5-24-2019

Qualities of Impactful Cyber Security Awareness Training

Fadi Labib
Portland State University

Recommended Citation
Labib, Fadi, "Qualities of Impactful Cyber Security Awareness Training" (2019). *University Honors Theses.* Paper 682.
https://doi.org/10.15760/honors.698

Qualities of Impactful Cyber Security Awareness Training

by

Fadi Labib

An undergraduate honors thesis submitted in partial fulfillment of the requirements for the degree of

Bachelor of Science

in

University Honors

and

Computer Science

Thesis Adviser
Wayne Machuca, Ph.D.
Cyber Security & Networking / Computer Information Systems

Portland State University
2019

Contents

Abstract 3

Definitions 4

Introduction 5

Contribution of Employees and Companies to Phishing 7

ISAT as a Solution 10

ISAT Shortcomings 13

Methods 16

Literature Review 17

Components of Effective Training 17

Delivery Methods 22

Lecture-Based Delivery Method 23

Programs/ Interactive Games Delivery Method 28

Group-Oriented Delivery Method 33

Simulated Attack Delivery Method 35

Discussion of Findings 43

Conclusion 46

References 47

Abstract

Social Engineering (SE) attacks are the most prevalent attacks targeting multiple industries, companies, and organizations. This research discusses the reasons for the prevalence of SE attacks and the weaknesses of the defense methods against it—Information Security Awareness Trainings (ISAT). Through an extensive literature review of the methods, experiments, and ideas of the past 20 years, the research compiles best practices for an effective ISAT program that is capable of changing employee behaviors and strengthening companies' security posture through its human element. The literature review is divided into two main sections. The first section is about the components that should be common to any type or format of ISAT regardless of the way it is delivered to the employees. The second section is about four different delivery methods by which companies could conduct ISAT and those are: (1) Lecture-Based Delivery Method; (2) Programs/ Interactive Games Delivery Method; (3) Group-Oriented Delivery Method; (4) Simulated Attack Delivery Method. From the literature review, it was determined that an amazing body of work related to designing and delivering an effective ISAT exists and that companies just need to find a way that works for them. Standard training is largely ineffective and thus companies must put in the time and effort to create materials that are relevant to their employees and combine multiple delivery methods. It is also important to note that ISAT should be a continuous year-round activity and not just done once a year or once in a lifetime. If companies learn to be patient and work out different trial and error scenarios, they will eventually find something that works best for them and as it matures, they will see an immense return on investment and an improvement of their overall security posture.

Definitions

Below are some reoccurring abbreviations that have been included here for convenience.

ISAT Information Security Awareness Training is the training given to employees to let them know the dos and don'ts of using technology with the goal of informing employees about security policies and procedures and preventing them from introducing security risks to the company.

SE Social Engineering is the manipulating human emotions or tricking victims into giving up personal or company confidential information by exploiting their trusting nature and their willingness to help others

BHSE Black Hat Social Engineers exploit people's weaknesses through phishing or another SE technique to obtain confidential information with the goal of using the information obtained to cause them harm. They could also be interested in harming the organization where the victims work.

InfoSec Stands for Information Security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. The information or data may be electronic or physical.

IT Stands for Information Technology and it refers to anything related to computing technology, such as networking, hardware, software, the Internet, or the people that work with these technologies.

ISA Information Security Awareness focuses on raising consciousness regarding potential risks of the rapidly evolving forms of information and the rapidly evolving threats to that information, which target human behavior.

Introduction

Workers in the information technology (IT) industry all agree that phishing, the fraudulent practice of inducing unaware individuals to reveal sensitive information about themselves or their company, is growing immensely and affecting the employees of many companies and organizations (Ki-Aries & Faily, 2017; McCormac et al., 2016; Flores & Ekstedt, 2016; Purkait, 2012; Ohaya, 2006; Orgill, 2004). The fraudulent practice perpetrators, for the purpose of this research, will be referenced as Black-Hat Social Engineers (BHSE). BHSE exploit people's weaknesses through phishing or another SE technique to obtain confidential information with the goal of using the information obtained to cause them harm. They could also be interested in harming the organization where the victims work. SE is about manipulating human emotions or tricking victims into giving up personal or company confidential information by exploiting their trusting nature and their willingness to help others (Dominguez et al., 2010; Frauenstein & Solms, 2009). Phishing attempts are forms of SE that have many variations, employ various tactics, constantly updated and quickly increasing in number and sophistication (Purkait, 2012; Kumaraguru et al., 2007; Ohaya 2006; Orgill, 2004).

According to Purkait (2012), "Phishing has become the most common channel for thieves to acquire personal information to aid them in identity theft". The typical way by which BHSE conduct phishing involves tricking victims into accessing a fake website by sending a fake e-mail, which looks reputable and contains a link that leads to a replica of a legitimate website. The legitimate look of the website deceives unaware users by providing them a sense of safety to disclose sensitive information under the false pretense that the website they are accessing is legitimate (Kumaraguru et al., 2010). In some cases, the attack leverages social media of targeted users to offer more personalized emails that guarantee a response from the victim (Jagetic et al.,

2007). Some of the phishing attacks conducted by seasoned BHSE involve tricking the victim into believing that they are an acquaintance. According to Jagetic et al. (2007), people are four times more likely to become phishing victims if a person appearing to be a known acquaintance solicits them.

As for the typical way of educating employees about the issue, it involves developing some form of Information Security Awareness Training (ISAT) module (Dominguez et al., 2010; Cooper, 2008). While many companies are realizing the momentousness of cyber security awareness training to diminish phishing risks (Caldwell, 2016; Shropshire et al., 2006), most of the training widely available to them is full of flaws (Ghafir et al., 2018; Ki-Aries & Faily, 2017; Caldwell, 2016; Shaw et al., 2008; Valentine 2006). These flaws hinder the advancement of the training to match the advancement of BHSE skills and techniques in gaining access to confidential data (Ohaya, 2006). The goal of this research is to establish that there is a gap between the quality of BHSE attacks (Flores & Ekstedt, 2016) and the quality of ISAT products available on the market to educate employees about the risks of not following good security practices (Cooper, 2008; Albrechtsen & Hovden, 2009; Caldwell, 2016). In addition, the research establishes that the gap could be narrowed down if companies prioritize training. BHSE attacks are consistently advancing and ISAT is failing to keep up.

Contribution of Employees and Companies to Phishing

Prevalence of phishing is a credit to a joint effort between both employees and companies, thus, realizing each of their contribution to phishing is a great first step in stopping the wide spreading of phishing attacks. O'Donnell (2009) states that for the "last five years, phishing has been growing rapidly, with an estimate citation of approximately 8 million daily phishing attempts all over the world" (as cited in Lungu & Tăbușcă, 2010). Furthermore, a report issued by the Anti-Phishing Working Group, in 2006, compiled 23,670 unique phishing attempts targeting 14,191 websites with the goal of committing malicious activity like identity theft and fraud (Dodge et al., 2007). According to BBC.co.uk (2017), the WannaCry Ransomware attack on the NHS in May 2017 "resulted in [a] significant meltdown of emergency services in the United Kingdom (UK)" (as cited in Ghafir et al., 2018). This issue could have been prevented had employees of NHS been trained on how to have good security practices (Ghafir et al., 2018). According to 2019, State of Phish report, released by Proofpoint security awareness training, "Across the board, [information security (InfoSec)] professionals identified a more active SE landscape in 2018. The vast majority—96%—said the rate of phishing attacks either increased or stayed consistent throughout the year, and more respondents said they experienced more attacks during 2018 than 2017" (Proofpoint, 2019).

Organizations attribute many security incidents they face to insiders and not external parties. Pricewaterhouse Coppers (PWC) (2015) findings suggest, "The behaviors of current employees were the source of 34% of security incidents" (as cited in McCormac et al., 2016). Ki-Aries & Faily (2017) emphasizes a point on the 2015 data breach report by PWC stating that a large number of internal data breaches were due to accidental employee error or employee's malicious intent. It is usually hard for users to detect signatures of fake websites and emails

because they appear legitimate. Many anti-phishing tools are available and could detect phishing emails and notify the users, but it does not help if the users ignore the messages (Kumaraguru et al., 2010). According to psychologists, people make poor and irrational decisions when under stress; they call it a singular evaluation approach to decision making. Stress could be simply an employee checking their emails while busy at work (Kumaraguru et al., 2007). Employees' decisions, under stress, could lead to them accidentally click on malicious links. End-users usually put security as a secondary task, when they access a service, say their bank account; their primary task is to check their account and not necessarily to check if they are actually accessing the legitimate website for their bank (Kumaraguru et al., 2007).

People [employees of a company or an organization] are the first line of defense against many information security threats (ENISA, 2006; PWC, 2010). It turns out, that the best way to exploit the weaknesses of this first line of defense involves the use of people—BHSE. It ends up being much easier for BHSE to tap into people's weaknesses than trying to bypass security implemented by companies who often use firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and other network equipment and computer security measures. Internal employees using the system have access to it without needing to go through the security systems implemented by the company to prevent access by non-internal users (Scott, 2009). Now, BHSE do not need to study the system they plan to attack or look for weakness, but rather they just need to develop their SE skills (Lungu & Tăbuşcă, 2010; Frauenstein & Solms, 2009).

Companies implicitly augment the prevalence of phishing attacks by putting tremendous emphasis on buying new hardware equipment and the latest and greatest bells and whistles to prevent hacking and data security breaches and forgetting, ignoring or neglecting the human element (Ghafir et al., 2018; Dominguez et al., 2010; Frauenstein & Solms, 2009). A survey

conducted by Kessel and Allan (2013) showed that "93% of companies globally are maintaining or increasing their investments in cyber-security to combat the ever-increasing threat from Cyberattacks" (as cited in Flores & Ekstedt, 2016). Most of that money, if not all of it, goes toward securing company physical assets like computers and network equipment. Companies focusing only on securing their perimeters from the outside world are not minimizing the risks of falling victim to security incidents. Organizations tend to forget that, "The security of any system is [like] a chain of components, only as strong as the least secure one. Confidence or assurance is also a chain, as strong as the least trusted link" (Dominguez et al., 2010). Even if organizations apply the best technology and numerous layers of strong defenses to mitigate security problems, all it takes is a small mistake from one of their members to undermine the strength of the security (Öğ˘ütçü et al., 2016; Dominguez et al., 2010; Shaw et al., 2008; Dodge et al., 2007). Phishing attacks can be catastrophic for victim companies; the cost is usually gauged based on three categories of damages: (1) loss of productivity from employees, (2) business impact through the loss of proprietary information, and (3) damage to business reputations. According to the State of the Phish Report, which surveyed nearly 15,000 InfoSec professionals, "67% of InfoSec teams surveyed said they suffered a loss of productivity for employees, 54% suffered business impact through a loss of proprietary information, and 50% suffered damages to business reputations" (Proofpoint, 2019).

ISAT as a Solution

Kumaraguru et al. (2010) define three categories of strategies to deal with phishing attacks. The first one is silently eliminating the threat by finding and taking down malicious websites and deleting phishing emails automatically. The second one is warning users about the threat by using toolbars, browser extensions, and other mechanisms. The final one is training the end users not to fall for the attacks through ISAT programs. Many experts recommend ISAT as one of the best solutions to address the human element of cyber security breaches (Dodge et al., 2007) along with other approaches like automated detection (Kumaraguru et al., 2010). Shaw et al. (2008) report that one of the reasons for the reduction between 2004-2006 on the number of reported security breaches was due to the investment of small and medium-size companies in InfoSec technology and ISAT programs. This continues to be the case in 2019. According to Proofpoint State of the Phish Report (2019), "57% of InfoSec Professionals said they have been able to quantify a reduction in phishing susceptibility based on their training activities; this is a 6% increase from what was reported in 2017" (Proofpoint, 2019). Furthermore, "In a survey conducted in 2004 by Ernst & Young, respondents named lack of security awareness by users as the top obstacle to effective information security" (as cited in Dominguez et al., 2010). Public officials, security researchers, and organizations have recommended ISAT (McCrohan et al., 2010). For example, the United States Military Academy (USMA) has actively been implementing hands-on exercises to teach security best practices, including email phishing exercises (Dodge et al., 2007). An Executive Order issued by President Bush in May 2006 declared, "that in its effort to protect the public against identity theft, the US Federal Government needs to improve its public outreach aimed at educating the public about the risk of identity theft, including advising them of measures that can be undertaken to protect personal data" (as cited in

Butler, 2006). McCrohan et al. (2010) include part of a 2009 statement by the press secretary upon the conclusion of the cyberspace review. It stated that "[c]alls for training and awareness predate Presidential Decision Directive NSC-63 [of 1998], the Clinton Administration's directive on security in cyberspace, and are part of President Obama's comprehensive review to ensure a secure global digital information and communications infrastructure". Investing in raising employees' security awareness is thus vital to the protection of companies' sensitive data.

While ISAT is the solution, organizations cannot just decide to buy some training package, check a box, and claim that issue is solved and move on; the training must meet certain criteria in order for it to be effective. The goal that ISAT is trying to achieve is complicated as, at its core, it is trying to harden "human assets" of a company (Cooper, 2008); it is by far the hardest asset to harden—a direct result of the fact that humans are the weakest link in the protection of an Organization InfoSec system (Ghafir et al., 2018; Caldwell, 2016; Flores & Ekstedt, 2016; Shropshire et al., 2014; Furnell & Clarke, 2012; Dominguez et al., 2010; McCrohan et al., 2010; Frauenstein & Solms, 2009; Shaw et al., 2008; Butler, 2006; Orgill, 2004; Schultz et al., 2001). The weaknesses of humans lie in their malicious intent or their carelessness in not following good security compliance behaviors (Shropshire et al., 2014). Shropshire et al. (2014) go further to explain that, "Each individual end user represents an endpoint in a computer network or a system and without security-compliant behaviors on the part of each end user; the network will not be secure[d]". Whitman (2003) identifies secure behaviors on part of end users to include things like patching software application, scanning for viruses, having a change password policy, and performing backup for data. "In addition, many end users lack the ability to appraise security risks and identify appropriate countermeasures" (as cited in Shropshire et al., 2014). In order for companies and organizations to minimize the risk of

breaches from employees' faults, they must make sure that all their employees develop Information Security Awareness (ISA) (Shaw et al., 2008). Kruger & Kearney (2006) define the focus of ISA as "the extent to which an employee understands the importance and implications of InfoSec policies, rules and guidelines, and, the extent to which they behave in accordance with these policies, rules and guidelines" (as cited in McCormac et al., 2016).

Research by IBM Global Technology Services (2014) claimed that about 95 percent of security incidents were human errors related. Thus, "security is not a problem of technology, but a problem of human nature and the behavior of information systems users and information system security awareness needs to be assessed and evaluated accordingly" (Ögˇütçü et al., 2016). The most effective way to prevent phishing attempts is through educating the end-users (the victims) so that they do not fall for it (Dominguez et al., 2010). More importantly is that the education program should be robust to ensure that workers understand their responsibilities and organization policies as they relate to IT and protection of resources they use constantly (Shaw et al., 2008).

ISAT Shortcomings

As important as ISAT is, neither the program designers nor the organizations applying the training give it the importance it deserves. Valentine (2006) writes, "This is the problem that security engineers and systems administrators have faced for the last 20 years. First, they spend half their time struggling with end users who open every single attachment that shows up in their inbox. The other half of their time, they spend working to convince upper-management that information security is . . . an important issue – a business issue – and one that needs to be included in next year's budget". In order for the training to be effective, the employees receiving the training along with their managers should feel that the training is important; many times, the users do not believe they had security concerns (Flores & Eksedt, 2016). Mistrust of ISAT program is understandable especially given the fact that many training programs are mediocre in their quality and effectiveness (Ghafir et al., 2018; Ki-Aries & Faily, 2017; Caldwell, 2016; Shaw et al., 2008; Valentine, 2006).

One of the biggest issues with traditional out-of-the-box ISAT programs is that they provide "a static solution to a fluid problem" (Cooper, 2008); they are not structured in a way to fit different organizations needs and sometimes they do not have a structure at all (Ki-Aries & Faily, 2017; Valentine, 2006). Different companies have different weak points and different types of people. The majority of ISAT programs do not account for such changes. The training is often lead by a security professional with no input from the users (Cooper, 2008). Typically, ISAT programs are not up to date (Cooper, 2008; Dominguez et al., 2010) and the security information they contain lacks "relevance, timeliness, and consistency" (Shaw et al., 2008). Users are generally not motivated to read about security or educate themselves about phishing (Kumaraguru et al., 2010; Kumaraguru et al. 2007; Valentine, 2006); the last thing they want is a

boring and irrelevant ISAT program. In addition, "information risk profiles never stop changing" (Shaw et al., 2008). "Rohyt Belani, CEO and co-founder of PhishMe . . . [stated that] standard [ISAT] modules can actually disengage employees . . . because they are typically boring and out of context, allowing employees to ignore or quickly click through without engaging with the security content being offered" (as cited in Caldwell, 2016). According to Ki-Aries & Faily (2017), "Research suggests current security awareness approaches do not entirely meet this requirement of designing for the user". Furthermore, "Some approaches rely on invocations of fear to change behaviors, or result in a lack of motivation and ability to meet unrealistic expectations, which may derive from poorly designed security systems and policies". Many pieces of training are framed in a way of directing people to do something but fail to provide a reason—the why (Cooper, 2008).

Many ISAT programs that organizations implement fail to have a follow-up element to them to make sure that the participants have retained the information they supposedly learned from the training (Caldwell, 2016). They often lack incident response procedures (Valentine, 2006). Shaw et al. (2008) state that most ISAT programs available fail to bridge the gap between perception and behavior. Ian Trump, a security lead at LOGICnow mentions another problem with ISAT program, which is the fact that "it's difficult to record success. When [ISAT] works – when a phishing email is not opened – nothing happens and it’s business as usual" (as cited in Caldwell, 2016).

ISATs developers themselves do not give enough focus to the quality of the training they create or hold it at the same importance as other security solutions (Dominguez et al., 2010; Valentine, 2006). When developers design and implement ISAT programs, they usually intend for it to achieve a compliance aspect (Ki-Aries & Faily, 2017); they could care less if employees

retain the information after they conclude the program. ISATs facilitators and planners do not conduct ISAT on regular basis and execute it badly and in an ineffective way (Caldwell, 2016). A successful ISAT program must account for all the weakness that this research mentioned. Multiple scholarly articles proposed approaches that deal with these issues. The rest of the research will cover those solutions and add more to the literature by suggesting combinations of the solutions presented to ensure companies deliver a continuous, holistic, customizable, and engaging ISAT program.

Methods

This literature review will cover the past twenty years looking for proposed solutions for effective ISAT programs. The articles were gathered through a search in Google Scholar and using Portland State University Library, ACM Digital Library, and Academic Search Premier. In addition, some journals were obtained through Elsevier. The search used the following keywords: "Information Security", "Security Awareness", "Security Training", "Social Engineering", and "Phishing".

An annotated bibliography was performed in all the articles that were obtained through the search terms and the ones relevant to the research were kept, and the rest were discarded. The journal articles that were kept went through a deeper analysis process looking for citations within them that mention relevant journals to the topic of effective cyber security awareness training. Many of the citations within the articles kept cited other articles that were already part of the initial list. However, some articles were obtained from the sources kept, and were not in the initial pool of relevant articles. This process continued until all the relevant articles that were referenced were part of the list. The new articles obtained through this process were analyzed and they provided valuable information to the specific topic that this research is addressing.

The rest of the research will be a thorough analysis of all the suggestions for effective training approaches that were obtained from all the articles. The proposed suggestions are divided into two sections. The first section is components of effective training and the second section suggests delivery methods for effective training. The four delivery methods suggested are (1) Lecture-Based Delivery Method; (2) Programs/ Interactive Games Delivery Method; (3) Group-Oriented Delivery Method and; (4) Simulated Attack Delivery Method.

Literature Review

The literature offers many suggestions to enhance the quality of ISAT programs so that the training achieves its goals of raising employees' security awareness and having a lasting impact. The solution involves two steps. The first step is a collection of common components and frameworks that should be part of every ISAT program, which will be discussed in the "Components of Effective Training" section. Then the second step is to pick one or multiple of four delivery methods discussed above.

Components of Effective Training

Frauenstein & Solms (2009) offers a model that would allow for the implementation of a holistic ISAT program. Their holistic approach contains three equal dimensions that companies should consider to enhance their security posture and to have a set of standards, guidelines and best practices that governs all of the three dimensions. The three dimensions are technological factors, organizational factors, and the human factor. Technological factors are about investing in security hardware and following security best practices of backups, patching, etc. while organizational factors have to do with human resources recruitment of skilled and trustworthy staff. Additionally, organization factors include making recruited staff aware of policies, standards and the reprimands for failure to comply. As for the human factor, they recommend ISAT programs that are up-to-date, relevant to issues that affect the company and have incentive or humor in order to engage employees.

Dominguez et al. (2010) offer a framework for the human factor element addressed in Frauenstein & Solms (2009)—that is a framework for implementing an effective ISAT program. The research bases their proposed framework on empirical data from a Puerto Rican study of two

highly regulated industries, banking, and insurance, with the goal of maximizing the return on investment pertaining to ISAT programs. There are seven inputs to any ISAT program, the more inputs added, the higher the quality of the ISAT program. The seven inputs in no particular order are: (1) Management Support; (2) Assessment (some form of quizzes to validate understanding and listen to users' inputs); (3) Policies; (4) Auditing; (5) SE Awareness; (6) Compliance and (7) Technology Tools (delivering training using advanced technology that can reach multiple people, like online recorded training).

The human factor is the focus of this research. In order to strengthen the human factor of security, organizations need to implement ISAT programs that are effective in raising employees' awareness of SE and have certain elements to them regardless of the chosen delivery method for the training. Most of these elements are best summarized through the nine lessons learned in Cooper (2008) while they were implementing an ISAT program at West Virginia University (WVU) for their students and employees. The first two lessons are to have a policy in place and seek and obtain approval of the policy to cover all constituencies before commencing with the training. These lessons agree with Frauenstein & Solms (2009) where they stated that policy and guidelines cover the three factors of the holistic ISAT program—including the human factor.

The third lesson is to "fully investigate and understand the content of any commercial package that is being considered for implementation" (Cooper, 2008). While Valentine (2006) discusses the merits of companies using widely available "Pre-Packaged Awareness Training" programs and offering those pieces of training as "fully formalized product line with live seminars", he also argues that they are quickly becoming obsolete (Valentine, 2006). Valentine (2006) discussed three merits that he liked. The first is that when organizations would buy those packages, they would offer it to all their employees with clearly set expectations so that

employees understand both the "what" and "why" relative to the policy. Second, he liked that the pieces of training are readily offered in an "assembly line" nature, which allows for a uniform and low-cost training that can reach multiple employees without any geographical boundaries. Finally, he liked that the curriculum could be easily adapted to fit organization needs. Valentine (2006) offers a solution to the obsolescence limitation that would grow the programs from their infancy using a fully realized multi-phased approach following specific methodology tailored to organization's needs and their specific security weak points. The multi-phased approach includes three key components: (1) Assessment Phase, (2) Identification Phase, and (3) Education Phase. In the assessment phase companies asses what assets they wish to protect along with their attack vectors; which employees are vulnerable to which attack vectors. In the identification phase, companies determine which employees interact with which data they identified in the assessment phase. By doing so, companies can be sure to break out of the "Security Basics" model and offer specialized training that is engaging and relevant to their employees. The third phase, the education phase, involves knowledge transfer that companies could achieve through a simulated attack approach as will be discussed later. The first two phases, involve finding the difference in the audience that will participate in the ISAT program. In McCoy & Fowler (2004), they found that it is important to define the different audiences the security training is targeting in the early stages of planning. For example, when they were implementing ISAT program for their university they quickly realized that splitting the audiences to simply students and faculty/staff was not sophisticated enough to account for differences within the students' group and the faculty/staff's group.

Reaching variety of audiences is critical that two separate pieces of research, one in 2016 and another in 2017, specifically focused in ways to identify the different audience in order to

create ISAT materials that are relevant to all the groups within the organization. First is the McCormac et al. (2016) research, which focused on individual differences as a mean to help ISAT programs developer determine which variables in human difference effect individuals' ISA and thus design tailored ISAT programs. The variables that were under study are age, gender, personality (using The Big Five model), and risk-taking propensity (the tendency of an individual to either take or avoid risks). The Big Five personality model has five factors and these are neuroticism, extraversion, openness, agreeableness, and conscientiousness. These researchers measured the variables using a questionnaire called "The Human Aspects of Information Security Questionnaire (HAIS-Q)" that was developed based on the knowledge, attitude, and behavior (KAB) model and distributed to 505 individuals (286 females and 219 males). For the age distribution, 12% of participants were in the range of 18-29, approximately 25% in each of the 30-39 and 40-49 ranges, approximately 22% in the 50-59 range, and 15% over 60. The participants were from 13 different sectors and 8 job areas including sales, laborers, professionals, management, and technicians/trade workers. The study found that conscientiousness, agreeableness, neuroticism, and risk-taking propensity significantly explained variance in individuals ISA, while age and gender did not (McCormac et al., 2016).

The second research conducted by Ki-Aries & Faily (2017), which assists ISAT designers and developers to find out how to cater their programs to multiple individuals by identifying security related human factors using personas. Personas are archetypical descriptions of users that embody their goals. This is the only research to date that uses the human-computer interaction (HCI) method to integrate human factors into ISAT using personas. The persona-centered ISAT methodology cycle involves six ongoing stages that can be embedded into business-as-usual activities with 90-days cycle of awareness activities. The six stages are (1)

establishing needs and goals using business supported requirements, (2) Personas, (3) Analysis, (4) Design & Development, (5) Implementation, and (6) Review.

The first stage involves eliciting requirements like, "assessments, surveys, and focus groups to establish business needs and current security culture, locations, risks, roles, responsibilities, resource, budget, and any other identified project related dependencies" (Ki-Aries & Faily, 2017). The second stage, and most crucial, is integrating personas. This is done by first organizing interviews with a random pool of users across the organization and using the results of the interviews to construct personas. The research recommends recording the interviews rather than taking notes to keep most of the information gathered intact. The information is then used to construct attitudes, motivations and business context for different personas and give each of those personas associated characteristics and a representative photograph to help humanize the persona. The third stage is the critical analysis of business needs, risks, and requirements against the identified behaviors and characteristics of each persona in order to establish and prioritize awareness needs. The fourth stage is designing and developing the tailored content to fit the data gathered from the previous three stages. The fifth stage is implementing and rolling out the program using a strategy defined at this stage. The final stage is to review and use the feedback to keep the program up to date and reflective of companies' needs (Ki-Aries & Faily, 2017).

Applying those steps to an actual company X, Ki-Aries & Faily (2017) found that, "persona-centered information security awareness approach has the capacity to adapt to the time and resource required for its implementation within the business, and offers a positive contribution towards reducing or mitigating Information Security risks through security awareness" (Ki-Aries & Faily, 2017).

Back to the Cooper (2008) article, the next two lessons that they learned are: (1) that companies should conduct a full assessment of the efforts to develop their own content; and (2) keep in mind that their best estimate of time and resources will most likely be exceeded. The sixth lesson learned is for companies to "follow the steps that prove to be successful and involve as many people as possible in the review steps" (Cooper, 2008). The seventh lesson is for companies to utilize "project management skills and avoid introducing requirements that may not have been a part of the initial planning of the project, while nevertheless failing to adjust schedule and budget" (Cooper, 2008). It is important for companies to use a Learning Management System that is common to all their constituencies is the eights lesson. The ninth and final lesson is to for companies to never give up and forge forward because successful ISAT program is both important and achievable for all employees of an organization.

Another recommendation to keep in mind, and that is not covered by the nine lessons from Cooper (2008) is mentioned in McCoy & Fowler (2004), where they found it helpful to have some branding for consistency and recognition and thus they created a logo and a yearly changeable theme. The curriculum is year round and every month has its own theme topic, for example, January's theme was "Password Safety & Security". Another important point was raised in Valentine (2006) research where they mentioned that ISAT should include an incident response element that is given to more employees rather than reserving it to incident response teams. Some companies do not even have an incident response team and it is more critical for those companies to integrate incident response to their ISAT program.

Delivery Methods

Once a company carefully designs a program based on the "Components of Effective Training" section and finds out their target audience and the content they need to cover, it is time

to pick the delivery method. An organization may pick one method or a combination of the method depending on what they see as most effective and within the limits of their constraints. The four delivery methods suggested by the literature are lecture-based, interactive games and programs, group-oriented, and finally simulated attacks delivery method. The research summarizes multiple works of literature that have tried and evaluated a single or combination of these four delivery methods.

Lecture-Based Delivery Method

The lecture-based approach delivers the content via online training, instructor-led training, or a combination of the two. It involves the use of multimedia, visual aids, quizzes, tests, etc. In the lecture-based delivery method, the content may be delivered in the form of hypermedia, multimedia, hypertext, or a combination. In Shaw et al. (2008), they conducted a laboratory experiment to investigate the impact of hypermedia, multimedia, and hypertext on increasing information security awareness among three awareness levels using an online training environment. They defined hypermedia as an interactive medium consisting of graphics, audio, video, plain text and hyperlinks that are all intertwined together to create a non-linear medium of delivery. Multimedia and hypertext are both defined as linear methods of delivery. The difference is that in multimedia, there are interactive elements, like hypermedia, but user accesses them in a linear fashion. On the other hand, hypertext is plain text with hyperlinks that lacks feedback capability and multiple cues.

The three awareness levels that the study used as a metric for each of the three forms of delivery were perception, comprehension, and projection. They defined perception as user's sense and ability to detect potential risk in their workplace. Comprehension was defined as the user's ability to assess and understand the dangers posed by different security risks and

projection is about the user's ability to predict the future course of security attacks. A user at the projection level would have the highest level of understanding of their environment and would be trusted to make timely decisions in emergencies. The results indicated the following: (1) that learners who have better understanding at the perception and comprehension levels can improve understanding at the projection level; (2) learners with text material perform better at the perception level; and (3) learners with multimedia material perform better at the comprehension level and projection level (Shaw et al., 2008). Thus when developing a lecture-based approach it is a good idea for developers to use hypertext materials to increase learners' perception, then use multimedia materials to increase learners' comprehension and projection. An effective lecture-based approach must be one that is capable of improving learner's understanding at the projection level.

Some literature implemented a lecture-based approach with an online element like McCoy & Fowler (2004) and Cooper (2008) and integrated additional reinforcement methods for topics learned during the online training they offered. Others like Robilla and Ragucci (2006) and McCrohan et al. (2010) went with strictly instructor-led training. Robilla and Ragucci (2006) measured the effectiveness of their lecture-based training using a 12 questions IQ test. Some even had a combination of both computer-based training and instructor-led training like Ghafir et al. (2018).

In McCoy & Fowler (2004) they offered their student, faculty and staff year-round lecture based security training. For students, their delivery method was targeted mass e-mails, articles in monthly technology newsletters, ads in student newspaper and presentation for different groups and clubs. They have also planned additional methods to reach their on-campus population using security awareness posters in their residence halls, mailbox stuffers, and table

tents in their dining halls. Since it was hard for the university to gather all students for an in-person training they went with a web-based training approach. When it came to training faculty and staff, they used a combination of multiple lecture-based training approaches including a free one-hour in-person training class covering multiple topics that are coordinated by different departments along with online training, covering the same topic, but targeting people who cannot attend the in-person session. They have also integrated into their training poster campaigns, articles in their monthly technology newsletter, targeted mass e-mails, and payroll stuffers. For administrators, with a tight schedule, they went with a more concise version of the training. Cooper (2008) followed more or less the same approach of McCoy & Fowler (2004) where their ISAT program was delivered as an online module to WVU students and employees. In addition to the online training, WVU published articles for a campus publication, presentations made at new employee/student orientation, poster displayed throughout campus, brochures with security tips distributed to employees and students, and information posted on websites visited by employees and students. In addition, they had targeted presentation delivered to specific audiences on demand. The reason for all of those alternative venues was to guarantee that the information learned from the curriculum is not forgotten and that employees and students are kept up to date on how to protect themselves from falling victims to SE. Effective lecture-based training should involve additional mediums in addition to lectures in order to cement the information and ensure continuous awareness.

Robilla and Ragucci (2006) discussed a limitation of a phishing IQ test designed by Mail Frontier to educate users on identifying phishing vs. legitimate emails. Once a user has identified all the phishing from non-phishing emails, they are given a score of how well they were able to find phishing emails. While data showed that 82% of test takers identified phishing emails

correctly, it could be attributed to the fact that some test takers identify all emails as phishing emails. This is especially the case as worldwide only 52% of the times are phishing emails identified correctly. The approach they are suggesting is keeping that same test but adding a context-aware element to it. The idea would be to modify the test to include phishing emails for web sites that the users are familiar with, rather than showing them websites of companies they have never heard of before and would not be able to distinguish legitimate vs. illegitimate email coming from them. The survey developed involved 12 questions, each with an e-mail familiar to the survey takers in Montclair State University (MSU) and participants are asked to identify if the email is a phishing attempt or not.

The ISAT program designed and deployed by Robilla and Ragucci (2006) had a formal education element to it. It was a lecture where participants learn about phishing and discuss its implications. Another example with a formal educational element to it, that is strictly instructor-led, was the study conducted by McCrohan et al. (2010). The study was a lecture-based approach that offered an intervention by randomly assigning subject to one of two introductory lectures about cyber threats due to poor password management. They picked passwords as a measurement of change in security behavior because of "their continued importance to computer security as well as their continued failure to provide adequate protection" (McCrohan et al., 2010). In addition, the tendency of human to select password from a small domain and that are easily guessable through widely available password guessing and password-cracking tools have been identified in numerous studies that are discussed in McCrohan et al. (2010) research. The results from Robilla and Ragucci (2006) test have shown that students at MSU are mostly oblivious to phishing threats, but through education, they were able to correctly identify most threats and also indicate positive appreciation of the session and its usefulness. As for the

McCrohan et al. (2010) research, they concluded that when users were educated by not only general background information but also putting it in perspective of dangerous of week password to e-commerce sites, it was possible to change their behavior to enhance online security for themselves and the companies where they are employed.

Robilla and Ragucci (2006) and McCrohan et al. (2010) suggest that there is a positive element to instructor-led lecture-based approach but that perhaps companies and institutions must look for more creative and non-standard approaches to phishing awareness and SE education. It looks like a lecture-based delivery method is a valid starting point. Conducting an IQ test could be a smart way to gauge employees' phishing awareness before applying a more sophisticated delivery approach (Robilla and Ragucci 2006).

Perhaps the best lecture-based approach is the one suggested in Ghafir et al. (2018) as it not only combined both computer-based training and instructor-led training but also used another delivery method. In the research, they talked about the benefits and drawbacks of computer-based and instructor-led training and then proposed a way to combine the best of both in a single hybrid system. This means their system would carry out situated learning, which would involve the use of a computer-based training tool along with visits by a trainer that will reinforce the knowledge gained by the employees through the computer-based training. The trainer would also offer special examples and topics that are customizable to companies' needs that have been identified during the planning stages. The instructor-led training sessions, while short and intermittent, would be continued through the computer-based tool with an integrated support mechanism. The training program offered in Ghafir et al. (2018) not only combines many of the elements discussed in the "Component of Effective Training" and offers a lecture-based delivery

approach involving both online and instructor-led portions, but it also designed a client-server program to administer the training.

Programs/ Interactive Games Delivery Method

Once time has been spent into planning for the curriculum and an effective lecture-based delivery method is designed, it might be worth it for companies to add more advanced delivery methods. Such methods would be beneficial in keeping employees engaged and ensuring that they retain the information for a longer duration of time than just a plain lecture. One such delivery method is using a program or an interactive game. Two pieces of research used the programming approach as the delivery method. First is Ghafir et al. (2018) and the second is Shropshire et al (2014).

The program Ghafir et al. (2018) designed and implemented is a client-server situational security awareness framework. The server-side, allows the administrator to configure the content of the security program including picking the modules that best fit companies' concerns. Each training module covers a specific topic or aspect related to organizations' security awareness. The program gives visibility to the administrator to monitor the progress of each user and assign deadlines for the completion of different modules. The client-side includes an integrated network framework that monitors users' activities on their workstations and will automatically present relevant and informative content using pop-ups. The framework also has the capability of checking password strength and offering additional information on security topics.

In Shropshire et al. (2014), they went with a program that is more focused on monitoring users' activity than Ghafir et al. (2018). Their program was another web-based security program called Perimeter Check. The program "analyzes the user's computing environment, identifies potential vulnerabilities, and recommends actions that might improve the safety level for various

computer activities" (Shropshire et al., 2014). The program was tried by undergraduate students enrolled in an introductory economics course at a large university in the southeastern United States. From 180 students only 54 visited Perimeter Check website and used the software. To measure the effectiveness of the web-based products, six measurements are used and those are: (1) perceived ease of use, (2) perceived usefulness, (3) perceived organizational support, (4) adoption intention, (5) conscientiousness, and (6) agreeableness. The results were that perceived ease of use and perceived usefulness were found to be significant predictors of software adoption intention. Adoption intention, as a predictor of initial use, was found to be significant although it explained less variance than expected. The majority of the sample population indicated an intention to adopt the security measure, but less than a quarter actually followed through on their intentions.

Overall, using a program to monitor users' security behaviors, which allows users to receive customizable modules, offers an advanced solution to enforce good security practices in a continuous manner. Another similar approach involves designing programs that teach security content, but those programs are games. Games offer a great way to teach security concepts; those games are usually called Serious Games (CJ et al., 2018). One example of such games is the one developed by Kumaraguru et al. (2010) called Anti-Phishing Phil.

The game involves a young fish named Phil who wants to eat worms so he can grow up to be a big fish, but he must be careful to eat real worms and avoid fake ones. Each worm could have a real legitimate web site, thus a real worm, or it could have a phishing URL that would make it a fake worm. The game is split into four rounds, each of which is two minutes long. Before each round begins, players must view a short tutorial that provides anti-phishing tips. In each round, the fish is presented with eight worms, each of which carries a URL that is displayed

when Phil moves near it. The player would move Phil around the screen to "eat" real worms and avoid or reject fake ones. The game rewards the player 100 points if Phil ate a real worm or rejected a fake one. The game slightly penalizes players, by deducting 10 seconds off their current round clock, if they had Phil reject real worms (teaching users to avoid false positives). Players suffer severe penalties by losing one of three lives if they caused Phil to eat a fake worm. Players must correctly recognize a minimum of six URLs within two minutes to move to the next round. When a player loses all three lifelines, the game is over. At the end of every round, a review screen is displayed, showing all of the URLs from that round and tips for identifying them correctly thus making sure users learn from their mistakes in a fun way.

Kumaraguru et al. (2010) conducted two studies on the effectiveness of the game. One was a lab study and the other was a field study. In the lab study, participants were asked to examine 10 websites (half-legitimate and half-fake) and determine phishing ones before playing the game and after playing the game. They recruited 28 participants with little technical knowledge and randomly assigned them to either reading anti-phishing tutorial created based on the game or playing the actual game. For the game, they measured learner's knowledge acquisition by examining false positives (legitimate website determined to be fake), false negatives (fake website is deemed legitimate), and the total percentage of correct Web sites identified before and after playing the game. The game, "performed roughly as well as the existing training material condition in terms of false negatives, and better on false positives" (Kumaraguru et al., 2010). The lab experiment has shown that posttest false negatives in both groups decreased significantly from the results of the pretest. As for the game condition, posttest false positives rates decreased significantly ($p < 0.03$). The summary of the lab study demonstrates, "that users show significant improvements in their ability to identify phishing links

correctly after 15 minutes of training with Anti-Phishing Phil, and with the tutorials developed based on the game. However, participants in the game condition were better able to distinguish between phishing and legitimate links than those in the other conditions and were thus less likely to incorrectly identify legitimate links as phishing links" (Kumaraguru et al., 2010).

The field study portion in Kumaraguru et al. (2010) involved 4,517 people. Participants would be shown six websites before playing the game (pretest) and then six more websites immediately after playing the game (posttest). To measure retention, a delayed posttest was sent to participant via their emails one week after playing the game. In total, each participant in the game condition saw 18 Web sites divided into three groups of three phishing websites and three legitimate websites. Each group had a random order of the websites within each of the three groups and even the groups were randomly shown to participants. The results also demonstrated that, "users are able to more accurately and quickly distinguish phishing [websites] from legitimate [websites] after playing the game, and that they retain knowledge learned from the game for at least one week" (Kumaraguru et al., 2010). The results from both the lab study and field study show that the interactive gaming approach has its merits, especially in reducing false positives.

Anti-Phishing Phil was used in another research, among other methods, to test if the game is actually effective in teaching security concepts related to SE and phishing. The multiple delivery methods used in Sheng et al. (2010) were simple web-based training, PhishGuru cartoon, Anti-Phishing Phil game, and a combination of Anti-Phsihing Phil plus a PhishGuru cartoon. The web-based training involved asking participants to read three links from the first page of Google search with the search query 'phishing'. For the Anti-Phishing Phil game, participants were asked to complete three levels of the game and were allowed to exit at any

point. The PhishGuru training was simply looking at one page of materials, which took participants an average of 0.5 minutes. To measure the effectiveness of the training, participants participated in a role-play task with two equivalent exercises administered before and after training. The research found that, "Anti-Phishing Phil, the PhishGuru cartoon and Anti Phishing Phil with the PhishGuru cartoon did not decrease participants' tendency to click on legitimate links and go to legitimate websites" and that all various educational materials performed similarly in reducing participants' susceptibility to fall for phishing (Sheng et al., 2010). The findings suggest that educational material including using the Interactive gaming approach may be an effective tool to enhance employees' security awareness. Interactive gaming in particular, is much better at making sure employees' don't identify legitimate links as phishing, unlike the basic web-based reading used in the research, which slightly reduced participant's tendency to click on legitimate links.

CJ et al. (2018) took a similar approach to Kumaraguru et al. (2010) where they designed a game called Phishy. Phishy is a game where a character lost in the seas has to overcome challenges in order to reach the shore, with imminent dangers prevalent at all times. Before the game starts, a comic format story is displayed to the player where a person called Sam, lured by the money award that a phishing email said he had won decided to click on the link on the email and provide his bank details. It was too late from him to realize that he was a victim of a phishing attempt and that criminals have taken all his money and left him on a boat with a hungry tiger in the middle of the sea. Sam needs to get back to the shore. In order to do so, he must hook up fishes to his snare and then answer a question whether a certain URL is a phishing attempt. False positives and false negatives result in deduction of points and the Tiger getting closer to Sam. However, a true positive or true negative will reward Sam points and the hungry

tiger will eat the fish. The game has three different levels, each level dedicated to certain types of URLs. After completion, a brief summary of all the questions from that level is shown. Before and after the game, players are asked a set of questions via a Survey. The player must answer the pre-game survey in order to continue in the game. When the game ends, a similar set of questions follow and the responses are analyzed to evaluate their performance. The game was successfully completed by 8071 associates within a month. The game data of associates who completed the game showed significant improvement in identifying phishing links. Furthermore, from the feedback it looks like players truly enjoyed the game, some even playing it more than once.

Group-Oriented Delivery Method

Another advanced delivery method is the group-oriented delivery method. The focus of the delivery method is to build a security culture where employees feel confident to share security risks with each other and benefit from each other's experiences. The training is usually focused on collective teams putting their minds together to tackle cyber security issues through dialogue, open-ended questions, group reflections, etc (Albrechtsen & Hovden, 2009). The importance of organizations having an information security culture is mentioned in Flores & Ekstedt (2016). Chow & Chan (2008) define organizational culture to be, "related to employees' perception of shared beliefs and values among employees in the work environment, and points out the quality (e.g., richness and friendliness) of social relationships at the workplace" (as cited in Flores & Ekstedt, 2016). According to Chang & Lin (2007), organizational culture in an information security setting is "significantly influenc[ing] information security measures (confidentiality, availability, and accountability)" (as cited in Flores & Ekstedt, 2016). Thus Flores & Ekstedt (2016) finds it to be a logical deduction to believe that fostering an information

security culture in the context of SE, could have a direct association with an employee's information security awareness, attitude, and beliefs about security threats.

In the research, they proposed three hypotheses related to the role of information security culture. The first hypothesis is that an organization's information security culture is positively associated with an employee's information security awareness. The second hypothesis is that an organization's information security culture is positively associated with an employee's attitude toward resisting SE; finally, information security culture in an organization is positively associated with an employee's normative beliefs about resisting SE (Flores & Ekstedt, 2016). They sent out a survey to 4296 employees (37% responded), between January 2013 and October 2013, from organizations operating in a variety of industries and found that the three hypotheses are statistically likely ($p < 0.01$). This means that all three hypotheses are supported by the data at a very high statistical significance rate. Thus, it is important for companies to integrate a positive information security culture to raise the awareness of employees in information security and resisting SE.

A great way for companies and organizations to build a positive information security culture is through an intervention similar to the one conducted by Albrechtsen & Hovden (2009). In the intervention, they created six small-sized workshops (15-20 participants each with about 100 participants total) aimed at improving the behavior and awareness of employees on cyber security issues. The workshop took place at a Norwegian public administration agency where they randomly placed 197 employees into an intervention group participating in the workshop and a control group not participating in the workshop.

The idea behind the workshop is not to be one-way communication but rather a forum of discussion where participants do most of the talking and create reflections. The security officer

would ask a simple question like 'Why do we need information security?' and the participants collectively answer the question. The participants of each workshop were divided into seven groups of 2-3 persons sitting next to each other and each group was given a different scenario that they tried together to come up with a way to deal with the scenario in a secure manner. After the scenarios, each group of participants presented how they dealt with the scenario and the other groups commented on the way the group handled it. They evaluated the effectiveness of the workshop in changing behavior by designing three surveys: one to be filled before the workshop, and two after the workshop. The first survey was performed one month before the intervention and the other two surveys were performed 1 month and six months after the intervention. Their statistical analysis revealed that the intervention was capable of changing a broad range of awareness and behaviors, while the control group showed no significant changes (Albrechtsen & Hovden, 2009).

Group discussion was even done earlier by Robila & Ragucci back in 2006 in addition to the instructor-led lecture. They followed it by a discussion of the nature of the phishing emails and the methods that can be employed by attackers to generate better-targeted messages as well as identify many browsers and web vulnerabilities. Next, it involved a discussion of ways to increase public awareness of phishing and fostered debates on aggressive vs. passive education. Creating an ISAT program that involves employees' input is a great way for them to have a stake in the security of their organizations.

Simulated Attack Delivery Method

Perhaps the most realistic method is the simulated attacks delivery approach. It involves performing simulated attacks through the usage of fake emails designed by the organization sponsoring the training to try to trick their employees into clicking links or downloading

attachments in the emails. Alternatively, organizations can request the assistance of an external specialized company to conduct phishing or SE attacks on their employees. This approach was suggested by Valentine (2006) to be used in the third phase after assessment and identification—that is the education phase. The idea would be to have a scenario-based training where employees are placed in test situations involving potential attacks. For example, it could be a SE attempt for employees with access to the company's server room. The idea would be to use the results from the attack to educate employees on areas directly affecting their work—that is, it is relevant to them. This is exactly what the United States Military Academy (USMA) did back in 2007.

Dodge et al. (2007) discuss the USMA unannounced simulated security exercises. In the exercise, participants are not aware of the simulated attack. The trainers would surprise them by sending unannounced phishing emails. Some of the important considerations the research took into account were making sure that when they send those emails they dissociate them from IT and that they involve legal staff. They decided to dissociate the emails from IT so that the trust between the IT staff and the participants, students at USMA, is not compromised. In addition, they recommended the involvement of legal staff as they "can provide opinions and guidance on human subject research requirement and assessment on personal privacy" (Dodge et al., 2007). In their simulated email attacks, they had different types of emails. The first type of emails was one that uses an embedded link to see if users would actually click it. The second type of emails was attachment email where the participants are tricked into opening an attachment. The third type was sensitive information emails, which measures participants' susceptibility to fall for SE and disclose sensitive information. The fourth and final type of email is one where the participants would be tricked into downloading an application or an executable. The results show

that the failure rate of an embedded link, attachment, and sensitive information were all high. Participants clicked on those links even though they admitted it looked odd. The one that had the most failures was the attachment type emails. Through the results, USMA were able to determine that when they conduct ISAT, they should focus on the danger of opening unknown attachments. Having sporadic and unannounced simulated attacks offer a safe environment to assess the elements that should be further stressed in future ISATs.

In Jagetic et al. (2007), they went with a realistic simulated phishing email approach where they actually "harvested freely available acquaintance data by crawling social network [websites]", building "a database with tens of thousands of relationships", and then cross-correlating the data with Indiana University's address book database to find students who could be used in the research. They then selected students ages 18-24 based on the "amount and quality of publicly available information they disclosed about themselves" (Jagetic et al., 2007) and used them in the study where they targeted the participants with phishing emails that were personalized to them. "A total of 1,731 participants were included in the study—921 subjects received phishing attacks and 810 had their email addresses spoofed" (Jagetic et al., 2007). The research here raises awareness about the weakness of humans regarding their willingness to share information about themselves publicly without stopping to think of the consequences.

The intent of the experiment was to "quantify, in an ethical manner, how reliable social context would increase the success of phishing attacks" (Jagetic et al., 2007). The control group in the experiment received an email but without the social context. The experiment found 16% success rate (defined as people falling for the phishing attempt) among the control group, which they attributed to the fact that there is a "subtle context associated with the fictitious sender's email address and the university domain name identified in the phishing hyperlink" (Jagetic et

al., 2007). The experimental group success rate was at 72%, which was higher than what they had anticipated. Some students continued visiting the phishing link after providing their university credential as they bought the message that is displayed upon successful sign-in, which would say that the server is busy, and ask them to try later. It was concluded based on the results that having a social context leads people to overlook important clues that could have given away that the link is not legitimate and thus they become vulnerable.

Other noteworthy results were that they found "females [to be] more likely to become victims [of phishing attacks] (77% versus 65% for males). Furthermore, the attack was more successful if the spoofed message appeared to be sent by a person of the opposite gender. This was true for both males and females, but the effect was more marked for males (68% if the message was from a female versus 53% if from another male)" (Jagetic et al., 2007). The research shows that simulated attack approach with social-context is highly effective and dangerous and thus companies implementing such methods would be able, in a realistic way, to tap into their employees' weakness and find strategies to mitigate such risks before a real malicious actor exploits those social weaknesses.

Kumaraguru et al. (2007) offer a way to use the embedded training email system to educate users rather than just serving as a test for the susceptibility of employees—like done by Jagetic et al. (2007) and Valentine (2006). The idea is to periodically send users simulated phishing emails, perhaps from their system administrator or from a training company, and educating them if they fall for the emails. Users would access these training emails in their inbox while they are checking their regular emails. These training emails are designed to look just like phishing emails, urging people to go to some website and log in. If people fall for the training email (that is, they click on a link in that email), they are provided an intervention message that

explains that they are at risk for phishing attacks and are given some tips to protect themselves (Kumaraguru et al., 2010). In a previous study, they have shown that users improved their ability to identify phishing emails directly after the training. Thus in this study, they are seeking to measure how well participants retain the information they learn through the training and how they will apply the knowledge to other emails.

They proposed five hypotheses of which four were supported. The first supported hypothesis was that "users learn more effectively when training materials are presented after they fall for a phishing attack (embedded) than when the training materials are sent by email (non-embedded)" (Kumaraguru et al. 2007; Kumaraguru et al. 2010). The second supported hypothesis is that "users retain more knowledge about how to avoid phishing attacks when trained with embedded training than with non-embedded training" (Kumaraguru et al. 2007; Kumaraguru et al. 2010). The third supported hypothesis is that "users transfer more knowledge about how to avoid phishing attacks when trained with embedded training than with non-embedded training" (Kumaraguru et al. 2007; Kumaraguru et al. 2010). The final supported hypothesis is that "confronted with a novel situation, those with higher scores on the CRT will be more likely than users with lower scores to click on the links in the phishing emails from companies with which they have no account" (Kumaraguru et al. 2007). CRT stands for Cognitive Reflection Test and it is a three questions test that in order to be answered correctly requires the test taker to suppress their impulsivity. Fredrick (2005), the designer of CRT, argues that it measures "the ability or disposition to resist reporting the response that first comes to mind" (as cited in Kumaraguru et al. 2007). Fredrick found that "higher CRT scores correlate with more risk-taking" (Kumaraguru et al. 2007).

To test their hypotheses in the study, they analyzed data for 42 participants randomly assigned to one of three conditions. First, an “embedded” condition in which participants were shown the training material when they clicked on links in the simulated phishing emails. Second is a “non-embedded” condition in which participants were shown training materials in an email message and the third is a “control” condition in which participants did not receive any training materials but received an additional email from a friend (Kumaraguru et al. 2007). The results found that users who were in the "embedded" condition learn more effectively when the training materials are presented after users fall for the attack and that they tend to make better decisions than those in the "non- embedded" condition. In fact, they found that users in the "non-embedded condition did not perform significantly better after training than those in the control condition (who had received no training)" (Kumaraguru et al. 2007). Participants in the "embedded" condition spent time reading the material presented to them after falling for the attack than those in the "non-embedded" condition and they were able to retain and transfer more knowledge than the "non-embedded" condition. The finding suggests that when people are given a reason that motivates them to read the training materials, they will read it. It looks like falling for a simulated attack is an effective way to tell the users that they have a problem and that they need to be trained. The research has also found that people in the "embedded" condition, when tested after seven days, retained the information and they were able to transfer their knowledge to other types of phishing emails (Kumaraguru et al. 2007).

In 2009, Kumaraguru et al. expanded their previous work by testing the effectiveness of the embedded-training system (PhishGuru) using a real-world study of 515 participants in order to measure long-term retention and the effect of two training messages. Simulated emails sent through the PhishGuru training system are more than just a mechanism of training delivery, "but

also a test of whether the recipient has learned how to distinguish legitimate from phishing messages" (Kumaraguru et al., 2009). "A real deployment of the system would not only train users but also assess their performance at regular intervals" (Kumaraguru et al., 2009). This approach offers a great way for companies to "identify and present training interventions only to those users who continue to fall for the simulated phishing attacks. In addition, this approach can be used to introduce recipients to new phishing threats over time and focus on those recipients who are most susceptible to the new threats" (Kumaraguru et al., 2009).

The 515 participants were randomly assigned to one of three conditions: "control", "one-train" (one message), and "two-train" (two messages). There were 172 participants in both the control and the one-train groups and 171 participants in the "two-train". All participants received three legitimate and seven simulated spear-phishing emails over the course of 28 days. The researchers had three hypotheses. First, " participants in the training conditions (one-train and two-train) identify phishing emails better than those in the control condition on every day except day 0" (Kumaraguru et al., 2009). Second, "participants who see the training interventions twice perform better than participants who see the intervention once" (Kumaraguru et al., 2009). Finally, "when asked to identify legitimate emails participants who view the training materials in the training conditions will perform the same as participants in the control condition" (Kumaraguru et al., 2009).

In Kumaraguru et al. (2009) they have found that participants who trained with PhishGuru retained knowledge for 28 days, more than the 2007 research where they have proven that information was retained after seven days from the training. They have also found that adding a second training message for people who fall for the phishing email decreased the likelihood of people providing their information to phishing websites. Furthermore, the training

did not decrease people's willingness to click on links in legitimate messages. The results suggest that simulated emails offer a great delivery method for training and one that will not discourage people from clicking on a legitimate link. The research shows that people will be more likely to focus on the training when they see that they have an issue—that is they were tricked into providing their sensitive information.

Discussion of Findings

Review of the literature for the past twenty years shows that major work has been done around the world to mitigate the risk to information security from the employees who depend on it and in some cases even those who are tasked with protecting it. Despite all these efforts, the 2019 State of the Phish Report indicates, "in general, end users are not familiar with commonly used [InfoSec] terms. In addition — and of particular concern — many are relying on IT teams to automatically discover and fix accidental downloads of malicious software. The lack of clarity with regard to the role of IT in attack prevention could be giving users a false sense of security and unnecessarily taxing [InfoSec] resources" (Proofpoint, 2019). Proofpoint determined that this is the case by asking "five relatively simple, multiple-choice questions of 7,000 end users across seven countries (the US, UK, France, Germany, Italy, Australia, and Japan). All questions focused on fundamental [cyber security] concepts, including high-profile topics (like phishing and ransomware), and lesser-known but frequently experienced attacks like smishing (SMS/text message phishing) and vishing (voice phishing)" (Proofpoint, 2019). In the report, they also highlighted average failure rate for multiple industries were ranging between 16% failure rate at the high end and 6% at the low end. As for average failure by department, they found that the highest were: (1) Commercial (19%); (2) Purchasing (14%); (3) Communication and Sales (13%); (4) Maintenance and Security (12%); (5) Executives, Legal, Marketing, Procurement and Treasury (11%). The alarming part of the report is that some of the departments keeping sensitive data are at the top of the list.

There are two reasons that could explain why this is still an issue to date. First, it could be that ISAT designer and trainers for companies, if exist, are not aware of this literature. Second, it could be that the designer and trainers are aware of the literature and that tools are available out

there that addresses many of the elements in the literature review, but companies are not invested in it. Proofpoint (2019) dedicates a great portion of their report to the helpfulness of mature phishing awareness training in combating SE. The report claims that they "observed a 9% average failure rate across all simulated phishing campaign styles and all industries" and that "it held steady from 2017, a good sign that end users continue to apply learned skills and remain alert to different phishing lures and traps" (Proofpoint, 2019).

All these results show that ISAT quality is inadequate, but training is progressively becoming more effective as companies invest more time on it and take it seriously. Proof Point report data "shows a terrific trend for organizations that are committed to longer-term security awareness and training initiatives: Average failure rates fall steadily as programs continue, with the biggest gains happening in programs that have been running for at least a year" (Proofpoint, 2019). Here are some recommendations based on the results obtained from the literature review. The first recommendation is that all companies should invest in having some form of ISAT as much as they invest in security hardware. They should also be patient with it, as it will not work magically the first time it is applied. ISAT quality improves as it increases in maturity. The second recommendation is for companies to know which types of employees are vulnerable to which type of attacks and how cybercriminals are targeting those specific job functions. "When organizations can identify their 'Very Attacked People (VAPs),' they can then test specific departments and individuals, isolate potential vulnerabilities, and deliver targeted security awareness training assignments to improve knowledge and reduce risk" (Proofpoint, 2019). This becomes especially important in the early planning stages of an ISAT program, when modifying a purchased package, or as the program is being refined. The third recommendation is that companies already implementing ISAT should continue developing their programs by finding

new attack vectors and applying continuous refinement as the threat intelligence landscape changes. The fourth recommendation is for the training to involve a combination of the delivery methods discussed in the literature review and be a year-round rather than just one-and-done compliance check task. The fifth recommendation is for companies to evaluate multiple packages available and think of ways they can modify them to fit their organizations' needs rather than starting from scratch. The exact combination of design and delivery method is up for each company to decide based on experiments. Eventually, they will find something that works for them and that is effective.

Conclusion

Phishing is one of the most prevalent methods used by adversaries to target companies and organizations as it takes advantage of common human weaknesses to conduct successful attacks with minimal technical efforts. The best defense against such prevalent practice is using ISAT programs. However, implementing a successful ISAT program is complicated and involves multiple considerations and design decisions. In addition, convincing companies and employees of its importance is an arduous task mainly because of the existence of many ineffective examples. In order to fix ISAT shortcomings, the literature recommends spending ample amount of time upfront designing the program and tailoring it to companies' needs and employees' needs. Once a decision has been made on content, as well as which employees will receive which training, companies may elect to choose one or more of four delivery methods. Those delivery methods could be lecture-based, program/interactive games, group-oriented, or simulated attacks. Each of the delivery methods has its own time and place in order to be most effective. Organizations and companies should figure out for themselves what combination to use and when, and make sure that their training continues in year round basis. As companies go through multiple trial and errors, their ISAT program will mature. The more mature the ISAT program is, the more effective it will be in changing people's behavior and companies will start seeing a huge return on investment. The research has shown that while employees continue to fall for SE attacks going to 2019, there have been noticeable improvements due to the effectiveness of ISAT programs. Thus, the take home point from this research is that ISAT programs can be effective in changing behavior and securing the companies human assets if they were taken seriously and given priority like any other security mechanism.

References

Albrechtsen, E., & Hovden, J. (2009). Improving information security awareness and behaviour through dialogue, participation and collective reflection. Computer & Security, 29(4), 432-445.

Butler, R. (2007). A framework of anti-phishing measures aimed at protecting the online consumer's identity. The Electronic Library, 25(5), 517-533

Caldwell, T. (2016). Making security awareness training work. Computer Fraud & Security, 2016(6), 8-14.

CJ, G., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V., & Lodha, S. (2018). PHISHY - A serious game to train enterprise users on phishing awareness. CHI PLAY '18 Extended Abstracts Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts, 169-181.

Cooper, M. H. (2008). Information security training: lessons learned along the trail. Proceedings of the 36th Annual ACM SIGUCCS Fall Conference: Moving Mountains, Blazing Trails, 207-212.

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. Computer & Security, 26(2007), 73-80.

Dominguez, C. M., Ramaswamy, M., Martinez, E. M., & Cleal, M. G. (2010). A framework for information security awareness programs. Issues in Information Systems, 11(1), 402-409.

European Network and Information Security Agency (ENISA). (2006). A user's guide: how to raise information security awareness (Rep.).

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computer & Security, 59, 26-44.

Frauenstein, E. D., & Solms, R. V. (2009). Phishing: how an organization can protect itself. Proceedings of ISSA 2009, 253-268.

Furnell, S. & Clarke, C. (2012). Power to the people? the evolving recognition of human aspects of security. Computer & Security, 31(8), 983-988.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. J Supercomput, 74, 4986-5002.

IBM Global Technology Services. (2014). Cyber security intelligence index: analysis of cyber attack and incident data from IBM's worldwide security operations 2014 (Rep.).

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social Phishing. Communications of the ACM, 50(10), 94-100.

Ki-Aries, D., & Faily, S. (2017). Persona-centered information security awareness. Computer & Security, 70, 663-674.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., Pham, T. (2007). School of phish: a real-word evaluation of anti-phishing training. SOUPS '09 Proceedings of the 5th Symposium on Usable Privacy and Security, 13 pages.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Protecting people from phishing: the design and evaluation of an embedded training email system. Institute for Software Research, 905-914.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny Not to Fall for Phish. ACM Trans. Intern. Tech, 10(2), 31 pages.

Lungu, I., & , Tăbuşcă, A. (2010). Optimizing anti-phishing solutions based on user awareness, education and the use of the latest web security solutions . Informatica Economică, 14(2), 27-36.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., & Butavicius, M. (2016). Individual differences and Information Security Awareness. Computers in Human Behavior, 69, 151-156.

McCoy, C., & Fowler, R. T. (2004). You are the key to security: establishing a successful security awareness program. Proceedings of the 32nd Annual ACM SIGUCCS Conference on User Services, 346-349.

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. Journal of Internet Commerce, 9(1), 23-41.

Ohaya, C. (2006). Managing phishing threats in an organization. Proceedings of the 3rd annual conference on Information security curriculum development, 159-161.

Ög˘ütçü, G., Testik, O. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. Computer & Security, 56(2016), 83-93.

Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. Information Technology Education, 177-181.

Pricewaterhouse Coopers (PWC). (2015). Turnaround and transformation in cybersecurity: Key findings from the global state of information security survey 2016 (Rep.).

Proofpoint. (2019). State of the phish 2019 Report (Rep.).

Purkait, S. (2012). Phishing counter measures and their effectiveness – literature review. Information Management & Computer Security, 20(5), 382-420.

Robila, S. A., Ragucci, J. W. (2006). Don't be a phish: steps in user education. Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education, 237-241.

Schultz, E. E., Proctor, R. W., Lien M., & Salvendy G. (2001). Usability and security an appraisal of usability issues in information security methods. Computer & Security, 20(7), 620-634.

Scott D. (2009). Social engineering: hacking the wetware!. Information Security Journal: A Global Perspective, 18(1), 40-46.

Shaw, R. S., Chen, C. C., Harris, A. A., & Huang, H. J. (2008). The impact of information richness on information security awareness training effectiveness. Computer & Education, 52(1), 92-100.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs J. (2010). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 373-382.

Shropshire, J., Warkentin, M., & Sharma, S. (2014). Personality, attitudes, and intentions: predicting initial adoption of information security behavior. Computer & Security, 49(2015), 177-191.

Valentine, J. A. (2006). Enhancing the employee security awareness model. Computer Fraud & Security, 2006(6), 17-19.

Whitman M. (2003). Enemy at the gates: threats to information security. Communication of the ACM, 46(8), 91-95.