Alex Bradshaw

CSCI 2290

Dr. Joshua Montgomery

February 28, 2024

The organizational responsibilities and knowledge needed to respond to a cyber incident is vast and extensive. Organizations fill roles based on experiences, training, or college education. This fills technical and non-technical jobs with capable individuals. While doing this seems like the correct thing to do it can leave gaps in an organizational cyber security defense plan. This is due to non-technical employees are likely to not have technical skills at the level of an Information Technology or Information Security employee that is well acquainted with best practices for a secure and safe network. Phishing attacks are at the forefront of this knowledge gap. To showcase the importance of cybersecurity best practices and procedures a mindset and culture of cybersecurity is paramount. Training and filling the knowledge hole is a great way to close the gap between technical and non-technical training. Closing the gap of technical skills and knowledge between technical employees and non-technical employees is essential for an organization to have a greater defense against cyber security incidents.

Phishing emails are one of the greatest threats to an organization that all employees will encounter including technical and non-technical employees (Internet Crime Compliant Center, 2022). Phishing emails use skills and techniques known as social engineering. Attackers use these techniques to gain the trust of their victims, also known as an organization’s employees. After the attackers gain the trust of their victim, they either gain information from the victim or have their victim unknowingly give the attacker access to a resource on the network or system that the victim is currently utilizing for their email services.

Phishing attacks are widely used and are commonly used alongside other malicious actions. (National Institute of Standards and Technology, 2023). The results of phishing as well as Remote Desktop Protocol (RDP) exploitation, and exploitation of software vulnerabilities are the leading reasons for exploiting the use of ransomware which is one of the most crippling cyber-attack vectors in the United States. These attacks coincide with the data presented by the IC3 for the internet crime statistics for 2022. (Figure 1)

Phishing attacks go after all employees at a company not just those trained in cybersecurity (MS-ISAC Multi-State Sharing & Analysis Center, 2023). Phishing attacks can be used in a multitude of ways including obtaining login credentials. This is done by someone impersonating someone you would trust such as people you work with, staff at your company or even government organizations. While impersonating they use the trust gained by their impersonation to obtain the login credentials. After the credentials (e.g., usernames and passwords) have been harvested they can be used fraudulently to gain unauthorized access to resources or information. There are ways for technical employees to assist in protecting non-technical employees using administrative privileges (National Institute of Standards and Technology, 2023). There are a few ways that technical employees can protect non-technical employees by having software to reduce the amount of phishing emails that the non-technical employees will see. Maintaining and having anti-virus software can reduce the risk if a malicious attachment or link is clicked on. Utilizing email filters so emails cannot be seen by the non-technical employees so places that are know to send high volumes of suspicious emails can be blocked. Utilizing and configuring email security can make sure only legitimate emails make it through by checking the authentication of emails. Enabling and configuring anti-phishing techniques and technologies can reduce the amount of phishing emails seen by non-technical employees by using threat intelligence to block common emails used for phishing or unauthorized contact with members of an organization. Technical employees can implement multi-factor authentication. While this seems to cause a headache for non-technical users this allows non-technical employees from be manipulated or tricked into become ground zero from a cyber threat or attack.

Building a culture of cybersecurity and awareness mindset is a critical component of any organization's defense plan against cyber security incidents (National Institute of Standards and Technology, 2018). Adopting this mindset will help develop a culture of security which will positively affect those who question whether something is safe and secure before continuing to say click on a link. This culture building will also encourage non-technical employees to gain technical skills. The more employees that have technical skills in areas of information security the better off the company will be when it comes to their security posture against potential cyber security incidents and attackers.

To build culture the company must first build and foster a cybersecurity mindset (National Institute of Standards and Technology, 2024). When building a culture of cybersecurity and awareness mindset is a critical component of building that culture. Building this culture allows the company to increase their ability to address cyber risks that will happen eventually. All companies are at risk. From mom-and-pop stores to the fortune 100 companies. Cybercrime is prevalent in the times that we live in and companies along with individuals need to stay alert and prepared for these incidents. The cybersecurity and awareness mindset will make individuals aware of appropriate behaviors that will contribute to a resilient workforce that will allow a strong culture to prevail that every organization needs.

After a culture is built and fostered it must continue to grow with the organization (National Institute of Standards and Technology, 2018). After a culture of cybersecurity and awareness mindset is implemented employee training is required. Employee training builds an understanding of risks and provides specific steps for mitigating them. Employee training comes in many forms including computer-based classes and practical exercises and even team exercises. The use of social engineering is prevalent and is used to spread exploits to unknowing and unsuspecting employees at an ever-increasing risk. The exploits will attempt to gain information from the unknowing and unsuspecting employee for their resources or to move within a system and gain resources from another employee. A main point in training is to increase knowledge and harden employees against these types of attacks and socially engineered exploits. Unfortunately, training will never harden employees to 100%. Although through these training employees can be hardened and mitigate how frequently and the amount these types of socially engineered exploits can be used against an organization. It is important to always put the culture of cybersecurity and awareness mindset out into the open. This can include internal awareness campaigns such as flyers or newsletters or even contests with prizes for the winners. Generating buzz around important security themes will help build a culture of cybersecurity and awareness mindset.

Closing the gap between non-technical and technical employees will be beneficial to a healthy cyber awareness company culture (National Institute of Standards and Technology, 2024). One of the first steps in closing the gap between technical and non-technical employees is communicating what non-technical employees need to know. This can be done efficiently through a newsletter or general sessions. Another way to close the gap is through training. Training should be conducted by those who are subject matter experts in the areas that the trainees or non-technical employees need to know. Training should be at the forefront of learning due to the knowledge gap between technical and non-technical employees.

To start the shift in culture the organization should implement a non-technical newsletter or blog for the whole company to begin to understand the fundamentals of cybersecurity

(National Institute of Standards and Technology, 2024). Translating technical jargon that is everyday vocabulary for technical employees such as Information technology and information security can be difficult. When communicating technical language to others the technical employee should try to use everyday vocabulary to communicate with the non-technical employees. If only technical terminology is used it may cause the dismissal or misunderstanding of the information the technical employee is trying to disseminate. This will make the information understandable and relevant to their intended audiences.

The best way to close the cyber awareness gap between non-technical and technical employees will be training (Cybersecurity and Infrastructure Security Agency, 2019). All employees, both technical and non-technical, are needed to keep up on basic cybersecurity training to be a strong defense against cyber threats. Basic cybersecurity training should include cybersecurity concepts, terminology, and activities. These trainings should be associated with real world scenarios to implement best practices against these real-world threats.

Through training your non-technical employees will become the first line of defense against cyber threats, primarily phishing. (Cybersecurity and Infrastructure Security Agency, 2019). Technical and non-technical employees are the first line of defense when it comes to defending from cyber-attacks. They are the most crucial part of any defense in depth techniques and policies that an organization can put forward. The skills needed to help defend the organization comes from knowledge. The best way to gain this knowledge is through practice and a culture with a culture of cybersecurity and awareness mindset.

Cybersecurity training must continue on an ongoing basis (Cybersecurity and Infrastructure Security Agency, 2019). Continuation of training will help reinforce what has already been learned and will introduce new knowledge and skills. The ongoing training will keep employees up to date on knowledge and updated skills. The training should be continued on an ongoing basis to reinforce skills and knowledge previously learned.

Maintained awareness is a great way to implement cybersecurity awareness and training (Cybersecurity and Infrastructure Security Agency, 2019). An organization must always have a watchful eye on trends happening in the organization, the business sector, the country, and the world. The company will be able to keep current through practical exercises and information to pass on to their organizations employees so they can have the best chance at stopping cyber-attacks before they start. The longer it takes to reinforce something the sooner they will forget the information (Lee, 2004). Memory lessens over time and the longer you wait to relearn the lower the retention will be. This is why maintaining awareness is a great way to implement cybersecurity awareness and training due to the constant reminder of the importance.

Training should be held every two to four weeks due to the forgetting curve (Murre et al., 2015). After 31 days memory retention was at its lowest of testing at 20 minutes, 1 hour, 9 hours, 1 day, 2 days, 6 days, and 31 days after the initial data was learned. (Figure 2) This may be because the time it took to initially learn what was needed for the testing did not take a long period of time due to the eagerness to learn the information. It also matters what time the training takes place (Finkenbinder, 1913). Retention of memory is best utilized in the morning around eight o'clock in the morning. The later in the day the less retention is observed with the lowest being five o'clock in the afternoon.

The training should be specific to the industry the training is being applied for (Anamova et al., 2020). Professional retraining programs designed for the best outcomes come from customers' requirements. After these requirements are set the advanced training programs become available for the employee to then participate in their retraining. The advanced training programs are all stored on a database that all employees can access for training. Professional training programs are created for the professional standards created by qualification manuals set by human resource services; this leads to standards set for employees from customers for specific requirements.

The organizational responsibilities and knowledge needed to respond to a cyber incident is vast and extensive. Organizations fill technical and non-technical jobs with capable individuals. While doing this seems like the correct thing to do it can leave gaps in an organizational cyber security defense plan. This is due to non-technical employees are likely to not be well acquainted with best practice for a secure and safe network. Phishing attacks are at the forefront of this knowledge gap. To showcase the importance of cybersecurity best practices and procedures a mindset and culture of cybersecurity is paramount. Training and filling the knowledge hole is a great way to close the gap between technical and non-technical training. Closing the gap of technical skills and knowledge between technical employees and non-technical employees is essential for an organization to have a greater defense against cyber security incidents.

Resources

Anamova, R. R., Bykov, L. V., & Kozorez, D. A. (2020). Algorithm for Designing Professional Retraining Programs Based on a Competency Approach. *Education Sciences*, *10*(8), 191. https://doi.org/10.3390/educsci10080191

Cybersecurity and Infrastructure Security Agency. (2019). *Cyber essentials. Your success depends on Cyber Readiness, Both depend on YOU.* Retrieved from https://www.cisa.gov/sites/default/files/publications/19_1105_cisa_CISA-Cyber-Essentials.pdf

Finkenbinder, E. O. (1913). The Curve of Forgetting. *The American Journal of Psychology*, *24*(1), 8–32. https://doi.org/10.2307/1413271

Internet Crime Compliant Center. (2022). Federal Bureau of Investigation. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Lee, M. (2004). A Bayesian analysis of retention functions. *Journal of Mathematical Psychology*, *48*(5), 310–321. https://doi.org/10.1016/j.jmp.2004.06.002

Murre, J. M. J., & Dros, J. (2015). Replication and Analysis of Ebbinghaus' Forgetting Curve. *PLoS ONE*, 10(7), 1–23. https://doi.org/10.1371/journal.pone.0120644

MS-ISAC Multi-State Sharing & Analysis Center. (2023). *Phishing guidance: Stopping the attack cycle at phase one.* Retrieved from https://www.cisa.gov/sites/default/files/2023-10/Phishing%20Guidance%20-%20Stopping%20the%20Attack%20Cycle%20at%20Phase%20One_508c.pdf

National Institute of Standards and Technology. (2018). *Cybersecurity is Everyone's Job A Publication of the National Initiative for Cybersecurity Education Working Group Subgroup on Workforce Management at the National Institute of Standards and Technology*. Retrieved from https://www.nist.gov/system/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf

National Institute of Standards and Technology. (2023). *Phishing.* Retrieved from https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing

National Institute of Standards and Technology. (2024). *Users are not stupid: Six Cybersecurity Pitfalls Overturned.* Retrieved from https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=936113

Appendix

TOP FIVE CRIME TYPE COMPARISON[4]

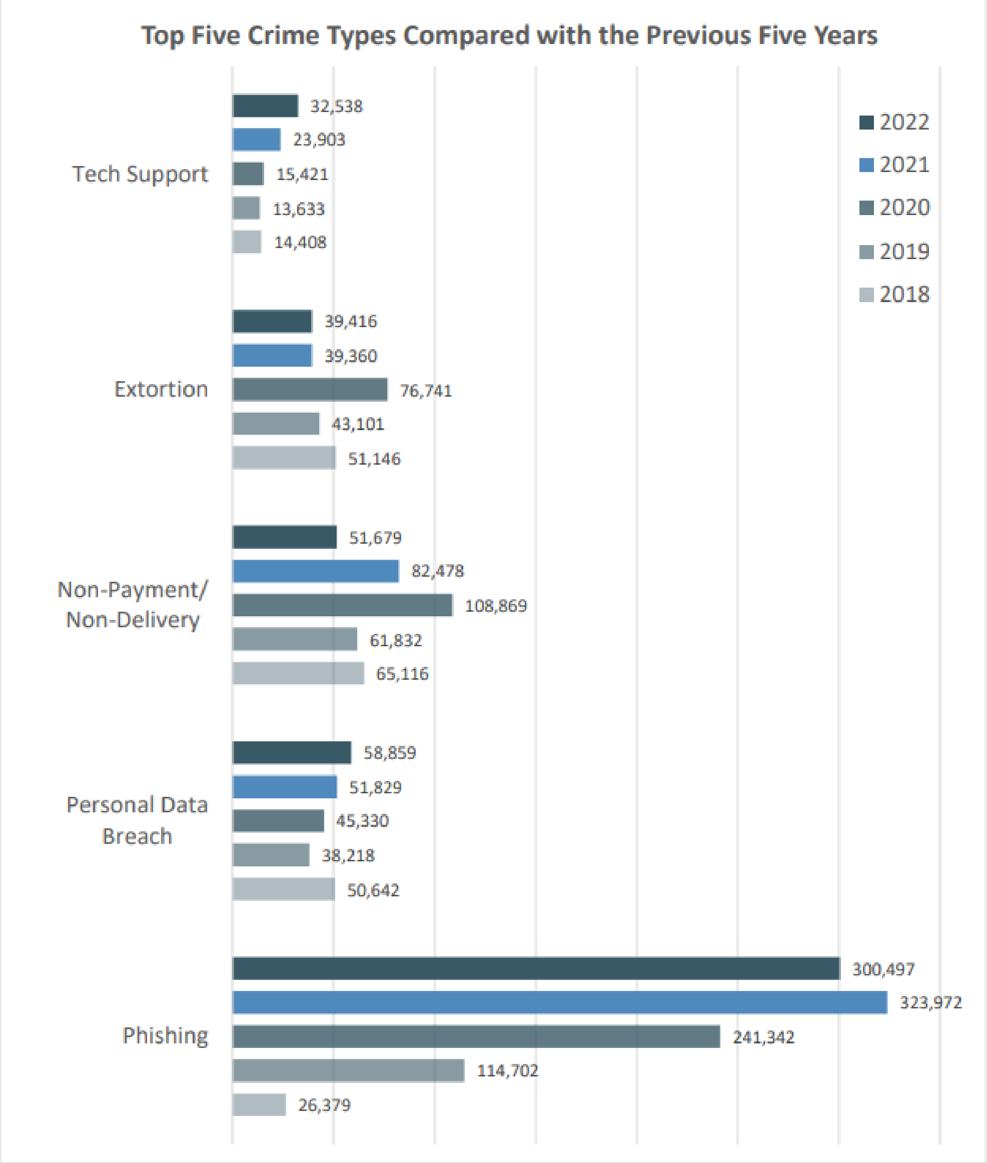

Figure 1

[4] Accessibility description: Chart includes a victim loss comparison for the top five reported crime types for the years of 2018 to 2022.

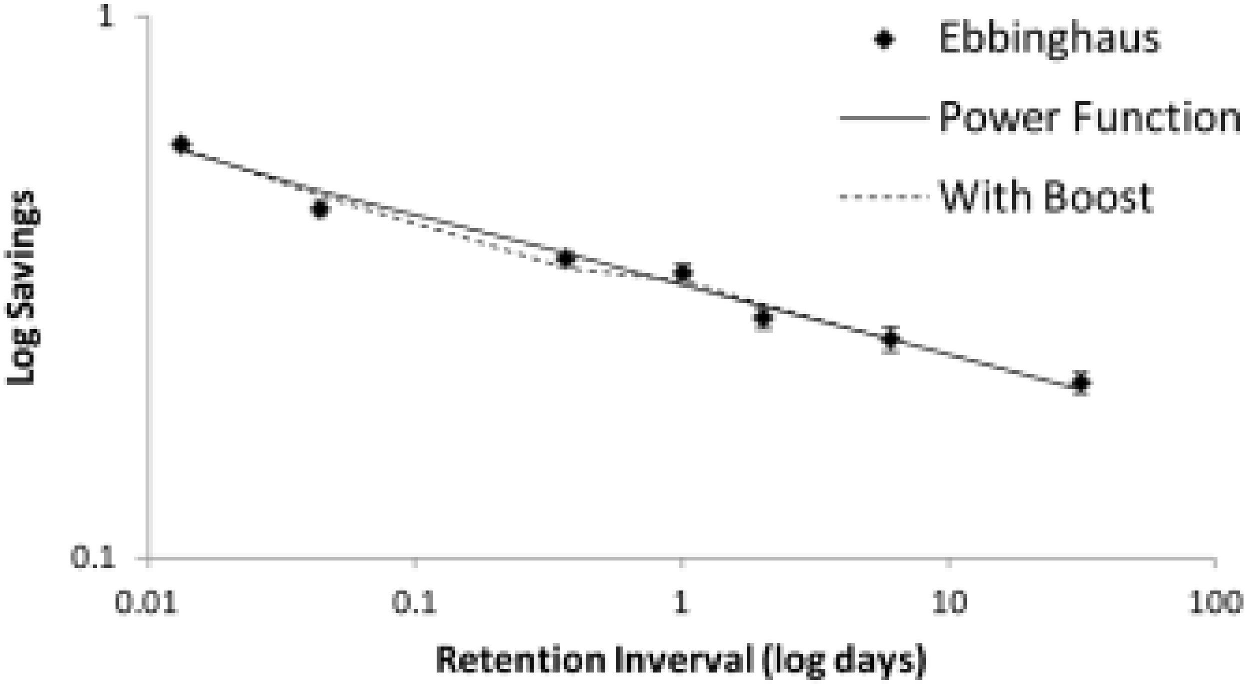
1
0.1
Log Savings
0.01
0.1
1
10
100
Retention Inverval (log days)
Ebbinghaus
Power Function
With Boost

Figure 2