a responsibility to you should be able to recognize a pattern of stressed effort in areas in which you hold responsibility. A common example would be simply the duties expected of you in your current job. As an employee or member of a workforce at any level or industry you most likely feel that if you fail at your assigned tasks, you will be held responsible for the outcomes of such efforts. One of the most extreme examples of responsibility is the US military. Time and time again the public hears heroic stories of surviving, injured, or fallen warfighters, who in effort of completing a mission, were able to generate extraordinary determination and will power. Should you ask people of this nature how or why they accomplished these feats they will often describe some level of responsibility whether it be to a unit, to their country, to the defense of their family and friends, or to the mission.

I believe that this innate drive found in humanity can be tapped to bolster cyber security as a whole. Often the value and importance to the organization that proper security posture provides does not translate well to lower-level members of such an organization’s workforce. One such method to provide an organization’s workforce with a sense of responsibility is to provide them a position of stakeholder in the success of the company (Delgado Ferraz & Gallardo-Vázquez, 2016). As is seen today, simply the knowledge that being accountable for a breech in security is nowhere near effective enough to discourage poor security practice. If organizations begin reshaping the culture of their workforces into a sense of ownership and responsibility of effort and action, it is proposed that SETA programs may have an improved effect. Employees would understand that by failing to meet good security practice, they are placing not only their lower position and the income of the C-suite at risk, but also the livelihoods of their team members and any other entities that a breech in security would affect. To accomplish this current SETA curricula would not need to be disregarded. Training professionals can incorporate the essence of responsibility into current training methodology. At the very least, frequent communication and solid leadership can bolster the sense of ownership and responsibility that each member of a workforce has to the other members of their teams. This can be expected to improve the effectiveness of current SETA standards and lead to the next generation of cyber aware employees; ready to incorporate best practices into their daily operations and personal lives.

**Conclusion**

Cyber security awareness training and SETA programs are effective at pruning much of an organization’s low hanging fruit. However, the complexity of modern attacks makes effective training of organization’s workforces much more critical to the survival of these organizations. Bad actors can completely evade digital security and IDSs if they can gain a foothold from an untrained or unaware staff member or employee of an organization. Because of this, many styles of SETA training programs have been implemented. Yet, the populous still hears of data leaks and breeches from large corporations on a nearly daily basis. Such training is critical to minimize the frequency of attacks, but a more effective training method is still needed. This document proposed that a focus on the responsibility and impact that employees can have when overlooking or undervaluing their access to systems into a training program can bolster the effectiveness and retention of training materials. The hope is that by reshaping workforces into a team mentality with a shared responsibility to the unit and their coworkers, security incidents will be less likely to occur and employees are capable of assisting their fellow team members in good security practice.

**References**

*34 Resources for Employee Cybersecurity Training*. (2021, November 10). SecurityScorecard. Retrieved April 6, 2022, from <https://securityscorecard.com/blog/resources-for-employee-cybersecurity-training>

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, *26*(1), 63–72. <https://www.sciencedirect.com/science/article/pii/S0167404806001556?via%3Dihub>

Delgado Ferraz, F. A., & Gallardo-Vázquez, D. (2016). Measurement tool to assess the relationship between corporate social responsibility, training practices and business performance. *Journal of Cleaner Production*, *129*, 659–672. <https://www.sciencedirect.com/science/article/pii/S0959652616301755?via%3Dihub>

He, W., & Zhang, Z. J. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249–257. <https://www.tandfonline.com/doi/full/10.1080/10919392.2019.1611528>

Kam, H., Ormond, D. K., Menard, P., & Crossler, R. E. (2021). That’s interesting: An examination of interest theory and self‐determination in organisational cybersecurity training. *Information Systems Journal*. <https://onlinelibrary.wiley.com/doi/full/10.1111/isj.12374>

Mouton, F., Leenen, L., & Venter, H. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186–209. <https://www.sciencedirect.com/science/article/pii/S0167404816300268?via%3Dihub>

Reeves, A., Calic, D., & Delfabbro, P. (2021). “Get a red-hot poker and open up my eyes, it’s so boring”1: Employee perceptions of cybersecurity training. *Computers & Security*, *106*, 102281. <https://www.sciencedirect.com/science/article/pii/S016740482100105X?via%3Dihub#bib0037>