The Importance of Information Security Awareness Training Programs

Final Thesis

Khalid Aldrouby

Course Code: Spri2022-S10-CAPS795.30782

Lonnie Decker

Table of Contents

Abstract

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 digital currency. From far away this may seem complex and highly technical which can be true to a certain degree, what companies tend to ignore is a simple factor and that is the human factor. If we rewind the time machine and look at crimes committed in the past that is in general not just cybercrime, we can see that whenever there is a trend of a new scam scheme or some sort of organized crime, we find a common factor and that is the human factor. For example, at a bank robbery, the criminal might be able bypass bank security while armed to get inside the bank, or in other cases force an employee to let them in either by deception or brute force. In another example it could be following someone at the door without having to swipe a badge gaining access to a building, these are just a few to name but they can be directly related to a criminal exploiting another person action to gain access and elevate their chances to carry on their crime. This paper is designed to uncover the benefits, risks and procedures that focuses on this human factor. Simply, how can an employee with limited access accidently or willingly cause catastrophic damage to a company without knowing their action can have such impact, then looking at how can that employee become enabled and empowered to be wary of such attempts and capable to respond effectively. Finally, how companies are enabling their employees to be able to defend against such cyber-crimes that targets the human factor.

Introduction

Starting this section with an introduction for the main point to be covered in this research that is "**Organizations that implement specific practices to reduce their risk to insider threat will reduce their annual reported security incidents**", this is the problem statement selected as a foundation for this research paper.

An end user on the inside that is unable to properly follow security procedures and continues to engage in bad security practices within an organization can have devastating impact on the enterprise. This is considered a threat and security risk that comes from within the targeted organization. It usually involves a employees, contractors and business partners who has access to sensitive information or in some cases privileged accounts within the network. This can be broken down into many different "descriptions" however as stated in the problem thesis statement. Careless insider is usually an innocent resource who commits actions that an adversary is looking to exploit by unknowingly exposing a system or information to external entity. This can take place in many different shapes or forms but in most scenarios, it comes from lack of good security knowledge or hygiene where the user is unable to identify such risks making them prone to a threat.

According to CISA, inside based threats (**CISA, 2020**) "The potential for an insider to use their authorized access or understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities. External stakeholders and customers of DHS may find this generic definition better suited and adaptable for their organization's use".

To better understand the direct impact on an organization, one question to begin with and establish a timeline narrowing the scope of this section is the thought process to what effect does

on-boarding procedures and user training that focuses on cyber security training has on the effectiveness of employee's ability to protect themselves from direct contact scam and\or exploit attempts? The answer in this case was part of a risk assessment program, companies are now incorporating an onboarding checklist to ensure HR includes a set of training material to go over with new hires. This helps educate newcomers on cyber security risks and help them understand security best practices on day one. Security training and awareness programs not only help educate users and build foundation for a strong "day one" approach, but it also inspires lasting behavior that would capture new employees attention to reinforce good secure habits while conducting business on or off company resources.

Another thought that was important to incorporate in this introduction to thesis was the ability of a solid cyber security system "airtight" approach designed to prevent security incidents caused by "innocent" insider threat usually known as "careless insider"? Here unfortunately, the answer is almost always not what organization wish for that an "airtight" system is the solution and as the author of this paper and from experience no matter how secure ones think their environment is. An end user with inside information can easily disrupt a company by participating in bad security habits. Just a few examples to go over can be posting password on sticky notes or hanging architecture diagrams on walls and leaving notes in conference rooms un-attended. That is a small set of examples that can bypass an enterprise cyber security program and place the organization at great risk.

Understanding insider threat is a crucial point that this paper attempts to highlight, so far, we understand the basics of how the mechanics from high-level works when an insider action results in an incident. And we can point out that insider threat exists within every organization where employees (insiders) comprise the core of an organization body and how they are key to

the success of its vision and execution plan. That considered, a threat against insiders that could be targeted or sourced by the insider for many reasons such as retaliation or perceived injustice and in some other cases sense of entitlement can and will have a consequence for the organization. Such incidents originate for many different reasons some are driven by financial gain, some for fame and other as indicated earlier to retaliate. Recession climate, workforce demographic changes or increased workload are factors that can play against organizations in a sense of protecting and ensuring the confidentiality integrity and availability. That is another reason that shows the importance of a framework that can be implemented to provider resources the tools and material they need to first identify such events happening in proximity within the organization and to defend against outsider's threats that they may experience via various tactics.

Starting to examine some of these tactics and uncover the level of sophistications that is being presented is a challenge for all types of organizations. Some can do better with technologies implemented and others fail to defend and fall victim to such threats. In both cases attacks will make it through to an insider and that's when they become crucial part in that line of defense where their action can dictate if company is at risk of being breached or not. One of the notorious tactics that attempts to exploit the user base is an attack usually referred to as **Phishing attack**. This type of attack happens when a threat actor sends an email that seems legit and coming from a trusted source in attempt to collect sensitive information from the target. This type of attack is usually combined with another type of attack known as **social engineering** where threat actor attempts to leverage initial data collected in attempt to gain further access to the victim host, network or information to escalate the sequence of this attack and further their knowledge in preparation for the next stage that may targets higher ranks within an organization that is known as **whale phishing attack** named this way since it targets primarily "big fish" of

an organization that typically C-level executives and board members that have direct access to sensitive material.

These types of attacks are usually seen in stage one of the attack surfaces, the initial contact phase. Once the victim provides enough information an attacker can deploy additional tactics to pivot from one user to another or what's more important to them is gain access to the victim account or host targeting them with **password attack** this can be done using different methods. In most cases for users in organizations that don't have solid security awareness training programs they tend to have exposed passwords or passwords easier to guess.

This level of access granted can be devastating for organizations since it can escalate quickly for them to the point of which they become a victim of ransomware or other types of attacks that can damage their operations and/or reputation. In a study done by SailPoint a leader in the identity and access management realm they dive into the number of annually reported incident attributed to insider threat or insiders targeted (**SailPoint, 2016**) "The number of annual incidents attributed to insiders is on the rise, and individual incidents are commanding more attention as their consequences become more damaging. The U.S. Government's focus on insider threat stems not only from the massive data breach perpetrated by Edward Snowden, but also from the fact that Snowden's disclosures came to light just three years after the Manning WikiLeaks breach. Response measures have come from a number of agencies and leading officials, including the White House. President Obama released the Cybersecurity Strategy and Implementation Plan (CSIP) and later the Cybersecurity National Action Plan (CNAP), which placed heavy emphasis on securing employee and contractor accounts at federal agencies to protect against data loss in the wake of the OPM breach, which occurred after attackers stole the password of a contractor. Additionally, Director of National Intelligence James Clapper placed

counterintelligence operations among his annual list of global threats to U.S. interests and the Department of Homeland Security expanded programs to monitor employee access levels through the Continuous Diagnostics and Mitigation (CDM) program. In May 2016, the Department of Defense published a change to the National Industrial Security Operating Manual (NISPOM) requiring any industrial, educational, commercial, or other entity with a facility security clearance (FCL) to establish and maintain an insider threat program to detect, deter, and mitigate insider threats". This combines both aspect of insider threat that can be looked at as a true insider threat where a resource going rouge or for the purpose of this paper as described in the first part of this introduction the focus on an unaware or naive employee that becomes part of a attack cycle unwillingly and unknowingly.

Literature Review

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 full-time employee or contractor with access to inside information and\or resources. This study will analyze the differences that security awareness programs can make to an individual and organization if they are aware and capable to handle scenarios that targets the human factor which tends to be the case almost on daily basis. In a more recent study done by one of the leading companies in the cyber space (**Crowdstrike, 2022**) "The FANCY BEAR adversary is associated with the 85th Main Center of the Special Services (aka Military Unit 26165) of Russia's Main Intelligence Directorate (GRU). Earlier in its operational lifespan, when conducting victim exploitation and credential collection, the adversary extensively used spear-phishing emails containing malicious documents or links that redirected to malicious infrastructure. However, after multiple exposures of its operations — particularly by the U.S. Department of Justice (DOJ) in 2018 — FANCY BEAR appears to have reevaluated their operational tradecraft and decreased their use of malware while shifting toward increased use of credential-harvesting tactics including both large-scale scanning techniques and victim-tailored phishing websites". This is one of many examples that sheds a bright light on the importance of having a second line of defense outside your technical and common email\web filtering solution knowing that such types of malicious content will find its way to an end user

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 bottom line where results are expected. Regarding a strict budget an organization may face the argument would be yes, there is cost associated in implementing a security awareness program but if it's not implemented and an individual action can become a security incident it can cost more than the initial investment required and that goes beyond financial damage to the point that the reputation of an organization specially in incidents that lead into data leak and ransomware is

devastating. Considering that the average ransomware payment in cases worked by Unit 42 that is a threat response unit operated by palo alto networks a leading organization in the cyber space (**Ryan Olson, 2022**) "The numbers are startling: The average ransomware payment in cases worked by Unit 42 incident responders rose to $925,162 during the first five months of 2022, approaching the unprecedented $1 million mark as they rose 71% from last year. That's before additional costs incurred by victims including remediation expenses, downtime, reputational impact, and other damages. Those costs are staggering when you consider the trajectory of their growth. The average ransom payment in cases worked by our consultants in 2020 was about $300,000. It's hard to believe that most transactions seen by our incident responders were $500 or less in 2016. Details of about seven new victims on average are posted each day on the dark web leak sites that ransomware gangs use to coerce victims into paying ransoms. Called "double extortion," the technique increases pressure on victims by adding a layer of public humiliation to the difficulty of losing access to files – identifying victims and sharing purported snippets of sensitive data stolen from their networks. The rate of double extortion we've observed translates into one new victim every three to four hours, according to Unit 42's ongoing analysis of leak site data."

This is one example, from a single report within a single organization that is on the front line of this cyber war. So, back to where this started in this section and to highlight this part within this literature review. Author supporting argument that cyber security is a team sport that takes all improve, this can be technology base improvements where applying controls and ensure systems are up to date maintained and managed by talented personal. also, to consider that organizations will have a large population that is not technical and will be targeted by a highly technical and sophisticated attacks in various forms therefore security awareness programs can

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 up in the theft of millions of identities including 3.6 million social security numbers, 387,000 credit and debit card numbers and 3.3 million bank accounts. Again, this is one of many examples and to keep in mind the fact that enterprises and governments aren't the only ones that are targeted individuals are also targeted and in fact one in 20 people were victim of identity fraud. Therefore, this type of attack can be prevented in most cases with a solid security awareness campaign so employees and individuals can become armed and enabled of how others may be attempting to manipulate them.

A common question that should be covered in this part of this paper is, is would a common person be targeted, or would an organization be targeted? well, most certainly. Hackers, corporate spies, cybercriminals and even nation states sponsored attackers all use social engineering tactics to gain unauthorized access to networks, sensitive information and systems. Their main goal is to steal intellectual property, personally identifiable information usually

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, someone in authority or a support staff. They usually tend to couple these attacks with psychological manipulation tactics like need, praise, or urgency. And there's not much technical controls that can prevent such threats other than for the victim to be always on the lookout suspicious when someone that they don't know makes contact. In these scenarios asking the right questions to independently confirm their identity by either contacting the company they represent or asking for other verification to ensure you are talking to the person or entity they claim to be calling from.

Bribery is just another form of social engineering tactics, sometimes cybercriminals know that a little bribery can be all it takes to trick and get insiders to do their dirty work. A study by (**University of Luxembourg, 2016**) describes that 30% of people are willing to divulge their password in exchange for a candy bar and even more shocking that 44% divulged their password if the candy bar was given first. This tactic known as bribery is commonly used in phishing emails. Cybercriminal attempts to convince the target that they will get something they desire if they click on a link or open an attachment. In these situations, as the old saying goes you don't get something for nothing therefore awareness campaigns that highlights these types of scenarios and educates employees to avoid such interaction and don't fall or be enticed to do something by promises of a gift or favor are great ways to empower the user base.

Next, is deception. Unfortunately, there are no solid or simple test for social engineers; in most cases they are skilled at deceit and lying they also come prepared with extensive research

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 tactics including a form of emotional manipulation to get

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.

Research Method

In this section, going over the research and approach taken to collect, analyze and interpret the data using qualitative and somewhat of a mixed method. Reason for selecting qualitative method is the time frame and target audience selected to better understand the topic of this research. While having a conversation with two prominent cyber security experts considering their advanced level of knowledge in the cybersecurity realm that would be of great significant to the results as the type and quality of security awareness training programs and how it can impact the results specifically for situations where they have prior knowledge that might be influencing the quality of this feedback.

An additional key item to point out in this conversation is highlighting the importance of both experts' ability to identify the benefits of such programs (Security Awareness Training), this research\conversation intends to show the likelihood of lapses in prevention should they notice and relate to risks based on this conversation and feedback received.

Both experts share their feedback that the author begins to evaluate and incorporate into the research results section to compare against the base of this paper and better understand the contrast between theory and real-life examples. That can help highlight whether the importance of such program and\or any deficiencies associated with relatively being high, meaning does it brings great value or relatively low value that it has very low to zero impact on the overall effectiveness of a security program.

As an author of this research paper having connections to a network of professionals that had the honor to work and learn from in previous roles, and with a solid understanding of information security and the impact it can have on companies. Both cyber security experts would be able to contribute to this research part of this conversation\discussion that would help us understand what impact it has and if it's something they think it should incorporate into the

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 very well it would be beneficial for this research to ask questions that can help others understand their background and involvement in current and previous roles. Other questions included are more focused on questioning their deep understanding of the specific topic to carefully inspect all aspects of the discussion and problem also to tap into their creative thinking when deciding what answer can be best answer to response with. That while maintaining good understanding that people in various positions and authority may have different technical skills which could influence their answers i.e., if the problem is looked at purely from a financial perspective vs having a clear sight into the entire problem regardless of financial constraints. This would be the biggest challenge this paper has to deliver and walk a very thin line between effectiveness and justification for cost and resources.

To provide another example of the expected feedback this conversation aims to dive into, is real world examples as mentioned previously. While constructing this paper one great example is the twitter attack in 2020, the story behind how twitter survived this attack and the plan to stop

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 support department within twitter asking them to reset their password. Employees started to report this to their security contacts but unfortunately few gullible ones were unknowingly cooperating with the bad actor doing what they told visiting a dummy site controlled by the attacker surrendering their credentials (username and password) as well as multi-factor authentication tokens. Within minutes of these events multiple twitter accounts with short handles were compromised. To elaborate further shorter handles are usually attractive and cost more hence the reason why they were compromised first in the early stage of this attack. By approx. 3:13 PM ET the handler for cryptocurrency exchange binance posted and unlikely tweet announcing that it was releasing $52 million worth of bitcoin to the community with a link to a fraudulent site. Over the next few hours total of 11 crypto accounts posted the same message with similar links. By 4:17 PM ET the handler of Elon musk tweeted a classic bitcoin scam visible to at then his 40 million followers. The stories of folks falling victim to this, that was the result of the initial phishing attack is devastating and heart breaking where people fell for such scam and did what they were asked to and ended up losing their own bitcoins and other sensitive information. This is the type of information expected and targeted part of the author conversation with both security experts and over all research design that focuses on highlighting such incidents and bring to light the importance of ensuring the workforce is ready to defend and not fall victim for such tactics. As a matter of fact, for this example incident twitter immediately after this incident announced a series of new security protocols, including mandatory employee training.

Results

Starting to dive into this conversation and the feedback received, we can determine that both experts obtained a solid experience in understanding various aspect of information security that is not only from a management perspective but also on a technical level.

Starting with the first conversation and feedback from the first security expert being very familiar with the topic of information security awareness training programs and having a direct role in supporting the underlying technology. Which is deployed in their current organization they have insight into the efforts and results that a small team can deliver with a relatively small budget. They can confirm that the return on investment is astonishing, going further to explain. With a well-designed program an organization can customize the contact required with the general population and follow a quarterly or semi-annual approach that a simple phishing simulation for example can yield high return in the form of identifying your most vulnerable users usually referred to as clickers. Let's say that we design a simulation campaign with instructions that misleads into clicking an obvious URL that should not be clicked. You then end up with a X number of clickers that actual clicked on something they probably shouldn't be clicking. You now have round one of trying to identify the group or groups of people in your organization that maybe vulnerable from phishing perspective. With that in mind you are able using technology to deploy some additional features that can protect them against such attacks. In this case specifically and to shed some light without exposing internal data they were able to work with a security awareness team to deploy something known as browser isolation that allows to proactively prevent malicious content from getting into their hosts while providing seamless experience for message delivery. Also understanding the behavior of the general population. With isolation implemented right they are now capable of defending against cyber threats not only within their mailbox but also while they engage in other types of browsing. That can be

directly attached to a security awareness program product that automatically detect and categorized “repeat clickers” which can be utilized to target such groups with additional content to help them improve their awareness for better security that would benefit both the individual and organization.

To that last point from this conversation mentioned above, in various scenarios they noticed that the feedback was not only the fact that individuals are becoming better at isolating such events during our conversation it was mentioned an event form 2020 during the pandemic one individual worked with closely had made comments regarding what’s being done in security awareness is paying off in their personal life where an elderly mother was a target of a vicious scam cycle surrounding the pandemic using social engineering technique customized as a health care insurance scheme. Some of these attacks were well designed to trick the victim to give up personal information and pretend to be representative of Medicare to gain more access to private data that would help them elevate their attack surface. With security awareness program this individual was able to sit with the elderly mother and using simple approach explain how these attacks can cause serious damage to the identity and financial records of a person. Unfortunately, not all stories have a happy ending like this one, they’ve encountered personally and professionally some devastating cases where folks lost access to their bank accounts for months, lost access to their identity where they couldn’t apply for any type of loans for months. They personally were a victim of such scheme but was able to defend against it whereas a target of something known as smishing. A technique usually means the combination of SMS (texting) and phishing, combining the two you have smishing which is the process cybercriminals use to “phish” by sending text messages instead the common process of email that phishing is known for.

Further feedback talking to both experts and focusing the results first for each, talking with the first security expert I'm able to establish now that they are very familiar with the concept of information security awareness training program. Also, having the experience from a technical and managerial point of view. They also believe that employee's behavior when it comes down to interacting with threats is very important to their organization. Also based on the feedback the author was able to establish that they themselves were a recipient of company training that focuses on security awareness mandatory by their respected organization. Based on that information they consider security training programs to be effective in mitigating threats targeting the human factor and can be considered as a good return on investment if they are well defined and constructed.

Next, the author focuses on understanding if that knowledge translates to a measurable impact that they were able to see or corollate based on their experience in the field. That did prompt for a question that aims to explore their engagement with recent events and how it impacted them. One that was mentioned almost immediately as first thing that comes to mind is the WannaCry ransomware because the employees played a major role in many organizations that fell victim to WannaCry. The reason being is that many employees with higher privileged accounts or admin privileges end up disabling security updates on their machines that let to infection spreading from their computer onto the rest of the corporate network. Hence, the security awareness program could have played a role on here, describing the importance of security patches/updates and explaining that when the updates are pushed to your machines they should be accepted and downloaded and not trying to avoid them just because your machine will be temporarily down. If we fail to elaborate the importance of security to all the employees, they will continue to avoid or find alternative ways how they can prevent these patches to take place

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 breaches had human involvement one way or another. About 80% of security breaches occur by phishing attacks. That would be a starting point in this argument by presenting the data to the leadership or anyone within the organization. Having concreate evidence is important to build a case and obtain support form leadership, which from that point on will help deliver the message to the rest of the company. Phishing attacks have been leading the way for most ransomware attacks as a method for cybercriminals to make money. Considering the impact that a ransomware attack could have to an organization, it's important to be taken seriously.

With that said, security awareness programs are one of the most effective methods we must focus efforts to counter. Phishing attacks originating by human interaction primarily. Building a security awareness program that is diversified from structured online courses to informal conversations, collaborations, and experimental exercises where information security teams are simulating phishing attacks is something that will benefit and bring awareness to the

overall organization about cybersecurity. Keep in mind security awareness should be just another layer or tool within the organization's security framework, you can't counter or defend an organization without having a stellar security awareness program in your organization.

Finally, while concluding the conversation with the first security expert next trying to better understand limitation by asking questions about the biggest challenges while trying to implement a security awareness program. A bit surprising as in most cases encountered cost was the main factor. However, based on this particular security expert feedback the biggest factor challenging a rollout of such program with consideration that this feedback coming for a large enterprise is the staff and resources required to develop and publish such material. That considered they would without hesitation implement a security awareness program at large scale and implement at a smaller scale if resources not available.

Authors conversation with the second security expert was like the first conversation based on their extensive technical experience provided some more specifics in comparison to the first that comes with a heavy managerial knowledge. This second expert being very familiar with this topic of information security awareness training programs. Having a management and exceptional architecting background understands how important it is for an organization to implement a solid program in place that empowers their employees in their day-to-day dealings ensuring they have the knowledge to fight against threats. Also, as a participant of such program themselves at their respected organization; it is clear that 2 out of 2 organizations (based on both feedbacks) have established a mandatory more than once a year type of training program. Next, asking about the importance of information security training programs and what do they consider them. For example, waste of time or great resource for employees; and the answer was precise that goes into explaining how security awareness programs are highly effective that is in terms of

fighting against various attacks such as social engineering and spam or other click baits that they may encounter in their day-to-day operations. However, the feedback from this security expert was clear that a well-defined security training program is a must for it to be successfully.

They also elected to pick the SolarWinds and Unifi breaches as a solid example they can recall that could've been partially mitigated and prevented if victims were armed with knowledge acquired previously from solid security training and awareness programs. This attack known as sunburst started as a routine software update as described by (**Dina of NPR, 2021**) "The routine software update may be one of the most familiar and least understood parts of our digital lives. A pop-up window announces its arrival and all that is required of us is to plug everything in before bed. The next morning, rather like the shoemaker and the elves, our software is magically transformed.

Last spring, a Texas-based company called SolarWinds made one such software update available to its customers. It was supposed to provide the regular fare — bug fixes, performance enhancements — to the company's popular network management system, a software program called Orion that keeps a watchful eye on all the various components in a company's network. Customers simply had to log into the company's software development website, type a password and then wait for the update to land seamlessly onto their servers.

The routine update, it turns out, is no longer so routine. Hackers believed to be directed by the Russian intelligence service, the SVR, used that routine software update to slip malicious code into Orion's software and then used it as a vehicle for a massive cyberattack against America. "Eighteen thousand customers was our best estimate of who may have downloaded the code between March and June of 2020," Sudhakar Ramakrishna, SolarWinds president and CEO, told NPR. "If you then take 18,000 and start sifting through it, the actual number of impacted

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.

By design, the hack appeared to work only under very specific circumstances. Its victims had to download the tainted update and then actually deploy it. That was the first condition. The second was that their compromised networks needed to be connected to the Internet, so the hackers could communicate with their servers. For that reason, Ramakrishna figures the Russians successfully compromised about 100 companies and about a dozen government agencies. The companies included Microsoft, Intel and Cisco; the list of federal agencies so far includes the Treasury, Justice and Energy departments and the Pentagon".

With the challenge described previously in this paper regarding getting support to implement such program, feedback from this second expert finds the following argument reasonable while making a case for their request. By lacking security awareness, you put at risk not only yourself (your employment, your savings and integrity of your identity) but also the company you're working for and its employees. Actions depending on your role can affect many other people and their livelihood. Which for me as a recipient of this feedback believes that this expert understands how important it is for organizations to implement such programs and

prioritize such efforts. However, they just like the first expert understand that the biggest challenge is getting the required staff and resources to develop then publish material required. Which brings us to the final point that based on their experience and read of the current landscape they would implement and advocate for such programs to be implemented without hesitation.

Conclusions & Recommendations

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, that may come from a look alike domain and quickly notify their security operation. Which in turn can take swift action to pull delivered messages and block the sender can have a huge impact preventing someone else from accidently clicking or interacting with an active campaign or threat actor. Also providing necessary education can truly help with the blind spots that an organization technical defense strategy is unable to detect as it was detailed in the literature review section within this paper. Some of the examples based on this research focuses on the human factor typically in the form of social engineering can be described to prevent some form of manipulation that may target employees and its counter measure can be concluded as followed:

1. Be always aware that a caller maybe impersonating another person.
2. Don't fall under pressure that could lead you into making bad decision, regardless of whether they are upset, yelling or in a hurry. Cyber criminals are comfortable using these tactics and have no remorse doing it over and over.
3. If your responsibilities require you to be in contact with folks external to your organization. You are more likely to be a target of a social engineering attack. Therefore, you must up the levels and be more vigilant in your dealings.
4. Understand and be able to locate or reference policies regardless of who is making the request.
5. Understand various methods available to confirm a caller is legitimate, for example trying to phone the caller back by ending the call first. Looking up the caller and then try to call them back for verification.
6. Always remembering that social engineers may know a lot about you or the company. They have the resources to perform extensive research and may have information from other victims therefore knowing things that only available on the inside does not legitimatize a call or email.

7. Never provide private or sensitive information to anyone who calls, unless due diligence and verification is completed to ensure you are interacting with legitimate contact.

This is a solid starting point to help build a strong foundation for security awareness program where the main goal is to help educate target audience on how they can be manipulated by social engineers, how can they be on the lookout for social engineering attacks and how these attacks may present themselves and playout walking through various scenarios. Also, how, and when sensitive information can be shared with others. Most important teaches them to be always suspicious specially with unsolicited contact made by email, social media sites, phones and in person at an event just to name a few. Also, help them build solid instinct and response tactic when something feels wrong and how they can simply say no and ask for help from others. And finally, to be able to take pride in defending against such attempts no matter how small and irrelevant it may seem while reporting unusual behaviors to a security department. And in turn for the security department to reward such efforts with recognition to help promote this type of behavior across the enterprise and build a culture that can thrive and be safe against cyber threats.

References

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

Appendices

Phishing attack: To initiate the attack, threat actor may send a link that brings you to a website that then fools you into downloading malware or providing the attacker your information. In many cases, the target may not realize they have been compromised, which allows the attacker to go after others in the same organization without anyone suspecting malicious activity.

Social Engineering attack: When threat actors bait the victim attempting to collect sensitive information by pretending to have information or services they can offer in return. One common example calling a victim to perform "password reset" for their network logon credentials due to a updated organization password policy update.

Whale Phishing attack: Like Phishing attacks, this however targets higher level of leadership that has access to sensitive material. Main audience can be c-level executives and/or board members and higher managements in critical areas such as finance, legal and human resources.

Password attacks: Type of attack that targets credentials, it could be pure guessing or based on information gathered previously. It can be brute force against a specific set of credentials or in other forms it can be dictionary based attack where an attacker has a pre-defined list of passwords to try against a specific set of credentials. In all scenarios attacker main goal is to gain unauthorized access to a set of credentials.

Insider Threats: When an employee (insider) acts with knowledge in malicious activity against their own organization. This term also used in this research paper to describe employees (insiders) that act without proper knowledge and have their action results in threat actors compromising part of the network.

Drive-by Attack: Type of attack that lures the victim to interact with a specific site they have infected with malicious content, when user visit that site actor then drops such contents causing the infection directly on the user account and\or system.

Web Attack: Type of attack that can be defined in many ways, primarily attack that reside and starts within the transport and application layer while visiting a site or receiving a URL that is malicious. Once activated it can cause the victim host to leak information and or be remotely controlled by the attacker.