Contents

Cybersecurity: Bridging the gap between training and the effective knowledge base of employees in cyberthreat mitigation

Jacob Cryer
Romaric Zoumlome

ABSTRACT

Since the invention of mobile devices (i.e., laptops, smartphones, tablets, laptops, and smart watches), a world of cybercrime and other threats have emerged. Just as these devices were created, so too was the Internet of Things (IoT) and the rapid development of Information and Communication Technologies sped their adoption in new countries with limited infrastructure. These conditions coupled with people who want infamy, chaos, sabotage and espionage makes cyber awareness and education more important than ever. The obligation falls to capital heavy organizations such as corporations and governments around the world. In this paper, we demonstrate the severity of cybercrime, the need to produce effective training methods, and institute effective cybersecurity programs at the professional level.

INTRODUCTION

Cybercrimes have devastating effects on world economies. In 2017, the average cost to an organization to manage cybercrime activities was $11.7 million (Security Magazine, 2018). For instance, Fischer Advanced Composite Components (FACC), an aerospace manufacturer in Austria, lost $54.5 million dollars in 2016 due to a data breach caused by hackers (Ashford, 2016). Centene Corporation, a healthcare company, was

similarly hacked and the attackers stole six hard drives full of personal healthcare information including social security numbers, usernames, and passwords of clients (Westgate, 2016). Seagate, a data storage company, had every single W-2 tax document stolen from its internal database, which included social security numbers, salary information, and various other data (krebsonsecurity.com, 2016). The Seagate attack was caused by a spear-phishing scam targeted at their CEO. The Internal Revenue Service (IRS), a U.S. government agency, was also hacked, with more than 700,000 accounts breached and information stolen (CBS News, 2016). Cyberattacks are a problem worldwide and the attacks are becoming more frequent and economically damaging. The problem is due to the multitude of entry points to organizational, and governmental information systems combined with the vast number of users who are targets for cyber criminals' scams. Other big businesses that have been hacked are Snapchat, 21st Century Oncology, Premier Healthcare, Verizon, Philippine Commission Elections, Wendy's, Yahoo, Dropbox, Cisco and Oracle (Armerding, 2017). There are many more businesses that could have been listed in the previous set of breaches and the number of businesses that experience cyberattacks will continue to increase. With the rate of breaches rising, it is worthwhile to investigate the methods that are being implemented to counter these threats and what measures are taken to ensure that professionals are being trained in an effective way.

Every breach poses the risk of monetary losses from three main costs e.g., the cost of temporarily closing a business to implement a Disaster Recovery Plan (DRP), the system integration expense caused by detecting and correcting breaches, and the cost accrued due to legal liability in the loss of sensitive data (Campbell et al., 2003). All three costs can occur from the lowest level of security defense, the uneducated end-user. When a business stops operating from any event many expenses are realized. For instance, the major cost of halting a business' operations is the loss of incoming revenue, and the decrease in a company's reputation, which will affect business-to-business activities when it reopens (Gordon, 2011).

Cybercrimes happen at a rate of 1.5 million per year, and roughly 47% of Americans had their identity stolen in 2014 (CBS Cyber, 2017). Cybercrimes still fly under the radar in regard to awareness and news coverage. More substantial is the 62% increase in the amount of cyberattacks from 2012-2013, which led to 594% more identities being stolen, and more than $18 Billion dollars in credit card fraud that year (CBS Cyber, 2017).

Phishing activities have resulted in the loss of an estimated $178.1 million from stolen credentials. Attackers used key loggers (a form of malware which records and stores victims' keyboard strokes and sends it to the attacker) to steal between $793,318- $16,604,605 (Alfroz, 2013). Phishing is a type of social engineering attack where a hacker uses a seemingly legitimate email link to trick users and ultimately steals their information (Fruhlinger, 2017). Once the users follow the link, or click on the attachment, they are unknowingly downloading another program that operates in the background of their computer. While online, nefarious individuals acquire users' personal information using such illegal means as phishing for monetary gains (Kim et al., 2011). Researchers noted that "One bank our team has spoken to said it cost them about $1 million per attack, in terms of call center costs, recovery costs, and actual money that could not be recovered" (Hong, 2012, p. 4).

The amount of information people post on social media, websites, and online shopping sites makes them more vulnerable to cyberattacks. There are an estimated 3.6 billion internet users worldwide, and this amount is growing everyday (Schultz, 2016). The rise of social media and other networking websites such as Twitter, Facebook, and LinkedIn, connects users more than ever before. Blogs, personal web pages, email, and YouTube enable users to connect from virtually anywhere in the world; but this connection comes with a price. The more information people upload onto the web, the larger the dataset cyber criminals have access to.

Beuran et al. (2016) analyzed Japanese cybersecurity programs and training methods to single out the most practical, efficient, and successful training techniques for new security professionals. The need to

perform such research developed in response to a National Center of Incident Readiness and Strategy report that displayed strong implication that cybersecurity professionals were not becoming competent in their discipline. The official document reported nearly 50% of cybersecurity professionals reviewed would require additional in Japan and that the workforce will be in a deficient of 80,000 workers (Beuran et al., 2016).

Based on the preceding discussion and because of the severe consequences of cybersecurity attacks, we believe that there should be additional training programs and schools created worldwide to help combat cybercrimes and breaches. Each program should focus on real-world scenarios and hands-on projects that will properly prepare students for real-life attacks. We believe that it is necessary to highlight training methods intended to reduce cyberattacks and evaluate their effectiveness. Therefore, we will present the most impactful and significant methods that help organizations of varying sizes and cultures to train their workforces.

TRAINING METHODS FOR EMPLOYEES

In this section, we present different types of training that should be used by organizations to improve the awareness of their employees. It should be noted that different orgnizations may need one or more of these types of training. Also, organizations should tailor these training methods to best fit their size and resources.

MILITARY

Cone et al. (2007) performed research and analysis on the Naval training simulation CyberCIEGE. This is a simulation video game that places the player in real-world scenarios designed to teach them awareness principles, basic information assurance techniques and illustrate the problems commonly found while using Information Assurance (IA) techniques e.g., monitoring the integrity, availability and confidentiality of a system. Within CyberCIEGE's design is a focus on information security and assurance training advancement. In real time gameplay, the player (i.e., the end user) is assigned the role of a ship's security officer and asked to complete levels and objectives to advance the ship's security level. Penalties are attached to failure to accomplish a goal within the designated time frame. Once players have completed an objective they receive level feedback on choices made as the security officer and they are expected to convey the principles and skills learned during the simulation activity. Cone et al. (2007) critique the CyberCIEGE video game and conclude that not enough research has been done on the CyberCIEGE game and its effectiveness. At the time of their research in 2007, they indicated CyberCIEGE was about to be released to over a hundred universities.

Adams and Makramalla (2015) compiled research on effective methods to teach employees cybersecurity skills and create a cybersecurity aware workforce. Their method was to analyze group video-game training programs based on four elements: progress mechanics, player control, problem-solving, and story (Adams & Makramalla, 2015). Among their reviewed gaming platforms were CounterMeasure, CyberCIEGE, CyberNexs, CyberProtect, NetWars, and Micro Games. The researchers then rated the games on their ability to create awareness, effective defensive and offensive strategies, and attacker centricity (Adams & Makramalla, 2015). The literature on this review extends beyond the previously stated examined aspects. Adams and Makramalla (2015) concluded among all the different elements that these cybersecurity training games use, the presence of an avatar, varying attacker types, and story allows the end-user to become aware of hackers' motives and infers enhanced education.

Based on the above literature, we believe that there are three aspects of cybersecurity training games that enhance the trainee's education and retention. Aspects such as avatar creation, a large scope of attack types, and an in-depth story could be integrated into employee training. A game designed to teach employees to handle cybersecurity attacks while implementing these effective game components could create a superior end-user when it comes to mitigating cyber threats.

GAME-BASED

Abawajy (2014) has studied delivery methods to train end users to handle sensitive information, determine email threat levels, and become an active defense when involved with identifying possible cyber threats. The study's examination was reduced to three primary delivery methods, i.e., game-based, video-based, and conventional methods. Abawajy

(2014) collected data from 60 participants. Twenty percent of the participants had some prior cybersecurity training and 60% enjoyed video games. The data collected indicated the extent of the participants' computer familiarity, technical knowledge to prevent cyber-attacks and the limits of their prior knowledge. Abawajy (2014) created quizzes to assess each delivery method's effectiveness in educating the user. Their results determined that the participants preferred video-based delivery methods, but the combination of all three methods was the most successful in creating a productive learning experience (Abawajy, 2014).

Abawajy (2014) implies that cybersecurity training programs should use a mixture of video, game, and conventional methods to education the end-user. The three delivery methods could be utilized in corporate cybersecurity training programs to create an environment conducive to learning and reduce training costs in the long term through reductions in the time to train employees. If employees are trained effectively and efficiently then this will reduce the need for retraining employees. The research also infers that the end-user may prefer one method, but this is not a clear indication that it is the optimal method to be used for training. Employee training programs should use a blended education program to optimize the success of training and reduce the need for future retraining.

Hight (2005) quoted Albert Einstein as once saying, "Problems cannot be solved with the same level of awareness that created them" (Hight, 2005). This quote applies to the methods that need to be designed and implemented to train end-users to become an effective "human firewall" against cyber threats. Hight (2005) examined the usage of technology and the importance that needs to be placed on the employees to become an effective defense against cybercrime. Through the review of Security Education, Training and Awareness (SETA) programs, she evaluated information security training within organizations and the limited degree of awareness among employees when faced with cyber threats at their organization. SETA programs have been defined as "an educational program that is designed to reduce the number of security breaches that occur through a lack of employee security awareness" (Hight 2005, p. 1). Purposefully designed, the SETA programs are meant to instill the perception employees need to have or acquire through information security

training (Overfelt, 2016). Hight (2005) concluded that a failure to implement a strong foundation of cyber knowledge in which to counter information theft would be catastrophic to an organization. They highlight three pivotal fundamental countermeasures in the defense against cyber threats: technology (hardware and software knowledge), operations (business process knowledge base), and various levels of knowledge through awareness programs, training, and education.

If businesses integrate these fundamentals through a progression of program difficulty then the research indicates employees will be able to mitigate cyberattacks (Hight, 2005). When these concepts can be integrated into training programs, organizations will see a reduction in costs associated in training and retraining employees in cybersecurity and other training programs.

CLOUD-BASED

Trickel et al., (2017) review the use of shallweplayagame.org (SWPAG), which is a website designed to be a secure cybersecurity learning environment. This takes the form of a Capture the Flag objective-based game where cyber security professionals of the future compete with each other to win the game and in doing so advance their knowledge base. SWPAG provides a platform that an IS instructor can provide to their students or employees to provide a safe and beneficial experience. Trickel et al. (2017) conclude that through open communication and advice via instructor-to-student and student-to-student provides the necessary conditions for active learning. Therefore, SWPAG is a useful tool for teaching students, but this method and application may be more suitable for the intermediate to advanced technology user.

ACADEMIC COMPETITION

Bashir et al. (2015) examined the effectiveness of competitions in teaching end-users and drawing prospective employees to the event to promote becoming a cybersecurity professional in the future. They argued that competitions were designed to enhance the self-efficacy of participants by pitting each participant against another in hopes that their competitive nature would raise the effectiveness of education. Studies

such as this can be skewed since the data are gathered from people who are outliers being that they are interested in cybersecurity before coming to an event and therefore likely have a strong propensity towards the information security world. However, Bashir (2016) provided corroboration that the attendees who were first-timers showed substantial improvement in the awareness level.

CYBERSECURITY AWARENESS CAMPAIGN

Bada and Sasse (2014) implement, examine, and critique their cybersecurity awareness campaign in the United Kingdom. They launched this campaign to single out internet users from the home to professional levels. Bada and Sasse (2014) "Get Safe Online" program was funded from both Governmental and private sector stakeholders, which is a clear indication of the interest, seriousness, and need for efficient cyber security education programs for all users. The Get Safe Online program provides practical counseling for users to learn safe Internet behaviors regarding the use of IoT devices and, at the same time, protecting the user's organization against fraud, identity theft, malware, and viruses. Bada and Sasse (2014) criticize the U.K. initiative for a number of its features. Their primary critique was the campaign's use of fear-inducing rhetoric to compel users to comply with recommendations. They believed that a learning experience should not use fear-based tactics and threats to encourage the user's self-efficacy. These awareness learning objectives should be presented without penalties and punishments attached to the point being made. Bada and Sasse (2014) conclude that creating a persuasive message through concern, caution, and threat mitigation could have been more conducive to produce a knowledge transfer reducing hacker's effectiveness in gaining sensitive information.

CONCLUSION

Global corporations have seen major financial loses because of increased frequency of cyberattacks. Effective cybersecurity training methods must be implemented, and cybersecurity policies must be followed to decrease the loss of revenue, intangible assets, and sensitive data. The business' first line of defense is the employee, which means that training is essential to prevent significant losses. Employees use social media while working, and post sensitive data to these sites, which is used by hackers to crack passwords. If effective cybersecurity training for employees is not implemented then the threat of cyber breaches will continue to rise. Employees need to be trained in a mixed learning environment to cover all learning styles. Organizations must consider implementing many types of training and be willing to revise training methods according to their workforce. This approach may increase employees' ability to stop threats and decrease the rate of data loss. Further studies need to be done to determine how employees are trained and how to create a more comprehensive training program. This is crucial to sustain a secure information system, which can be the difference between success and failure in the global business environment.

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237-248.

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: an attacker-centric gamified approach. Technology Innovation Management Review, 5(1), 5-14.

Armerding, T. (2017). The 16 biggest data breaches of the 21st century. Retrieved January 25, 2018, from https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html

Ashford, W. (2016). $54m cyber fraud hits aircraft supplier share price. Retrieved January 09, 2018, from http://www.computerweekly.com/news/4500271523/54m-cyber-fraud-hits-aircraft-supplier-share-price

Bashir, M., Lambert, A., Wee, J. M. C., & Guo, B. (2015). An examination of the vocational and psychological characteristics ofcybersecurity competition participants. Proceedings of the USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE).

Bashir, M., Memon, N. D., & Wee, J. M. C. (2016). Self-Efficacy in

Cybersecurity Tasks and Its Relationship with Cybersecurity Competition and Work-Related Outcomes. In ASE@ USENIX Security Symposium.

Beuran, R., Chinen, K. I., Tan, Y., & Shinoda, Y. (2016). Towards Effective Cybersecurity Education and Training.

Beuran, R., Pham, C., Tang, D., Chinen, K. I., Tan, Y., & Shinoda, Y. (2017). CyTrONE: An Integrated Cybersecurity Training Framework. In ICISSP, 157-166.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security, 11(3), 431-448.

Cyber Crime Costs $11.7 Million Per Business Annually. (n.d.) Retrieved January 09, 2018, from https://www.securitymagazine.com/articles/88338-cyber-crime-costs-117-million-per-business-annually.

Fruhlinger, J. (2017). What is phishing? How this cyber attack works and how to prevent it. Retrieved January 25, 2018, from https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs?. Journal of Computer Security, 19(1), 33-56.

Hight, S. D. (2005). The importance of a security, education, training and awareness program, November 2005. Retrieved 01 January 2018 http://www.infosecwriters.com/text_resources/pdf/SETA_SHight.pdf

Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74-81.IEEE Computer Society.

Kim, W., Jeong, O. R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. Information systems, 36(3), 675-705.

Krebs on Security. (2016). Retrieved January 09, 2018, from https://krebsonsecurity.com/2016/03/seagate-phish-exposes-all-employee-w-2s/

News, C. (2016). Massive IRS data breach much bigger than first thought. Retrieved January 25, 2018, from https://www.cbsnews.com/news/irs-identity-theft-online-hackers-social-security-number-get-transcript/

Ravi, V., Naveen, N., & Pandey, M. (2013). Hybrid classification and regression models via particle swarm optimization auto associative neural network based nonlinear PCA. International Journal of Hybrid Intelligent Systems, 10(3), 137-149.

Schultz, J. (n.d.) "How Much Data is Created on the Internet Each Day?" Archive Office 365 Email, Exchange, Social, Mobile & More! GWAVA, 08 Sept. 2016. Retrieved. 01 Apr. 2017. https://blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/

These Cybercrime Statistics Will Make You Think Twice About Your Password: Where's the CSI Cyber team when you need them? (n.d.). Retrieved April 08, 2017, from http://www.cbs.com/shows/csi-cyber/news/1003888/these-cybercrime-statistics-will-make-you-think-twice-about-your-password-where-s-the-csi-cyber-team-when-you-need-them-/

Westgate, A. (2016). Centene data breach underscores escalating problem. Retrieved January 09, 2018, from http://managedhealthcareexecutive.modernmedicine.com/managed-healthcare-executive/news/centene-data-breach-undersco