Security Training Program for Social Engineering

Joseph Perry

School of Cybersecurity, Old Dominion University

CYSE 494: Entrepreneurship in Cybersecurity

Professor Porcher

June 21, 2023

Security Training Program for Social Engineering

Introduction

Social engineering attacks have become one of the most significant threats to organizations in the 21st century. The prevalence of social engineering attacks has made it necessary for organizations to implement vigorous security measures. According to reports from ISACA, social engineering attacks were identified as the most prevalent attack type analyzed in 2022 (Crane, 2023). This trend highlights the efficiency and effectiveness of social engineering techniques utilized by cybercriminals. Social engineering attacks consist of a multitude of manipulative techniques like phishing, pretexting, smishing, and tailgating. Cybercriminals utilize these manipulative techniques to influence individuals into compromising security measures. Cybercriminals can bypass vigorous security measures by exploiting individuals as they are the weakest link in cybersecurity. The impact of social engineering attacks on organizations can be catastrophic. A successful social engineering attack can lead to financial losses, reputational damage, and legal consequences.

Cybersecurity has become necessary for organizations to be successful due to the inherent risks the rapid evolution of technology and connectivity has caused. Furthermore, cybersecurity plays an indispensable role in mitigating these risks and ensuring the protection of valuable assets. Organizations must recognize the significance cybersecurity has in protecting their operations, reputation, and stakeholder trust. As previously stated, a successful social engineering attack can lead to catastrophic consequences like financial losses, reputation damage, and legal consequences. To address the prevalence of social engineering attacks

targeting organizations, a comprehensive security awareness and training program must be implemented. This program aims to educate employees to identify and respond effectively to social engineering attempts made by cybercriminals. By improving employees' knowledge and awareness on social engineering attacks, organizations can significantly reduce the success rate of social engineering attacks on their organization.

The program will educate employees about the multitude of social engineering techniques, such as phishing, pretexting, smishing, and tailgating. Furthermore, training sessions will focus on recognizing the signs of a social engineering attempt, such as suspicious emails or phone calls, requests for sensitive information, and abnormal behavior. These training sessions will provide job-specific training on social engineering attempts relevant to employees' roles within the organization. The program will emphasize secure communication practices, employees verifying senders, utilizing encryption when appropriate, and using caution with untrusted links or attachments. Baseline cybersecurity practices, the use of complex passwords, frequent password changes, and multi-factor authentication, will also be emphasized to ensure a strong cybersecurity foundation. The program will establish proper incident reporting procedures. These incident reporting procedures will ensure that employees report any social engineering attempts or incidents to the appropriate personnel. Frequent social engineering simulations will be conducted to assess the effectiveness of the program and identify areas for improvement. These simulations will provide valuable feedback to further improve the program's efficacy and effectiveness. Since social engineering techniques continue to evolve, the program will have ongoing awareness campaigns and regular updates to keep employees informed about the state of social engineering techniques. Continuous training will be provided to ensure that employees stay up to date with evolving social engineering techniques. The

comprehensive security awareness and training program aims to mitigate the vulnerability of individuals as the weakest link in cybersecurity. It is essential for organizations to address these issues through security awareness and training programs. Understanding

Review of Literature

The article "Social Engineering: The Neglected Human Factor for Information Security Management" published in the Information Resources Management Journal describes social engineering as a combination of techniques used to manipulate victims into performing actions that compromise security (Luo et al., 2011). Furthermore, the authors argue that although technological measures have been developed to address security issues human factors that contribute to security breaches have not. According to the article, social engineering attacks rely on human cognitive biases. Furthermore, the helpfulness of human users and their psychological weaknesses are exploited for cybercriminals to be successful in these attacks.

The article discusses psychological aspects and personality traits that can be exploited by cybercriminals. It introduces concepts like diffusion of responsibility, trust relationships, and guilt. The article describes a multitude of social engineering techniques, including pretexting, phishing, and dumpster diving. Pretexting involves creating a scenario to manipulate victims into performing malicious actions. Phishing is a scam technique that obtains private information by impersonating emails that appear to be from a reputable sender. Dumper diving is when cybercriminals search through garbage to find items that contain sensitive information. To mitigate the risks of social engineering attacks, the article suggests a defense-in-depth approach that expands beyond technological solutions. As in social engineering technological solutions do not completely mitigate successful attacks. Furthermore, rather than only technological measures, policies, procedures, standards, employee training, awareness programs, and incident

response should be implemented. This article further delves into the psychoanalysis of Social Engineering and its effects on information security. The idea is that individuals' cognitive biases and psychological weaknesses are used heavily in social engineering attacks. Security awareness and training programs are critical in addressing these tactics used by cybercriminals. By integrating technical, managerial, and operational measures, organizations can create a safer work environment for all employees. Furthermore, this system must continue to adapt and grow as cybercriminals continue to find new avenues of success. The programs must continue to stay tailored to up-to-date information. This continuous adaptation will foster a secure-minded culture. This relates to the security awareness and training program by including technical, managerial, and operational measures.

The article "Social Engineering: A Literature Review" discusses the concept of social engineering and the role information security awareness programs have in addressing social engineering threats (Ghafir, Prenosil, Alhejailan, & Hammoudeh, 2016). The authors highlight that social engineering is the practice of exploiting human weaknesses through manipulative tactics. The article also emphasizes the concept that social engineering attacks target individuals instead of technical vulnerabilities and system protocols. The article suggests that raising information security awareness among users is necessary to combat social engineering threats effectively. It is necessary to provide all users with knowledge about information security threats and ensure users understand their responsibilities in the security process.

Furthermore, the security awareness and training program aims to educate users on information security and their role when an incident occurs. The article also explores the effectiveness of innovative information security education programs in increasing user and employee awareness and reducing cyber security incidents. Information security training

provides significant benefits in relation to overall employee satisfaction. Awareness and education programs have a positive impact on employees' attitudes and behavior toward information security. The article provides a comprehensive overview of social engineering and its implications in cybersecurity. Overall, information security awareness programs are important in combating social engineering attacks and enhancing user awareness which reduces the risks of cybercrimes.

This research paper provides an overview of social engineering attacks and provides suggestions for defense mechanisms in the context of information security (Salahdine & Kaabouch, 2019). Furthermore, it explains how social engineering utilizes manipulative techniques to exploit human psychology. It emphasizes that human emotions are both strengths and weaknesses regarding information security. For example, human emotions can be a strength that drives innovation, however, they can also be a weakness when it comes to decision-making and assessing risks in the context of technology. This further explains the duality of how human emotions have positive and negative effects on information security. The paper provides an in-depth explanation of understanding social engineering, awareness of vulnerabilities, defense approaches, the importance of training and awareness, and the attack framework model. The importance of training and awareness is evident. Although an organization invests resources and money in creating technical and managerial controls to improve its information security, if the employees are not aware of information security practices it is pointless. The security training and awareness program strives to make employees aware of the proper information security practices.

The article emphasizes the importance of information security awareness programs within organizations (Abawajy, 2012). The article mentions that employees within organizations

generally have varying levels of security awareness. Therefore, it is important that the security awareness and training program takes into consideration the differentiating levels of knowledge among employees. It is important that all employees can properly receive security awareness and training despite differentiating levels of knowledge. Furthermore, providing employees with information security best practices and role-based training is necessary. The article also emphasizes that employee behavior is the primary source of data breaches that result in catastrophic events. Negligence or malicious actions by employees typically lead to security incidents. The security training and awareness program addresses this issue.

Furthermore, the security training and awareness program focuses on changing employee behavior to reduce the risk of data breaches. The results of a study conducted by Dodge in 2007 assessed the effectiveness of training in increasing awareness of phishing attacks. The increased awareness of phishing resulted in a reduction in victims falling susceptible to phishing attacks. The article also emphasizes the importance of ongoing awareness and measurement to create a security-minded culture within an organization. Ongoing awareness and measurement consist of continuous effort, regular assessment, addressing evolving risks, engagement, communication, continuous training, and metrics and analytics. By creating a security-minded culture within an organization the risk of social engineering attacks decreases significantly.

The focus of this study was to investigate the relationship between individual differences and information security awareness (Bettinghaus et al., 2016). To analyze the relationship between individual differences and information security awareness the Human Aspects of Information Security Questionnaire (HAIS-Q) was utilized to measure information security awareness. The HAIS-Q assessed the knowledge, attitude, and behavior regarding information security policies and practices. The findings of the study yielded that age and gender held no

significant relationship with information security awareness. Furthermore, the findings of the study also resulted that personality traits had an impact on employees' knowledge, attitude, and behavior regarding information security. The personality traits that were found to have an impact on employees were conscientiousness, agreeableness, emotional stability, and risk-taking propensity. The study indicated that individuals with higher levels of conscientiousness are usually more aware and adhere to information security policies and practices. Individuals with higher levels of agreeableness are more likely to consider the importance of information security and follow the necessary procedures. Individuals with higher emotional stability were also more likely to consider the importance of information security and follow the necessary procedures. Individuals with higher risk-taking propensity were less likely to have higher levels of information security knowledge and follow the necessary procedures. These findings suggest that also understanding employees' personality traits can assist organizations in tailoring information security training programs to effectively enhance information security awareness. By providing comprehensive security awareness and training programs organizations will be able to effectively address these issues.

The focus of this study was to investigate the influence of social engineering strategies on users' judgments of the safety of clicking on links attached to emails (Butavicius, Parsons, Pattinson, & McCormac, 2016). The study focuses on phishing and spear-phishing emails. Phishing is the fraudulent practice of sending emails or other messages appearing to be from a reputable source to deceive individuals to reveal sensitive information. Spear-phishing is a targeted attack on one or more victims. An example of spear phishing would be an attacker sending fraudulent emails only to the financial department of a company. The study involved presenting users with emails that are authentic or phishing emails. Each email utilized different

social engineering techniques such as authority, social proof, scarcity, or none. Based on the provided emails participants were asked to determine the safety of the links attached. The study yielded that the authority strategy was the most effective and the social proof strategy was the least effective. The study also yielded those individuals had difficulties differentiating between genuine and spear-phishing emails. The study highlights the importance of educating users about social engineering tactics, such as authority, scarcity, and social proof. By raising awareness and providing training on recognizing these strategies, users can become less susceptible to phishing attempts. Additionally, the study also emphasizes how impulsivity and decision-making can influence users' susceptibility to phishing attacks.

The study emphasizes the critical role of security awareness and training in defending against social engineering attacks ("IEEE," 2019). It recognizes that humans are the weakest link in information security and the increasing prevalence of social engineering techniques that exploit human vulnerabilities. The biggest risk to information security lies in the actions or inaction of employees and organizational personnel that lead to security incidents. Furthermore, human error, lack of awareness, and social engineering vulnerabilities are all risks organizations face.

To mitigate these risks, it is important for organizations to recognize the importance of security awareness and training. By educating employees about threats, implementing security best practices, and promoting a security-minded culture, organizations can influence their employees to make decisions that do not compromise security. Frequent training programs, social engineering simulations, and continuous awareness about threats can decrease the likelihood of employees causing security breaches due to human error or manipulation.

The articles discussed in this research paper emphasize the importance of the relationship between social engineering and information security awareness. They highlight the multitude of social engineering techniques utilized by cybercriminals to exploit human weaknesses and the necessity for defense mechanisms that expand beyond technical solutions. Human factors play a significant role in security breaches. Furthermore, addressing this issue through the proper security awareness and training program is necessary.

Interdisciplinary Perspective

The problem of social engineering attacks targeting organizations has a strong connection to multiple concepts I covered in classes outside the cybersecurity major at Old Dominion University. Social engineering attacks have a strong connection to psychological, sociological, and behavioral concepts I learned while taking Psychology and Sociology. Social engineering is strongly connected to these concepts because it focuses on exploiting various cognitive biases, social dynamics, and human behavior to manipulate individuals. Furthermore, implementing these concepts into the security awareness and training program enhances its effectiveness in mitigating social engineering attacks.

Psychological theories play a critical role in understanding the behavior of attackers and victims. The manipulative techniques utilized by cybercriminals in social engineering attacks exploit cognitive biases such as authority bias, scarcity bias, and trust bias. For example, an attacker capitalizes on authority bias by impersonating the CEO in an email sent to an employee, requesting sensitive information. By implementing these cognitive bias theories into the security awareness and training program employees will be able to recognize the cognitive biases cybercriminals use during a social engineering attempt. Sociological theories provide further insight into the social dynamics and cultural factors that influence individuals' susceptibility to

social engineering attacks. Furthermore, understanding concepts like conformity, and group dynamics contribute to the design of the security awareness and training program. Understanding these concepts aids in the design of training modules that influence organizational culture to value security.

The integration of psychological, sociological, and behavioral theories into the security awareness and training program acknowledges the nature of social engineering attacks and their relation to fields of study such as psychology and sociology. By utilizing knowledge in these disciplines, the security awareness and training program can design relevant training, address social dynamics, and facilitate behavioral change. These concepts enhance the effectiveness in preventing and mitigating the social engineering attacks organizations face.

Determining Innovation Effectiveness

To ensure the security awareness and training program's effectiveness, frequent social engineering simulations, incident reporting procedures, and continual awareness campaigns are implemented. These practices are put into place to mitigate several barriers such as noncompliance, time constraints, and the evolving nature of social engineering techniques that pose risks to the program's success. To determine the effectiveness of the security awareness and training program the primary measure of success is in the reduction of social engineering incidents within the organization. Through the information provided by incident reporting procedures, the reduction of social engineering incidents will be able to be measured against the social engineering incidents that occurred prior to the program. Key indicators that will assess the security awareness and training program are data breaches, financial losses, reputational damage, and legal consequences. The effectiveness of the security awareness and training program will also be assessed based on employees' level of awareness and understanding of

social engineering techniques. Regular assessments through social engineering simulations will further assess the security awareness and training program's effectiveness.

Turning the Innovation into Reality 2 pg

As technology continues to evolve, Cybersecurity continues to become more and more essential to today's society. The widespread of information, while it has brought plentiful benefits, it has also introduced our society to concerns over privacy. An Implementation of a comprehensive security awareness and training program can overall benefit the safety of both larger organizations and individuals.

To mitigate the threat of these social engineering attacks, the implementation of a comprehensive security awareness and training program must be bound by several integral components.

Firstly, Employees must be trained on the various social engineering techniques used today like, tailgating, vishing, phishing, and pretexting to name a few. Training must be held in order for employees to properly identify these social engineering attempts. Employees must be ahead of the game in identifying the warning signs of these social engineering attempts. The program should signify the importance of secure communication practices. Whether it is company-specific, or using things such as; sender verification, or encryption usage. The program should also emphasize caution regarding untrusted links, attachments, or outside email addresses. Most importantly highlights good cybersecurity practices which include but are not limited to using strong passwords, changing said passwords frequently, and making sure they are held in a secure place.

In the case of a social engineering attack incident having a plan of action for these situations is also vital. The program must encompass an incident reporting procedure. This will

allow for real-time responses to attacks, and proper reporting to the correct department. Simulations of attacks must also be in place in order to effectively test and perfect the plan of action. In order for this program to work effectively, there must be continuous testing and updates in order to fit the scheme of what is needed. This continuous push for awareness and the need for diligence will inevitably create a safer work environment. Allowing for adaptation and feedback are key aspects of the growth and effectiveness of any system.

As with all things, some barriers must be addressed. A few barriers that may arise when implementing a training program such as this include, Time, resistance, and the pace at which cyber security grows. With Time, programs such as this require the attention of all workers and may be viewed as something that will hinder efficiency. With Resistance, employees may not want to conform to new safety standards, and all levels of an organization must be per the program for it to run successfully. Lastly, the program must stay up to date with the current social engineering tactics, in order to keep the program up to date.

In conclusion, one hundred percent safety across the board is impossible, but with the implementation and success of the Security and Training program safety is at its highest. The success of the program can be seen through the reduction in incidents and employee response. Continuous adaption, monitoring, and Comprehension across all levels of an organization are key to the strengthening of defense against social engineering attacks. Implementing a Program such as this one is not only vital but crucial in today's age.

Summary of Next Steps

Throughout this project, I have gained a lot of knowledge that will aid me in my future endeavors. The most important concept I learned was viewing problems from a multidisciplinary

perspective. Prior to this project, it was difficult for me to view problems from a multidisciplinary perspective. I think that having a multidisciplinary perspective aid in more comprehensive and innovative solutions. Initially, I underestimated the psychological and sociological aspects of cybersecurity. For example, I was unaware of the cognitive biases cybercriminals take advantage of to conduct social engineering. Although I took classes in Psychology and Sociology prior to this project I was unable to draw connections between Psychology, Sociology, and Cybersecurity. Throughout this project, I also learned the importance of an entrepreneurial mindset. An entrepreneurial mindset is important because it embraces innovation and seeks opportunities for growth and success. This same mindset is what cultivated all the innovations that make a positive impact on the world. By having an entrepreneurial mindset I was able to deepen my understanding of social engineering as well as problem-solving. I also learned throughout this process that collaboration can be difficult due to the challenges of coordinating so many different factors. However, I found it beneficial because it enhances problem-solving capabilities. If I were to have done anything differently, I would have focused more on effective and efficient collaboration to form a more comprehensive and innovative solution. Collaboration is essential to tackling complex challenges. Furthermore, this project helped improve the collaboration skills I will use later when collaborating with others.

References

Abawajy, J. (2012, July 5). User preference of cyber security awareness delivery methods. https://www.tandfonline.com/doi/full/10.1080/0144929x.2012.708787

Bettinghaus, E., Fogel, J., Furnell, S., Gosling, S. D., Kruger, H. A., Pan, Y., Parsons, K., Schultz, E., Shropshire, J., Vroom, C., Baranowski, T., Benet-Martínez, V., Cellar, D. F., Costa, P. T., Donaldson, S. I., Figner, B., & Heinström, J. (2016, December 1). *Individual differences and information security awareness*. Computers in Human Behavior. https://www.sciencedirect.com/science/article/abs/pii/S0747563216308147

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016, May 28). *Breaching the human firewall: Social Engineering in phishing and spear-phishing emails*. arXiv.org. https://arxiv.org/abs/1606.00887

Ghafir, I., Prenosil, V., Alhejailan, A., & Hammoudeh, M. (2016, September 26). *Social Engineering Attack Strategies and Defence Approaches | IEEE ...* IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/7575856/

IEEE. (2019, January 17). Educating and raising awareness on cyber security social ... - IEEE xplore. https://ieeexplore.ieee.org/abstract/document/8615162

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011, July 1). *Social Engineering: The neglected human factor for information security management*. Information Resources Management Journal (IRMJ). https://www.igi-global.com/article/social-engineering-neglected-human-factor/55064

Salahdine, F., & Kaabouch, N. (2019, April 2). *Social Engineering Attacks: A survey*. MDPI. https://www.mdpi.com/1999-5903/11/4/89