The Importance of Information Security Awareness Training Programs

Final Thesis

Khalid Aldrouby

Course Code: Spri2022-S10-CAPS795.30782

Lonnie Decker

□□□□□□□□□

Like many other aspects of information security specially now more than ever while the entirety of the information security community struggles in this phase that is usually referred to as the active cyber warfare era, there are many options readily available for companies to implement that will help shore up and defend their systems, employees, and intellectual properties. The recent shift in attacks is directly related to the rapid expansion of internet and

counterintelligence operations among his annual list of global threats to U.S. interests and the

[illegible]

Starting this chapter of literature review first by describing this thesis statement that is "Organizations that implement specific practices to reduce their risk to insider threats will reduce their annual reported security incidents". The differences between organizations that implement security awareness programs and those that don't implement such programs can be significant to the overall protection of accounts and services. The discussion revolves around the effectiveness of technical controls versus targeting the workforce to make them aware and better at handling situations that can become security incidents if and when mishandled by a resource (Human factor) on the inside, whether it's dredr4o3369.15789(k)-0.956417.843 0 Td [(p)-0.95479431(t)-2

mailbox for them to click and cause a security incident that may or may not be contained in time before harm is done.

In today's world, security incidents became a very common occurrence. Most of these events targets the human factor as indicated by a recent research showing email (phishing attacks) is the leading cyber-attack type that organizations must deal with according to IBM X-Force's 2021 threat intelligence index report (**X-Force, 2021**) "Phishing emerged as the top infection vector in 2021, surpassing vulnerability exploitation, which took the lead in 2020. Phishing was observed in 41% of the incidents X-Force remediated. While vulnerability exploitation dominated in Q3 of 2021, the significant number of phishing-related incidents X-Force observed in Q1 and Q4 pushed this infection vector into the lead for the year".
This is yet another example on how attacks are primarily targeting organizations, and how it is focusing on their workforce instead of focusing only on systems and vulnerabilities that might be available as an additional attack surface used to supplement the attack cycle whether by elevating their access or establishing persistence.

Unfortunately, most organizations today overlook the importance of security awareness programs and tend to focus on the technical aspect of protection for example take deploying email security filtering solution that can improve overall protection against phishing attempts. This can only provide what the author refers to as perimeter protection for known threats well-defined outside what commonly referred to as zero day that considers the high volume of messages and the continuous evolution in attack tactics and techniques. This is one of the primary reasons why phishing and end user targeted attacks continue to lead the charts of cyber security threats organization must deal with and take seriously.

In this literature review we would uncover and go over some of the details involved in how to differentiate and compare between individuals that are educated on the topic of cyber security threats also aware on how to follow best practices compared to individuals that unaware of the consequences and various techniques used in various attacks such as phishing, smishing, phone scams and the extended list of attacks they would encounter. All of that while collecting answers and feedback from top cyber security experts as it would be explained later in the research method and result section of this paper, finally walking through the process and plan to deploy interaction analysis interviewing two cyber security experts with advanced knowledge within information technology in general and information security to be more specific. This would ensure establishing grounds around the case of how important security awareness programs can be for an organization not only based on the author experience and the research done part of this paper but also based on opinions and previous studies referenced including feedback collected from real life examples talking to top security experts that operate in this field.

This paper does consider with open mind that the argument is valid, that in few cases security awareness programs can be an overhead to strict budgets and that they may not prove to be effective in dealing with all cyber threats. Important point is in most of these cases the true reason behind such failures is typically an incorrect roll out or limited rollout that impacts the

be priceless in increasing and providing effective defense when all else fails which based on data reviewed so far is guaranteed to occur and when it does, organizations and personal must be ready to act and defend against such occurrences.

Next, to break down various tactics and how it can unfold social engineering can come in various shapes and forms, one type is known as phishing attack that accounted for 80% of all security incidents in 2020 per (**CSO Online, 2020**). They are typically launched through email, text, social and voice (phone calls). The annual cost for digital based scams that includes ransomware attacks averages at around $4.1 billion. The impact is serious and real. Just take one example for the massive data breach in the state of South Carolina which started with a targeted social engineering attack known as spear phishing email that was sent to employees and ended

referred to as (PII) and trade secrets. Keep in mind that their goal in most cases is motivated by financial gain, however attacks can also be motivated by malicious or political reasons.

Effectiveness in attacks can vary, impersonation is probably one of the most effective and common social engineering tactics. Cybercriminals will attempt to impersonate people in many situations for example a person that is in need, so

prior to mounting an attack so they can seem as completely legitimate to the victim and in most cases it works. Best defense against such attempts is to always limit what we divulge regardless of how legitimate someone seems on the other side, avoid the temptation to do something against an organization policy or against best judgment and common sense and that can be improved while responding and interacting with such threats by security awareness trainings since technical defense mechanisms are susceptible and unfit to protect against such threats that focuses on the human factor. the complexity is on the rise as it was mentioned previously in the introduction section of this paper and diversion is usually coupled with deception and that is when one cybercriminal distracts the target while another cybercriminal executes an attack. This is more common in physical attacks for example on the street when someone bumps into the victim and pretend to drop their stuff on the ground, while the victim genuinely helps that person a third person steps in and steals a badge, wallet, or phone of the victim. Another scenario is building access where one person walking into the building badges in and get distracted by someone yelling for help for another social engineer to sneak into the building unnoticed. In these situations, educating employees on how to always be aware of their surroundings and what is happening especially if something unexpected happens to prevent distractions from controlling the situation and stop such attacks in its tracks.

Finally, obligation type of social engineering is on the rise, and it is when cybercriminals target employees whose jobs are typically designed to help others for example customer support representative, service desk staff, marketing and publicity contacts and administrative assistants. Since their roles requires answering questions by nature and providing support to other people in these positions are more susceptible to social engineering attacks carried on by cybercriminals. These are usually targeted with coupled tex es.cialcks 5194(s)-1.7465(25956417( )-465(t)-2.536431(e)3.1578

them to give up information that can be used at a later stage. To defend against such tactics an employee that can recognize that the person on the other side could be a cybercriminal and not let them coerce or tempt them into providing information that may help them gain unauthorized access is important. Also learning how to handle pressure and seek help of others in such scenarios is important and crucial. That is one area where security awareness training is so important in allowing organizations to stand by their employees letting them know that they are not alone and there are ways to get help when needed.

overall information security program. Also providing real life examples to help better understand the direct impact it has or has not for one's organization overall security posture.

This conversation begins with a simple and clear explanation for the reason behind this discussion. It states the reason clearly which is the fact that we are trying to better understand this topic by asking questions to better understand and evaluate the importance of information security awareness training programs, also the need to keep in mind that there's truly no right or wrong answers. Stating that based on their extensive experience in information technology is why as an author interested in their take and feedback based on this conversation.

Few questions were truly asked to validate and make it clear to the research community that as an author both experts are being introduced properly. Even though knowing both experts

next one is fascinating. The attack started mid-morning on July 15th, 2020, when a threat actor was trying to phish employee credentials by calling up the consumer service and technical

just so they don’t have to interrupt their activities. That seems to have been the case for many organizations considering that their employees’ thought was a good idea to disable security updates.

This feedback obtained from the first security expert demonstrates a solid proof that there are challenges in getting approvals and resources to deploy such programs at an organization especially at large scale for global enterprises. Next part of this conversation dives into an area that if they had to convince others on the importance of security awareness programs, what approach would they take in an open and honest argument. The answer was the fact that there is data to support the argument of importance on security awareness programs. The data shows that employees are the weakest link to security, indicating that majority of cybersecurity breaches involve human interactions. They were able to recall correctly in 2021 alone 85% of all the

customers is far less. We don't know the exact numbers. We are still conducting the investigation." On Thursday, the current administration announced a roster of tough sanctions against Russia as part of what it characterized as the "seen and unseen" response to the SolarWinds breach.

NPR's months-long examination of that landmark attack — based on interviews with dozens of players from company officials to victims to cyber forensics experts who investigated, and intelligence officials who are in the process of calibrating the Biden administration's response — reveals a hack unlike any other, launched by a sophisticated adversary who took aim at a soft underbelly of digital life: the routine software update.

[illegible]

Adding final conclusions and concreate findings that this research paper aims at, the consequences for organizations can be devastating for an insider that is unable to understand how threats that may come through a simple mail offering them free gym membership for a year, or a phone call from a person pretending to be calling to renew their vehicle warranty, or a text message with a link to click accepting a 25$ gift card from the local brewery. As simple as the previous examples can be, the reality remains the same that people tend to drop their guard while interacting with such threats in the digital world. Also, the fact that people are easily distracted and trying to go on with their day when they receive such threats which can be a something they can interact with not fully understanding the consequences, considering the number of nontechnical employees each company have on average and how it out numbers the staff of technical folks the chances for a person to fall for such attempts is relatively high. Take that and add the complexity some of these attacks are deploying and the fact that organizations may not have a solid security control in place becomes the perfect hunting ground for adversaries (Threat actors).

In this conclusion, having a solid security awareness training program is not the endgame. It is not the perfect solution that will eliminate all threats and stop them from progressing. That is not the point of this paper the author trying to convey, point is the fact that security is like a warrior armor. Having proper head gear, shoulder protection, chest armor, gloves and many other items make it possible to defend against attacks. Similarly, the case in cyber security, having permitter defense, defense in-depth and technical safeguards is crucial. Having a security awareness training program is key in ensuring that the full “body” of an organization is capable and aware when and how to defend itself in the face of threats that can and will bypass various layers implemented at a network, host, application protection layers. A

user with the ability to detect a phishing email, t

□□□□□□□□□□

IBM Security X-Force. (2021). X-Force Threat Intelligence Index 2021.
https://securityintelligence.com/posts/phishing-attacks-top-cyber-threat-create-deploy/

Rotvold, Glenda (2008). How to create a security culture in your organization
https://www.nsi.org/pdf/awarness-articles/Create%20a%20Security%20Culture.pdf

Redspin (2009). 94% of Companies Fail Email Test
https://www.darkreading.com/vulnerabilities-threats/redspin-94-of-companies-fail-email-test

Moti Zwilling (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study
https://www.tandfonline.com/doi/abs/10.1080/08874417.2020.1712269?journalCode=ucis20

Miko T. Siponen (2000). A conceptual foundation for organizational information security awareness
https://www.researchgate.net/profile/Mikko-Siponen/publication

Crowdstrike (2022). Global Threat Report
https://www.crowdstrike.com/global-threat-report/

Ryan Olson (2022). Average Ransom Payment up 71% this year, approaches $1 Million
https://www.paloaltonetworks.com/blog/2022/06/average-ransomware-payment-update.

SailPoint (2016), Stopping the insider threat
https://docs.sailpoint.com/wp-content/uploads/SailPoint-TheChertoffGroup-Stopping-The-Insider-Threat-White-Paper..

Dina Temple-Raston (2021). A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack
https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

Universite du Luxembourg (2016). Social Engineering: Password in exchange for chocolate.
https://www.sciencedaily.com/releases/2016/05/160512085123.htm