Comparison of Social Engineering Cybersecurity Attack Prevention Strategies

Effects of Company Culture on Cybersecurity

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Emily Huo

Spring 2022

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Kent Wayland, Department of Engineering and Society

Daniel Graham, Department of Computer Science

General Research Problem

How can companies effectively protect against social engineering attacks?

Recently, there has been a 125% increase in volume of cyberattacks year-over-year (Schiappa, 2021). Money spent by companies to recover have also increased. In 2019, the average cost a company spent to recover from a cyber-attack was $761,000. In 2020, the average cost had more than doubled to $1.85 million (PurpleSec, 2021). In addition to the monetary consequences, cyberattacks create noticeable denial effects in the physical space. These can be catastrophic, ranging anywhere from the disruption of electrical grids to the destabilization of entire nation-states. In a recent incident, Colonial Pipeline was hit with a ransomware attack on May 7, 2021, causing a shutdown of its entire 5,500 mile gasoline pipeline system. Colonial Pipeline is critical infrastructure as one of the nation's largest pipeline responsible for 45% of the East Coast's fuel supplies. A state of emergency was declared and in the end, Colonial ended up making a payment of $4.4 million to stop the leak of nearly 100 gigabytes of stolen data. The effects of the 6 day halt were serious and caused a shortage of gas at gas stations and increased fuel prices (Turton, 2021).

The increased number of cyberattacks is correlated with an uptick in social engineering attacks, or attacks that rely on psychology through manipulation and deception. These attacks exploit humans, who are the weakest link in cybersecurity. In the case of companies, this problem lies within employees. This is because humans are error prone and might make the same mistake multiple times. It can be much easier and cheaper for a hacker to send a phishing email in order to elicit the necessary information to get into a system than it is to bypass security measures such as firewalls. Therefore, how can companies effectively protect against social engineering and cybersecurity attacks in general? An investigation into the effectiveness of

different social engineering attack prevention strategies and what aspects of company culture foster this effectiveness will be conducted to address this question.

Comparison of Social Engineering Cybersecurity Attack Prevention Strategies

How can different defense strategies be combined together to create a cybersecurity defense campaign that will prevent social engineering attacks?

With a rise in social engineering attacks, investigation into different strategies to prevent social engineering cybersecurity attacks have also started. Recently, research has been conducted to define security requirements for the "proper and secure use of the Information Technology services in organizations" with the focus on mitigation of social engineering attacks. This resulted in a model of Social Engineering InfoSec Policies being created for public and private organizations to implement in order to protect its confidentiality, integrity, and availability, or CIA (Alharthi, 2021). However, this is just a start and there are still many questions left to be answered.

There is a total of 18 formal Social Engineering InfoSec Policies each defending against a different social engineering cybersecurity target point. Ideally, a company would have all 18 policies implemented. The policies outline requirements that would help combat the target point if translated into technical processes within the organizations' systems (Alharthi, 2021). However, it has been found that companies only incorporate around half of these. Companies do not have an unlimited amount of money to spend on cybersecurity defense and effectiveness of each policy varies. Therefore, it is imperative to make smart investments into defense tactics since companies might not be able to implement all of them. How effective each policy is and what combination of policies work best to achieve a certain cybersecurity defense goal should be investigated. To do this, a set list of social engineering cybersecurity attacks will be determined

based on how dangerous it is and its frequency of occurrence. Then, each proposed policy will be investigated and analyzed to determine its effectiveness against this list of attacks. This will be accomplished through simulations with employees such as a simulated phishing email to model a real social engineering cybersecurity attack. Since social engineering is human centered, this will be repeated multiple times with employees of varying levels of awareness. Since each policy aims to defend against a different social engineering target point, each policy has a different goal. The strengths and weakness of each strategy will be identified and how well it achieves its goals will be measured. The different policies will be compared and contrasted, and finally, different combinations of policies will be tested out together to determine which defense strategies can effectively work together.

Ultimately, these sets of simulations and experiments will provide companies with a better idea of what policies and strategies best fit their goals, helping them prioritize what they should incorporated with their limited funds when implementing a cybersecurity defense campaign. It can also help companies combine several different strategies to formulate a multi-level defense plan to increase their protection.

Effects of Company Culture on Cybersecurity

What aspects of company culture foster effective cybersecurity?

Cybersecurity is a big concern for companies and a successful cyberattack can lead to catastrophic consequences. Thus, in order to have the most effective defense, companies can not solely focus on the technical aspect of cybersecurity. Companies must look beyond and get to the root of the problem, the people.

Current investigations into cybersecurity strategies do not place enough emphasis on company culture and the effect it has on the psychology of employees. Employees are the main

actors in a defense campaign against social engineering attacks on companies, so company culture will heavily impact the effectiveness of any defense put into place. Company culture is a shared ethos of an organization. It describes the attitudes and behaviors that executives clearly and consistently communicate and expect from all members of the company. If the culture does not create an environment of psychological safety for employees, weak points will be created and make a company more vulnerable to social engineering attacks. By better understanding the influences of company culture, a company can gain a more thorough comprehension of the impact employees has on cybersecurity. Companies can then use this to design a more complete approach to cybersecurity and increase the effectiveness of their defense against attackers.

Background and Theoretical Framework

It has been found that company culture "must emphasize and value cybersecurity" and that cybersecurity should be a part of "corporate strategy and culture" (Chatterjee, 2021; Touhill, 2014). This is supported by the EY Global Information Security Survey 2018-2019 which revealed that the biggest vulnerability was deemed to be "careless/unaware employees" at 34% (McIlwraith, 2021). Company culture starts at the top and trickles down, so executives are a key actor and play a big role in fostering effective cybersecurity. They are the ones that initiate change and have control over what gets funded. Regular employees with no technology background are another key actor. These are the people who are most likely to fall for social engineering attacks and thus are the most vulnerable and targeted.

A company that does not emphasize the importance of cybersecurity will not train employees to prioritize cybersecurity, so I will be studying the role executives play in changing aspects of company culture to foster a strong security culture. Corporate culture encompasses a multitude of things, but I will be focusing on employee psychological safety. Without a culture

that fosters employee psychological safety, employees will not prevent and stop the propagation of a social engineering cybersecurity attack. Thus, I will investigate how company culture can foster employee psychological safety in order to increase a company's resistance against social engineering cybersecurity attacks.

Evidence Collection and Methods

Company cultural factors such as "subjective norms, organizational values, and expectations" have been cited to have significant impact on positive compliance behaviors regarding cybersecurity (Chatterjee, 2021). Through analysis of evidence from different sources, I hope to understand what aspects of company culture contributes to a strong defense against social engineering and cybersecurity attacks. I will use the evidence gathered from the literature review to discover what company cultural factors instill a sense of psychological safety in employees. Then, I will analyze how that sense of psychological safety impacts employee beliefs and actions which will directly impact how a company is able to protect themselves and respond to a social engineering attack. By first narrowing down which aspects of company culture are the most important in cultivating a sense of psychological safety in the workforce, I can investigate how those influences attitudes and behaviors in employees. Finally, I can explore how those changes in attitude and behavior either positively or negatively affect cybersecurity defense strategies against social engineering attacks.

Positive compliance behaviors are a result of employee's psychological safety, which is imperative in order to have a successful long-term defense campaign. For example, if a company makes it a disciplinary offence when an employee falls victim to a simulated phishing attack, this may make employees "feel caught out" (Ashenden, 2021). This impacts the employee's psychological safety because "nobody likes to get things wrong" and the employee may feel that

they have been “tricked” in this situation and will be “much less likely to be motivated to try and improve security” (Ashenden, 2021). To further understand how companies can create a culture of psychological safety in order to establish a strong cybersecurity defense, relevant sources of literature on employee psychological safety will be examined for evidence.

After literature review has been conducted, I will have identified the main aspects of company culture that contribute to employee’s psychological safety. I will then aim to understand the link between psychological safety in the workforce and how those can positively or negatively influence employee attitudes and behaviors. These attitudes and behaviors will in turn impact the effectiveness of an organization’s defense against social engineering attacks. Company executives can then use this to successfully implement these aspects of company culture to make a change in employee’s psychological safety to foster effective cybersecurity. This will help increase the effectiveness of their defense against cybersecurity attacks by learning more about the root of the situation, humans, and help them implement a more holistic approach to cybersecurity.

Conclusion

As technologies evolve and the field of cybersecurity changes along with it, one thing that attackers can rely on is that humans make mistakes. Because of this, the strategy of social engineering and social engineering attacks will never go away. Companies need to learn how to effectively protect themselves against these attacks. By having a better understanding of what different social engineering attack prevention strategies target and how effective they are, companies can use this to combine strategies together and make the best defense that fits their goals. Coupling that with a change in company culture to emphasize employee psychological

safety, companies will be able to establish a strong security culture and more effectively defend themselves against cyberattacks. Not only will this save companies money and the trouble of recovering from a breach, but they will also have a strong reputation for caring about their customer’s data and privacy.

References

2021 CyberSecurity Statistics Trends & Data. PurpleSec. (2021). Retrieved from *https://purplesec.us/resources/cyber-security-statistics/*

Alharthi, D., & Regan, A. (2021, April 29). "A literature survey and analysis on social engineering defense mechanisms and infosec policies." *International Journal of Network Security & Its Applications (Vol. 13, no. 2).* 10.5121/csit.2021.110104.

Ashenden, Debi. (2021). "The future human and behavioural challenges of cybersecurity." *The Oxford Handbook of Cyber Security*, 722–734. https://doi.org/10.1093/oxfordhb/9780198800682.013.48

Chatterjee, Dave. (2021). *Cybersecurity Readiness: A Holistic and High-Performance Information Security Culture Framework*. Thousand Oaks, CA: SAGE Publications, Inc., https://dx.doi.org/10.4135/9781071837313

McIlwraith, Angus. (2021). *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness (2nd ed.)*. New York, NY: Routledge. https://doi-org.proxy01.its.virginia.edu/10.4324/9780429281785

Schiappa, D. (2021, July 14). With Ransomware Costs On The Rise, Organizations Must Be More Proactive. *Forbes*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2021/07/13/with-ransomware-costs-on-the-rise-organizations-must-be-more-proactive/?sh=60145e142dd5

Touhill, G. J., & Touhill, C. J. (2014). *Cybersecurity for executives: A practical guide*. Hoboken, NJ: Wiley.

Turton, W., & Mehrotra, K. (2021, June 4). Hackers Breached Colonial Pipeline Using Compromised Password. *Bloomberg.com*. Retrieved April 1, 2022, from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password