EXECUTIVE SECURITY AWARENESS PRIMER

by

Gregory W. Toussaint

A Capstone Project Submitted to the Faculty of

Utica College

April 2015

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Cybersecurity

ABSTRACT

The purpose of this paper was to create a primer for a security awareness program to educate senior level executives on the key aspects of cyber security. This is due to the gap area that was discovered in the lack of both executive security awareness programs, and the lack of executives that fully abide by their company's security policies. This, coupled with research showing that executives are highly targeted by attackers, was the impetus behind this project. It was determined that the content of an executive security awareness program should be similar to that of a security awareness program for all other employees, with the differences being in the delivery and time frame of each segment. Due to this, literature was reviewed on the various topics of security awareness. Research revealed the importance of capturing an executive's attention, in order to keep their interest in the program. It was recommended that individuals charged with creating an executive security awareness program begin by having one on one meetings with the executives in their company. These meetings will help assess the time constraints of their company executives as well as their current knowledge of the various security awareness topics. This will help with tailoring the program specifically to their company executives. This primer may be used by any company or organization in the beginning stages of creating their own security awareness program for executives. Keywords: Cybersecurity, Professor Albert Orbinati, Executive Security Awareness, Internet Safety.

ACKNOWLEDGEMENTS

I would be remiss if I did not thank a handful of people for their support and guidance along this process of completing such a large undertaking of obtaining my master's degree. First, and most importantly, I am thankful for the support I received from my wife Brenda. Throughout this process you dealt with me not only spending time on my coursework, but also at my two jobs, all while caring for our beautiful baby girl, Lily. Speaking of Lily, you are too young to understand this right now, but you were amazing throughout this as well. I was terrified that I was going to be doing all of this while having sleepless nights, but you decided to be an amazing baby and slept for 11 hours, all night, every night. Just because I am done though does not mean I am ready for the sleeping habits to change! In regards to the rest of my family and my in-laws, I received nothing but support and words of encouragement. You helped push me along, and I am grateful. Mom, you are the kindest and gentlest person I know, and you helped get me through the tough times. To my sister and brother-in-law, Michelle and Jamie, you two are an inspiration to me. You are extremely busy people, but still manage to pull it all together and are amazing parents with a wonderful family. I also could not have done this without the guidance of my capstone professor, Albert Orbinati. Your constructive criticism was spot on, and really helped me become a better writer. I would like to give a big thanks to my second reader, Phil King, and my third reader, Leslie Corbo. Not only were both of you willing to take the time to help, you were eager to do so. This really meant a lot to me. I'd also like to thank Vern McCandlish. Vern, you gave me a great deal of guidance. Not only throughout the master's program, but also in life. Lastly, I want to thank my father. Dad, although your guidance is now sent from above, I can still hear your words of wisdom and encouragement every day. You are the most amazing person I have ever known, and I am so proud when people tell me I am just like my father.

TABLE OF CONTENTS

LIST OF ILLUSTRATIVE MATERIALS

STATEMENT OF THE PROBLEM

Definition of the Problem

The news routinely runs stories about senior level executives from various companies and organizations that have been targeted in cyber-attacks. Some of the more recent headlines read, “Hackers target ‘top pharmaceutical executives' to gain trading advantage” (Sparkes, 2014), “Executives Targeted in 'Darkhotel' Attacks - Industry Reactions”(Kovacs, 2014), and “Research Exposes Attacks on Military, Diplomats, Executives” (Roberts, 2015). In order to help determine why this may be, some recent incidents will be reviewed below.

Incident review 1: Business email compromise. The Internet Crime Complaint Center (IC3) is a joint organization between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). Recently, IC3 released information on a type of attack which is becoming increasingly prevalent. IC3 calls this attack the *Business Email Compromise* (BEC) (Internet Crime Complaint Center, 2015). In this attack, high level executives like Chief Financial Officers (CFOs) are being targeted, and in some cases their email accounts are being compromised. The compromised email account is then used to send a phishing email to other executives in the financial department in order to request a wire transfer of funds to a specific bank account. The bank account belongs to the attackers, who are motivated by the financial gain (Internet Crime Complaint Center, 2015). Since the email either specifically originated from the executive’s email account, or is spoofed to appear to come from the executive’s email account, it appears credible to the recipient. This makes the recipient more likely to believe that the email is legitimate. This is especially true in today’s world where many company employees do a large amount of their communicating through electronic means. In just over a one year time period, from October 1, 2013 through December 1, 2014, there have been a total of 1,198 known victims

from this type of attack in the United States alone, totaling $179,755,367.08 in losses. The combined losses worldwide totaled $214,972,503.30 (Internet Crime Complaint Center, 2015). This does not even account for those who have not yet identified the loss, or have decided not report it. In this case, it is clear that the reason the executives are being targeted is due to their ability to transfer large amounts of funds outside of the organization. The typical employee would not have the ability to do this.

Incident review 2: FIN4. *FireEye*, a large security company specializing in cyber intelligence and incident response, released a report in 2014 about the threat group FIN4. This report highlights FireEye's investigation and analysis into recent cyber-attacks conducted by FIN4. To summarize the activity of this group, they have been recently targeting senior level executives of publically traded companies in an attempt to gather insider information that could be used to gain an advantage in the stock market. The information they have been known to target is non-public, including information on mergers and acquisitions. They have used numerous means to target these executives, including various forms of social engineering and phishing. The threat group FIN4 has targeted over 100 organizations since the middle of 2013 (Vengerik, Dennesen, Berry, & Wrolstad, 2014). In this case, it appears that the reason executives are being targeted by FIN4 is due to their firsthand knowledge of mergers, acquisitions, and other insider information that could be used for buying and selling stocks. This differs from the case above where executives were being targeted for what they can do, rather than what they know.

Incident review 3: hotel Wi-Fi. In November, 2014, NBC News reported that business executives were being targeted while on travel, through the use of hotel Wi-Fi. The attackers discovered a way to push malware to computer systems connected to a hotel Wi-Fi. The malware

was designed to place a backdoor on the computer, allowing the attackers full access to the infected system. This also allows the attackers to implement a key-logger in order to capture everything typed on the system, including information such as credentials. This information is then used by the attackers to gain entry into their main target, which is the executive's company network. Per the NBC article, the security company Kaspersky predicted that there may have been thousands of compromises by attackers since 2008, spanning across hundreds of hotels (Kharpal, 2014). It is not as clear with this attack why the executives were targeted, although an argument could be made that they were targeted for both what they know and what they can do. Regardless of the attackers' intent, acquiring an executive's credentials can help the attackers achieve their ultimate goal, whether it is to steal data, money, or even cause a denial of service or destruction. Just having the ability to send email from the executives account alone can be a powerful capability.

Executive security awareness. There is one common factor between all of the above cases that could have helped prevent the attacks from being successful, and that is the targeted executives having a strong *awareness* of the various cyber-attacks, and an understanding of how to prevent and detect them. This knowledge could be gained through an executive security awareness program. It is important for all individuals to receive security awareness training, regardless of their job title, but unfortunately many senior level executives may not find the time to participate in their organization's security awareness program. Many executives also appear to be exempt from abiding by their organization's security policies. Kevin Beaver, the Principal Information Security Consultant and founder of Principle Logic LLC argued this point by giving the example that executives do not typically follow their organizations' security policies on mobiles devices. He stated that the reason for this was that most people did not want to attempt

to enforce the policies on their management (Beaver, 2015). There appears to be a lack of security awareness training directed towards these senior level executives. This is concerning considering that senior level executives are highly targeted, coupled with the argument that many executives do not abide by the security policies set forth by their organizations.

Most recently, the hacker group Guardians of Peace (GOP) threatened the families of Sony employees. This is the group that claimed responsibility of the politically motivated Sony hack over the release of the comedic film *The Interview* (Mandell& Weise, 2014). This clearly shows that not only are senior level executives at risk, so are their families and assistants. This indicates a need for security awareness for these individuals as well.

Project purpose. The purpose of this project is to create a primer for an executive security awareness program directed towards educating C-level employees and other executives, along with their assistants and families, on the key aspects of cyber security. This will increase the executives' own security posture as well as that of their assistants and families. This primer will be created with the understanding that there is a balance that must be found between security and business continuity. In order to accomplish this, two main questions must be addressed. Understanding the full breadth of these questions and their answers will help mold the foundation of an awareness program specifically targeted at senior level executives. These two questions are as follows, and will be the premise behind the research conducted in the literature review.

- What content should be included in an executive security awareness program?
- What are the best methods for engaging and educating executives?

Justification of the Problem

According to the 2014 Verizon Data Breach Investigations Report (DBIR), in 2009 two of the top three reported actions taken by cyber threat actors were brute force attacks and the usage of back doors. Phishing, a form of social engineering, was close to the bottom of the list at number 14 (Verizon, 2013). These top actions are specifically attacks against infrastructure. In 2013, two of the top three reported actions taken by cyber threat actors were the use of stolen credentials and phishing (Verizon, 2013). These top actions typically result from attacks against people rather than infrastructure. Note that phishing moved from a position close to the bottom of the list in 2009 up to a top position in 2013. Stolen credentials, the other action at the top of the list, are often times the result of phishing. This indicates that attackers appear to have realized that it is easier to break through a human's barrier to gather information then it is to defeat intrusion detection systems (IDS), intrusion prevention systems (IPS), and other security devices. Attackers seem to take the path of least resistance, which accounts for the change in attack techniques from 2009 to 2013.

One of the main reasons that security awareness is critical is due to the fact that attackers are targeting humans *now*, more than they ever have in the past. As previously discussed, senior level executives may not have the time to allocate towards security awareness and often times do not follow their own organizations' security policies. Due to this, senior level executives should not be trained like other employees. Tailoring a cybersecurity awareness program specifically for senior level executives may be the best way to educate them before a major incident occurs.

Deloitte conducted a study in 2014 which involved the interviewing of multiple Chief Information Security Officers (CISOs). Numerous times throughout their findings report, the study referenced that most CISOs feel that their biggest downfall in creating truly effective cyber

security programs was a lack of funding. The study specifically stated that "funding is still the #1 barrier to effective cybersecurity" ("2014 Deloitte-NASCIO", 2014, p.9). This further justifies the creation of an executive security awareness program in that executives will gain an understanding of the importance of cyber security programs, so that they may properly allocate funding.

Gaps in Current Research

As cyber-attacks become more prevalent in the news, many organizations are now conducting some type of security awareness program. This helps the weakest link, which in most cases is the human element (Schmidt, 2011). The issue is that many executives are extremely busy and may not take the time to participate in the security awareness programs that have been created (Bailey, 2015). There is plenty of research available on typical security awareness programs, and there is even some research available as to why security awareness is important for executive level employees. However, there appears to be a large gap area in the availability of research based guidelines for creating an executive security awareness program. There are various companies on the Internet that will create an awareness program and tailor it to the organization's needs, but these are premium services that come at a cost. As an example, at the time of this writing *Trustwave* currently charges $1,500.00 per year for a security awareness program for 100 users (Trustwave, 2010). For a company with only 100 employees, this may be a large annual expense. Based on Google searching for executive security awareness programs, very few of the companies that are offering security awareness as a premium are advertising anything related to an executive security awareness program. This gap area in the lack of executive security awareness training is the impetus behind the creation of this primer for a security awareness program tailored towards senior level executives.

Defining the Audience

Through showing that senior level executives are highly targeted by cyber-attacks spanning all industries from financial to defense, aerospace, and beyond, and by identifying what makes executives vulnerable and what they can do to increase their security posture, will assist in the creation of a security awareness program specifically targeted at executives. A primer for an executive security awareness program of this nature would most benefit those who are just starting to take on the task of creating a security awareness program tailored for executives. Senior level executives, their assistants, and their families will also benefit from this research and the creation of a primer for an executive security awareness program.

LITERATURE REVIEW

Introduction

The main topics and the key points contained within cyber security awareness programs are important for all employees to be aware of and understand. This includes entry level employees up through senior executives, including the CEO, President, and any other company head. As discussed in the Statement of the Problem, senior level executives are highly targeted by attackers. Therefore, one could argue that it is even more important for them to have a strong awareness of threats that exist, and how to detect and prevent them.

The purpose of this project is to create a primer for a cybersecurity awareness program targeted towards senior level executives. Since the main topics and key points of a typical security awareness program are to be included in the executive security awareness program, they will be researched and closely examined below. The main differences between a traditional security awareness program and an executive security awareness program will be the method of delivery, examples used, and timeframe in which each portion is delivered. The most effective ways to capture an executive's attention will be examined along with their typical time constraints. All of this information will specifically help tailor an awareness program for senior level executives.

Security Awareness Topics

Cell phones. Most companies and organizations worldwide are now relying on the use of cell phones to conduct business on a regular basis. These smart phones contain company email, documents, contacts, and other sensitive data. The security of these devices must be considered. The *Consumer Reports' Annual State of the Net* survey revealed that in 2013 there were approximately 3.1 million Americans that had their smart phones stolen (Consumer Reports,

2014). To prevent the data from being stolen, a password should be enabled on the phone with an auto locking function that activates when the phone has not been in use for a short period of time. Many devices have a function to wipe the phone of all data if a wrong pass code is entered a set number of times. This function is also useful to prevent brute force attempts to guess the pass code. Finally, most new cell phones have the ability to remotely wipe the phone if it becomes lost or stolen. In cases such as this, the phone may be gone but the data would be considerably more secure. Lost data is likely much more costly to a company than simply replacing a lost or stolen phone. This is shown from the results of a study conducted by the *Ponemon Institute* that revealed the following:

> On average the cost of a data breach for an organization represented in the study increased from $5.4 million to $5.9 million. The cost per record2 increased from $188 to $201. We define a record as information that identifies the natural person (individual) whose information has been compromised in a data breach (Ponemon Institute LLC, 2014, p. 2).

The importance of this becomes clear when reviewing *The Symantec Smartphone Honey Stick Project*, explained below.

Symantec (2012), a large security company, intentionally lost cell phones containing mock personal and corporate data. In this project they tracked what transpired with the smart phones once they were found by someone. The purpose of this study was to show what someone could expect if they lost their smart phone. Their key findings revealed the following:

1. 96 percent of lost smartphones were accessed by the finders of the devices
2. 89 percent of devices were accessed for personal related apps and information
3. 83 percent of devices were accessed for corporate related apps and information

4. 70 percent of devices were accessed for both business and personal related apps and information

5. 50 percent of smartphone finders contacted the owner and provided contact Information (Symantec, 2012, p. 11).

This information coupled with the results from the previously discussed *Ponemon Institute* study shows the importance of keeping corporate data contained on mobile devices secure.

Passwords. The *Verizon Data Breach Investigation Report* mentions numerous times that attackers target users' passwords (Verizon, 2014). Acquiring a user's password, regardless if they have administrator rights to a system or network, may be all an attacker needs to gain a foothold on the inside of a corporate network. Once an attacker has a user's password, a number of malicious activities may be conducted. The attacker could use the password to log into the user's email account and send malicious email. These email messages are more likely to be trusted due to it originating from the mailbox of an employee. The password could also be used to access computer systems on the corporate network. It is irrelevant if the computer system that the attacker is able to access has any valuable data, as there are multiple ways to pivot and gain access to other systems on the network. Dodd (2012) demonstrated in a whitepaper that the *Metasploit Framework* is a tool that can be used to find other systems on a network and pivot to those systems. This shows the importance of password protection. In order to protect against having passwords compromised, the following should be considered.

Length and complexity. For many years, it has been thought that the complexity of a password is most important in preventing it from being guessed or cracked, although more recent studies have shown that the password *length* is actually more important than the *complexity*. In a study conducted by Carnegie Mellon University, multiple password conditions were analyzed

and they showed that a complex password policy requiring a minimum of 8 characters, including at least one uppercase letter, one lowercase letter, one number, and one special character, contained easier to crack passwords than a basic password policy requiring a minimum of 16 characters, with no other stipulations (Kelley et al., 2012). In a whitepaper written by security company Eset, it was stated that, "Despite the IT policies that are prevalent throughout the world, really great passwords can be created that do not use upper- and lowercase letters with numbers and special characters. The really important thing is length" (Harley & Abrams, 2009, p. 11). Due to this, a password policy requiring a passphrase with a minimum of sixteen characters would be preferred over a policy requiring a complex, but shorter, password.

Two-factor authentication. In addition to passwords, a secondary form for authentication can greatly reduce the risk of an attacker gaining unauthorized access. The second form of authentication can be something that the user has, like a number generating token. The actual user can also be the second form of authentication through the use of biometrics, by scanning their retina or fingerprint. According to Valente (2009), "It has been proven that username and password alone do not provide sufficient security for sensitive information that needs more protection than other information" (p. 4). Some companies are leveraging the added security benefit of two-factor authentication, including Google. When logging into any of the various Google services, users have the option of a second form of authentication, including a pin sent by text message, audio call, or mobile app. Google also has the option of a USB key that plugs into the computer as a secondary form of authentication (Google, n.d.). Options such as these would help increase the security posture of anyone using these services.

Unique passwords. The security company *Webroot* conducted a study on password habits where they surveyed more than 2,500 individuals. Their findings showed that 35% of the people

surveyed had at least ten accounts that were password protected. Only 10% of those individuals used unique passwords for each for each of the accounts (Webroot, 2010). Using the same password for multiple accounts is a dangerous practice. If an attacker is able to compromise the password to one account, they will immediately have the password for the other accounts as well. For example, imagine that an individual uses the same password for their online banking as they do for their email account. If the individual's email account password is compromised, the attacker will also have obtained the password for the individual's online banking. For this reason, using the same password across multiple accounts should be avoided.

Storing passwords. Although using a unique password for each individual account is the best security practice, it is not the easiest. The more passwords an individual has to remember, the better their chances are of forgetting one. For this reason, individuals may be tempted to write their passwords down or store them in a document on their computer. This is a security concern. While discussing the findings of their study, *Webroot* offered the following password security tip, "In addition, don't write down passwords and store them for your own recall on a notepad or in a Word document, both of which leaves them vulnerable to prying eyes. For help, use a password management tool" (Webroot, 2010, para. 11). Password management tools can advantageous for using unique passwords for each account, but they also have their disadvantages.

Password management tools. There are various tools available to help with the storage of passwords in a more secure environment than writing them down or storing them in a word document. Some of these tools are free and some come at a cost. The premise of these tools is that an individual only has to remember one password to unlock their password database, which contains all of the passwords for each of their accounts. There are two main types of password

management tools; those that store the passwords locally on the electronic device and those that store the passwords in the cloud. Both types offer encryption in order to protect the passwords stored in the database. There are advantages and disadvantages in using either type, and there are also advantages and disadvantages in using password management tools in general.

First to be examined are password management tools in general. The obvious advantage of using these types of tools is that an individual would only have to remember one password, and would still be able to use unique passwords for each individual account. An obvious disadvantage is if attackers are able to acquire the main password for the database, along with acquiring the database itself, they would be able to access all of the other passwords contained within. A study was conducted by the University of California at Berkeley that closely reviewed some of the most popular password management software. They discovered that each one they reviewed contained vulnerabilities that could potentially allow an attacker to acquire the user's credentials (Li, He, Akhawe & Song, 2014). This of course is a disadvantage of using password management tools and could defeat the purpose of using them to begin with. When considering the use of password management tools, the risk versus the usability must be considered.

Next to be examined are password management tools that store the database in the cloud. The biggest advantage of this comes in the form of convenience. With the database in the cloud, the passwords are accessible from any device that has access to the Internet, making it easy for a user to quickly get their passwords from almost any location. The Berkeley study showed that there are concerning disadvantages of this type of password management tool as well. The study showed that there are multiple vulnerabilities to be concerned with regarding cloud based password managers (Li, He, Akhawe, Song, 2014). These vulnerabilities could allow an attacker to potentially gain access to the password database. Further, an attacker does not necessarily

have to compromise the user's computer system to access their password database, since it is stored in the cloud and not on the local system. *LastPass* is a popular password management tool that utilizes cloud storage of their users' password databases. In May of 2011 they posted information on their site stating that they identified an anomaly and discovered some data that flowed out from one of their databases. This indicated the potential of theft of some of their users' password databases. The risk was for those who did not use strong passwords for their main database, as there was the potential of brute force attacks on the stolen databases (Siegrist, 2011). Although the risk was only to those who did not have a strong master password, all users had a forced password change. This shows additional disadvantages of using cloud based password managers.

Finally to be examined are password management tools that store the database locally to the computer, phone, tablet (etc.). The advantage of having a locally stored password database is that an attacker would have to first compromise the device that the password keeper is stored on before attempting to compromise the password database and steal the passwords. Once a database is stolen though, the disadvantages are the same as previously discussed with cloud based password management tools, in that the attacker can attempt to brute force the password database. Also, if the main password to the database is known, the attacker would be able to unlock the entire database.

Companies such as LastPass appear to work diligently to close the gap on security concerns as they are identified. As an example, LastPass released a statement on their site in response to the aforementioned Berkeley study. They thanked the researchers for their work and stated that they have taken measures to address the problems identified by the research team (Gott, 2011). This indicates that as time moves forward, tools such as this are closing security

holes. The concerning part are the security risks that are not yet known about. There is a continual struggle in the balance between security and convenience.

Sharing passwords. The aforementioned *Webroot* study showed that 54% of the individuals surveyed have shared their passwords with at least one other person in the year leading up to the survey. They recommend that if a password has been shared, in order to remedy the situation, the password should be changed (Webroot, 2010). Even if an individual believes the party they are sharing their password with can be completely trusted, there are many ways that the integrity of the password can be compromised. For example, the individual receiving the shared password may not have as strong of a security posture and unbeknownst to them may have keylogging malware running on their computer. As soon as they type in the shared password into their computer, it could become compromised. Webroot stated that passwords should not even be shared with a spouse (Webroot, 2010). Some may find this difficult, but as shown above it is a key step towards increasing an individual's security posture.

Public Wi-Fi. A survey on public Wi-Fi usage was conducted by *Opinion Matters for GFI Software*. Of the 1,000 workers they surveyed, they discovered that over 95% admitted to using open, public Wi-Fi to conduct company business, including email (Kelleher, 2013). This is concerning due to ease of using software to sniff, or capture, traffic on open Wi-Fi networks. A simple Google search on how to sniff open wireless networks reveals a plethora of information and step by step guides. Being able to view this data over open Wi-Fi networks through sniffing, or packet capturing, software is a major security concern. As an example of this concern, software was released in 2010 called *Firesheep*, and was dependent on being connected to the same Wi-Fi network as the victim. Without going into the technical details, the software allowed for an attacker to essentially steal another person's web site authentication. This included social

media sites such as Facebook, meaning that an attacker that was on the same open Wi-Fi as their victim would be able to log into the victim's Facebook account without ever needing credentials (Shirriff, 2010). This shows the importance of using caution with open, public Wi-Fi. This may not only have an impact on company executives, but could have an impact on anyone connecting to open, public Wi-Fi, including an executive's family or assistants.

Email. Email is a vital part of communication in the corporate world, although it also accounts for a large number of malware infections. A study conducted by *Osterman Research* was released in January of 2013. The study revealed that 64% of organizations in the year prior to the study had malware infections on their network with the root cause being email (Osterman Research, 2014). This shows the importance of having a strong understanding of how to spot a malicious email. The following is an examination of how to do this.

One way that attackers attempt to infect their victim's computer through email is with a malicious link that, when clicked, downloads malware to the computer. Often times, the attackers will hide what the actual link is behind a fake link. In short, this simply means that the link displayed in the email may appear to be a legitimate website, but when clicked it actually opens a malicious page (Better Business Bureau, 2014). Hovering the mouse pointer over a link contained within an email, or on a website for that matter, will show where the actual link goes. Figure 1 below shows as an example of a malicious email. Note that the link appears to go to the legitimate CNN domain of www.cnn.com. Also note that the remainder of the URL was made as an example and does not actually exist.

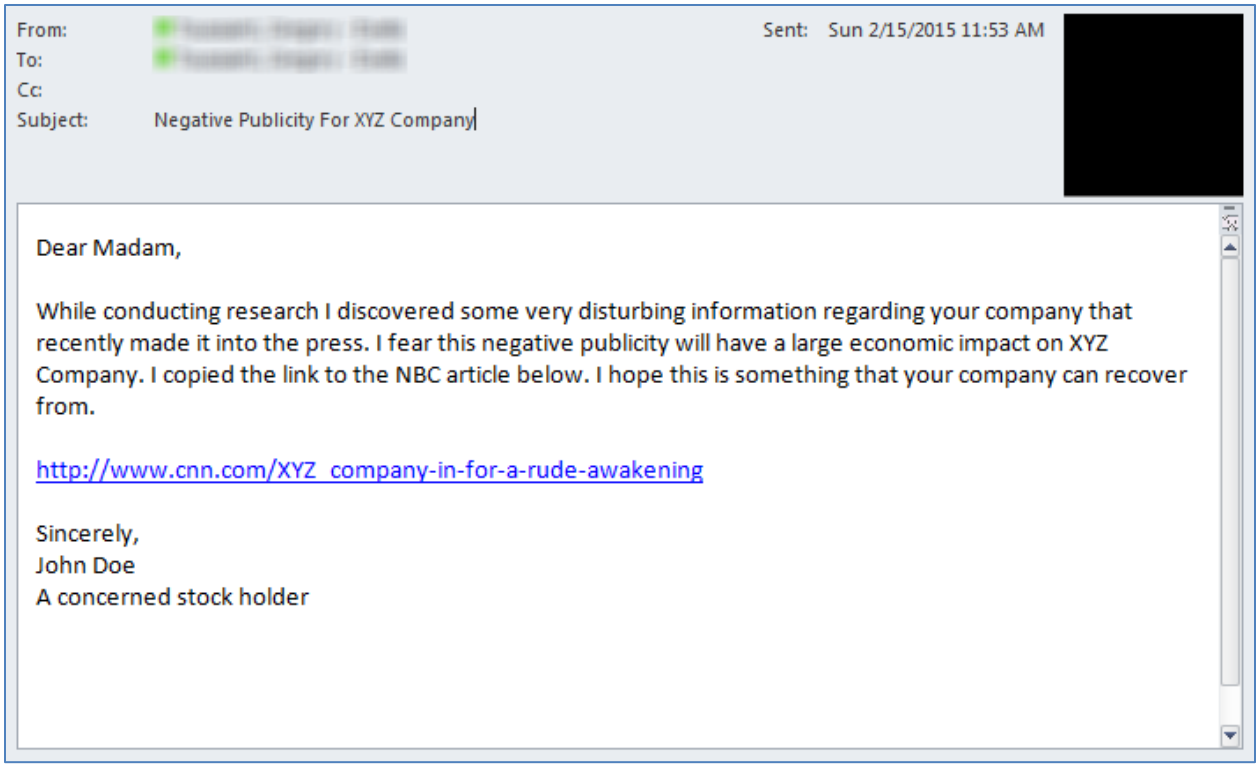

Figure 1. Example of a malicious email.

Although the link in the above example appears to go to the legitimate CNN domain, the true link is hidden below it. Figure 2 shows the same email with the mouse pointer hovering over the link. Notice the box that appears above the link shows the actual URL, which has been highlighted yellow. If the link contained within the email is clicked, it will direct the browser to the hidden link, rather than the CNN link that is displayed. Note that the underlying link has been made up for demonstration purposes and does not actually exist.

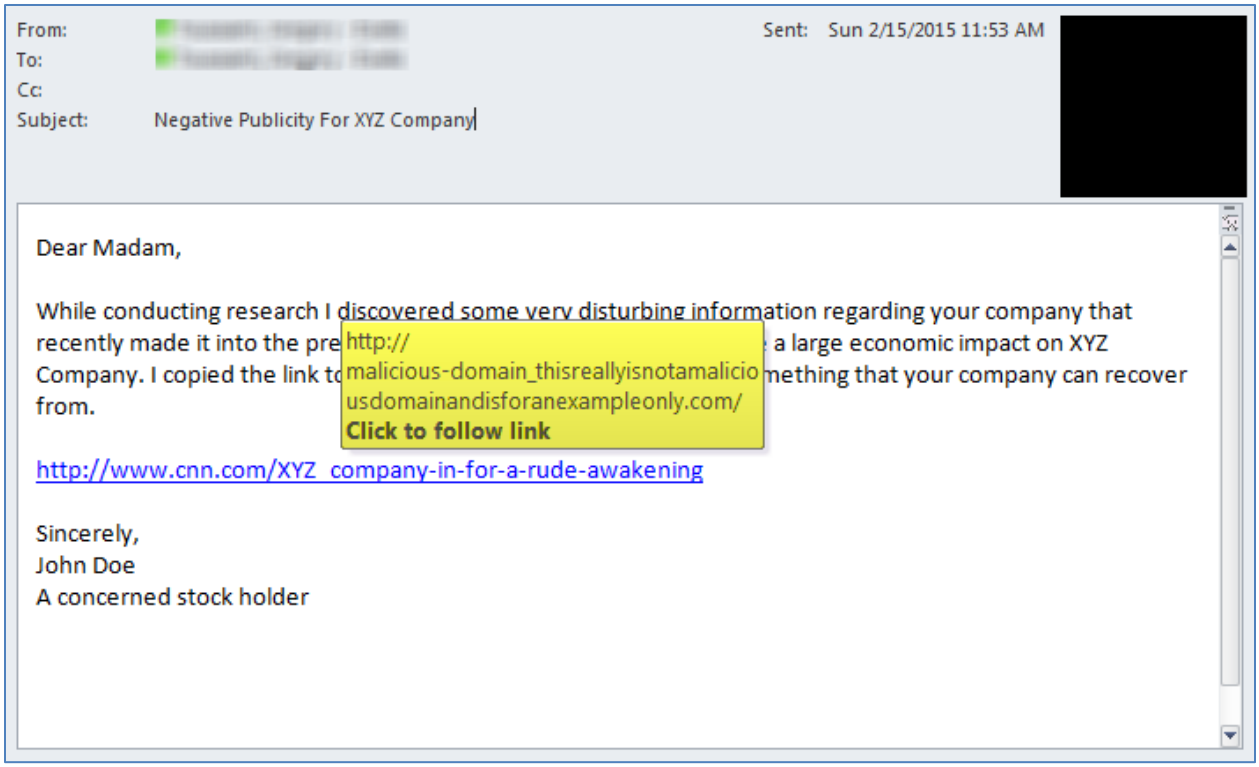

Figure 2. Example of malicious email while hovering over the apparent CNN link.

A method that can be used to detect the above activity is to set the email client to view email in plain text only. This will clearly show the underlying link directly in the body of the email, directly following the faked link. Figure 3 shows the same example email from above, viewed in plain text. Note that the malicious link is clearly seen directly after the CNN link, and has been highlighted in yellow.

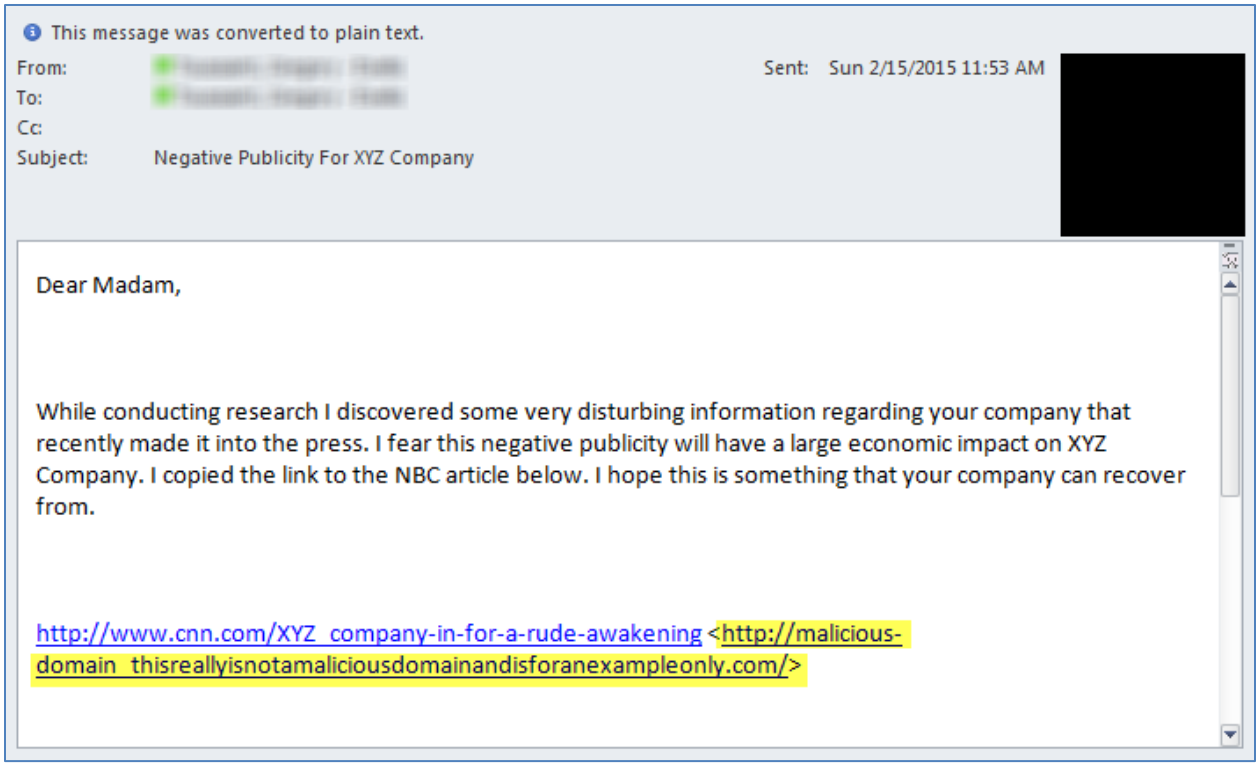

Figure 3. Example of malicious email viewed in plain text

The *University of Rochester* offered some additional tips in spotting malicious email messages in their *Security tip of Week* archives, shown below:

- There are misspelled words in the e-mail or it contains poor grammar.
- The sender's name doesn't seem related to the sender email address.
- The message is making you an offer that is too good to be true.
- The message is asking for personally identifiable information, such as credit card numbers, account numbers, passwords, PINs or Social Security Numbers.
- There are "threats" or alarming statements that create a sense of urgency. For example: "Your account will be locked until we hear from you" or "We have noticed activity on your account from a foreign IP address."
- The domain name in the message isn't the one you're used to seeing. It's usually close to the real domain name but not exact. For example:

    - Phishing website: www.regionsbanking.com
    - Real website: www.regions.com
- Beware that some phishing emails use attachments (coupons, etc) which can house malware.
- Shortened URLs can present danger. Be careful to verify all web addresses. It is safer to simply manually enter URL's into your web browser (University of Rochester, n.d., para. 14).

Although some of these indicators may exist in a malicious email, criminals are crafty and may devise an attack that does not have any of the above indicators, so vigilance is important. Shyaam Sundhar, a Senior Researcher at PhishMe, Inc. discussed that malicious emails are evolving in order to bypass security devices. Sundhar explains that this changing environment "can leave the final line of defense to an educated user, which makes it important for users to be security aware and report such incidents on time" (Sundhar, 2014, p. 8). This shows the importance of user education on identifying a malicious email. Further, it is important to submit suspicious email for analysis in a timely manner, and also to know where suspicious email should be submitted to.

Social engineering. The *United States Computer Emergency Readiness Team* (US-CERT) posted a security tip to their website regarding social engineering. They stated that, "In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems" (US-CERT, 2013, para. 1). This type of attack can occur through various means. An individual could conduct social engineering face to face with someone or through a phone call. This could also be done through email. The US-CERT's website also states that, "Phishing is a form of social engineering.

Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization" (US-CERT, 2013, para. 2). The previous malicious email example from Figure 1 falls in line with this explanation of phishing. The example email utilizes the trustworthiness of CNN in an attempt to get individuals to click on the link.

Social media. A survey conducted by the *Pew Research Center* revealed that in 2014, Facebook remained the most popular social media site with 71% of adults using it (Duggan, Ellison, Lampe, Lenhart, & Madden, 2015). This number does not account for the other social media sites on the Internet. With the majority of adults using social media, attackers could target numerous victims through this platform. Many companies use a set of security questions to assist an individual with resetting a forgotten password. These security questions often times ask for personal information. For instance, a question may ask what street the user lived on as a child, or maybe their pet's name, or their mother's maiden name. Information that individuals post on their social media accounts may give away the answers to these security questions, allowing an attacker to successfully answer the questions and obtain access to their victim's account. Further, criminals also use social media to determine when families will be on vacation, in order to burglarize their homes (Shullich, 2011). This shows the importance of locking down security settings on social media sites and only allowing close friends and family access to view the information. Taking that one step further, the best practice would be to always assume the world is able to see everything that is posted on social media, and to not post anything that everyone should be able to see. This way of thinking can also help save reputation. There are multiple news stories released regarding individuals who have gotten themselves into trouble by what they posted on their social media accounts.

Also to be considered in regards to social media is EXIF data. Johannes Ullrich of the *Internet Storm Center (ISC)* explained that EXIF data is contained within images taken by modern cell phones, and may store GPS information about where a picture was taken (Ullrich, 2010). This information could be used by criminals to determine where their victims live, go to school, work, etc. Some social media sites may strip the EXIF data from photos that are posted, but the best method in making sure that EXIF data does not get leaked is to strip the photos of their metadata before posting them online. This can be done in Windows by conducting the following, "Right-click on a picture and choose Properties, then open the Details tab and click Remove Properties and Personal Information. You have the option to strip out some or all of the attached EXIF data" (Nield, 2014, para. 4). Some basic Internet searching also reveals a large number of other programs for a variety of operating systems, which have the ability to strip metadata.

Physical security. Physical security must also be considered in a cybersecurity awareness program. As previously discussed, attackers may use social engineering tactics in an attempt to steal data. Some of these tactics may include physical attempts to steal data through various means. The following areas were discovered to fall within the topic of physical security.

***Clean desk*.** Radha Gulati discussed a scenario where a member of the janitorial staff could gather intelligence while cleaning around an employee's desk, and asks, "How many people would suspect a member of the janitorial staff could hack into the network" (Gulati, 2003, p. 5). The *CERT* division of the *Software Engineering Institute* at *Carnegie Mellon University* posted information on their site regarding various cases of insider threats. Multiple cases involved a custodial staff member as the culprit (CERT, 2011). These are interesting point as most companies and organizations have some type of cleaning crew. These cleaning crew

members are most likely seen by employees on a regular basis. Employees could become complacent around the cleaning staff, and may trust that they would not snoop around their work areas.

Disposing of information. One method that attackers may use to gather information about their target is to rummage through a company's trash that is left outside for disposal. This technique of "dumpster diving" can result in the attacker gaining some valuable knowledge about the company, which could in turn be used to craft highly targeted social engineering attacks (Houchins, 2002). It would appear that an attacker could gain extensive knowledge based on documents that an employee may not consider sensitive or of any value. For example, an employee may discard of an internal flier advertising an upcoming company social event. An attacker could use this information to craft a phishing email about the event and send it to employees, or if the event is being held in a public area, an attacker could make it a point to physically be at the public location an attempt to eaves drop on conversations.

Identification and company badges. Many organizations use badges for employees to wear while at work. These badges typically contain the employee's picture, name, and possibly access level. Some companies also utilize the badges with their door entry systems, requiring the employee to swipe their badge at a sensor to unlock the door to their workplace. The *Tennessee Office of Homeland Security* posted a security newsletter from the *Security Awareness Company* that discussed how attackers could fake an identification badge by using a camera to take a picture of an individual's badge from a distance (The Security Awareness Company, 2012). Employees that allow photographs to be taken of them while wearing their company identification badge run the risk of the photo being posted to the company web site, social media,

or other public area. This could make it easy for an attacker to simply zoom in on the identification badge and use it to replicate a fake.

Tailgating. A report created by the *Security, Resiliency & Technology (SRT) Integration Forum* stated that "Common courtesy dictates holding doors open for one another. In an access controlled environment, however, this behavior is called tailgating and allows entrants to circumvent 'badging' by not presenting authentication for entry" (Hassfield et al., 2014, p. 4). An individual who used the aforementioned technique of creating a fake company identification badge could use this method of tailgating to prevent from having to swipe the fake badge to gain entrance. The individual that the attacker is tailgating may see that the attacker has a company badge displayed, and may believe the individual truly has been allowed access. This may be more easily accomplished if the attacker intentionally has their hands full, prompting the individual they are tailgating to open and hold the door for the attacker.

Electronic device locking. A final topic to in regards to physical security deals with locking electronic devices. Many electronic devices have the functionality to lock them when they are not in use. The security company *Sophos* posted on their website that forgetting to lock the computer when stepping away from it leaves the information on the hard drive vulnerable (Prout, 2015). This concept of locking the computer is relevant for other electronic devices as well. For instance, if a cell phone has some type of access security measure activated, like a passcode or biometric scanner, and it gets lost or stolen, the attacker will be much less likely to retrieve any sensitive information off of the device.

Importance of Security Awareness

As shown in the previous discussion topics, there are many ways in which an attacker can target an organization. Many of these attacks involve targeting employees. An employee that is

not aware of the various types of attacks may not be diligent in detecting when they have been targeted. A survey was completed in 2014 by *PricewaterhouseCoopers*, and was co-sponsored by *CSO Magazine*, the *Software Engineering Institute at Carnegie Mellon*, and the *United States Secret Service*. This survey revealed the following:

> The merit of awareness programs is quite clear: 42% of respondents said security education and awareness for new employees played a role in deterring a potential criminal, among the highest of all policies and technologies used for deterrence. (Mickelberg, Pollard & Schive, 2014, p. 14)

The fact that security awareness programs helped protect the companies against potential attacks, possibly even more than policies and security devices, is a strong point outlining the sheer importance of security awareness.

Another metric from the *PricewaterhouseCoopers* survey outlined that companies that did not have security awareness training for new employees reported an average loss of $683,000 per year. The companies that did have security awareness training for new employees only reported an average loss of $162,000 per year (Mickelberg et al., 2014). This is a $521,000 difference indicating the importance of security awareness, and that it could save a company significant money.

Executive Security Awareness

As discussed previously in the Statement of the Problem, company executives are some of the most highly targeted employees. For this reason, it is important for executives to have a strong understanding of the security awareness topics reviewed above. Ernie Hayden, a former Chief Information Security Officer (CISO), stated, “I recall many discussions about the strong demands that senior management, board members and commissioners place on IT for free and

open access to their computers, unburdened by rules and policies" (Hayden, 2012, para 2). This highlights another reason behind the importance of properly educating senior level executives with security awareness. The more access an individual has, the more dangerous it can be if their device or account becomes compromised. Although, credentials to a basic account without any administrative access are also dangerous for an attacker to acquire.

In order to properly create a security awareness program targeted towards senior level executives, it will be important to have an understanding of effective methods on educating and communicating with executives. Hayden offers that the executives should be given an understanding as to why they are being targeted, and that this should include explaining actual situations where security issues arose due to the executives having elevated rights that the typical user does not have. He also explains that it is important to train any assistants the executives may have as well (Hayden, 2012). Other individuals that have a close relationship to the executives should also be given a solid understanding of security awareness. This includes family members like a spouse and children. An attacker could potentially target these individuals to get to the executive.

Hayden also mentions that it would be helpful to create a communication channel specifically for the executives to use when reporting suspicious activity, and offers that the response to these submissions must be quick or else the executives may decide to no longer submit suspicious activity (Hayden, 2012). This could be done prior to starting the executive awareness training by creating a unique email address for executive submissions and/or a specific phone number that rings in to the cyber security personnel..

In a study conducted by *Ponemon Institute LLC*, the following was stated:

> The chain of communication to the senior executive team is definitely broken. Eighty-five percent of US respondents and 89 percent of UK respondents don't meet with senior executives routinely about cybersecurity risks. The majority of the security professionals are not able to effectively articulate the security risk or demonstrate clearly that security is aligned with the goals of the business (Ponemon Institute LLC, 2013, p. 47).

This gap in communication appears to be an important one that could be one reason why there is a lack of security awareness targeted towards senior level executives.

The *Ponemon* study also showed that a large number of IT staff that does not provide security metrics to senior level executives indicated that the reason for this was because they felt that "The information is too technical to be understood by non-technical management" (Ponemon Institute LLC, 2013, p. 17). This point can also translate to a security awareness program. The information contained within the program should be non-technical, and understandable for the average non-security employee to understand. The senior executives rely on their cyber security staff to have the technical understanding so they don't have to. Executives are business oriented and not likely cyber security professionals.

The *Security Awareness Program Special Interest Group PCI Security Standards Council* published the *PCI Data Security Standard* on *Best Practices for Implementing a Security Awareness Program*. The document discusses the importance of management to have an understanding of the financial and reputational damage that could be done if cardholder data was compromised (Security Awareness Program Special Interest Group PCI Security Standards Council, 2014). This is specifically in regards to credit card information, but can translate to any industry. Using examples of other breaches that have occurred to others in the same industry, and showing what the damages were, would likely peak management's attention.

Pace Productivity conducted studies on the amount of time that various employees spend working each week. Their studies revealed that employees with the title of *President* and *Vice President* spend the most hours working each week (Pace Productivity, 2010). This is a good indication that the intended audience of an executive security awareness program are likely some of the busiest employees in a company. These executives will likely have much less time to spend on security awareness education than the typical employee.

DISCUSSION OF THE FINDINGS

Summary of Literature Review

Three main research questions were the focus of the literature review. The first question addressed was: What is required to create an executive awareness program? The second question addressed was: What is the importance of executives having an understanding of security awareness? The third question addressed was: What methods should be used in delivering a security awareness program? These three questions form the basis of creating an executive awareness program. An awareness program for executives, or anyone else for that matter, would not be possible without first having content to include in the program. This is the reasoning behind the research that was conducted on the main security awareness topics. In order gain an executive's attention when presenting the material, it would be helpful to know why it is important for executives to have an understanding of security awareness. This information, coupled with an understanding of methods that can be used to educate senior executives, ties all of the pieces together that are required to create an executives security awareness program.

An attempt was made to review research based whitepapers and articles in determining the content that should be included in a security awareness program. Multiple studies were reviewed in order to discover various trends. In some cases, news stories were reviewed in order to show current activities regarding the topics at hand. These news stories were used as corroborating evidence in furtherance of the information that was being presented by the whitepapers and studies. Information from large security companies was reviewed in order to gather another perspective from those directly involved in cyber security and security awareness.

Requirements in Creating an Executive Awareness Program

The literature that was reviewed revealed the importance of multiple key topics that should be covered when educating employees on security awareness. Many of these main topics include sub topics that could be presented in multiple training segments. It is important that these topics be covered in all security awareness programs, including programs targeted at senior level executives. A review of the research conducted on these topics and discussion of how they fit into a security awareness program is provided below.

Cell phone security awareness. The literature revealed that over three million Americans had their smart phones stolen in 2013 (Consumer Reports, 2014). This is concerning due to the amount of companies and organizations that rely on the use of cell phones on a daily basis. Many of these cell phones that were stolen not only contained personal information, but very likely contained sensitive corporate information as well. This could include information such as email messages, contact lists, documents, and more. The study conducted by Symantec (2012) revealed that "96 percent of lost smartphones were accessed by the finders of the devices" (p.11). This information, coupled with the study results from the Ponemon Institute LLC showing that a data breach could cost a company $5.9 million on average, should be enough fuel for a company to find importance in securing the data on their corporate cell phones. The following are recommendations that could assist in keeping corporate data contained on company cell phones safe:

- A locking security mechanism should be utilized on a company phone. This could be a passcode, fingerprint, pattern recognition, or any other means to unlock the phone prior to usage.

- The phone should be set up to automatically wipe all of the data on the phone if a set number of failed unlocking attempts occur.
- The phone should be set up with the ability to remotely wipe the data should it become lost or stolen.
- The phone should never be allowed to connect to an open, public Wi-Fi.

These suggestions should also be used on personal cell phones as well, in order to keep personal data safe.

Password security awareness. The literature reviewed showed that passwords are highly targeted by attackers (Verizon, 2014). Almost everyone in a corporate environment is given a username and password. Regardless of someone's ranking in a company or organization, their passwords are important to keep safe. Even if an individual does not have any sensitive information on their computer system and does not have access to any sensitive information, an attacker could still utilize the user's credentials to access other computer systems on the corporate network. This was demonstration by Dodd (2012) who showed that the *Metasploit Framework* could be used to jump to other systems on a network. Further, if an account is compromised, it could be used to send phishing email messages to other individuals. In this scenario, since the email was sent from an email account internal to the company, this would increase the likelihood that the malicious email would be trusted by the recipient. This shows the importance of password protection. In order to determine how a user can create a secure password, and properly protect it, literature was reviewed on password length and complexity, two-factor authentication, keeping unique passwords, storing passwords, and sharing password. The findings from the literature reviewed on these subjects are discussed below.

A security awareness program should include the importance of password length and complexity. The study conducted by Carnegie Mellon University showed that password length was more important than password complexity. Further, the study showed that a basic password with a minimum requirement of 16 characters was more secure than a complex password requiring a minimum of 8 characters (Kelley et al., 2012). Harley and Abrams (2009) agreed with this point in stating that password length is the important part in making a secure password. Based on the literature, the security awareness program should recommend the use of pass*phrases*, rather than pass*words*, and have a minimum of 16 characters. Microsoft's Safety and Security Centre contains a free password checker that allows a user to enter text into a field in order to check the strength of the password. The Microsoft web page states, "Microsoft does not retain information entered into this password checker. The password you enter is checked and validated on your computer. It is not sent over the Internet" (Microsoft, n.d., para. 3). The use of a password checker utility such as this is a good interactive exercise to include in a security awareness program.

Another aspect of authentication that is important to discuss in a security awareness program is two-factor authentication. The literature reveals that using two-factor authentication is much more secure than just using a password alone. Due to the security that accompanies the use of two-factor authentication, commercial companies that offer services to the general public are starting to offer two-factor authentication, including Google. A security awareness program should outline the security measures behind two-factor authentication, and should encourage users to utilize this technology where available, even with their personal, non-work relate accounts. This is especially important for the executive security awareness program due to the due to the fact that executives are highly targeted, and the information that they have access to

could be detrimental to the company if acquired by an adversary. Further, the power that an attacker gains when having access to send email from an executives account could be quite dangerous for a company.

Utilizing unique passwords for each separate account should also be stressed in a security awareness program. The Webroot (2010) study that was reviewed showed that a very low percentage of people included in the study used unique passwords for each of their accounts. When using the same password across multiple accounts, an adversary only has to compromise one password to gain access to the multiple accounts. For this reason, it is important that this topic is discussed in the security awareness program, and a recommendation be made that users use a unique password for each account that they have, both work related and personal.

A company or organization adopting an executive security awareness program may want to include information on password management tools. There are advantages and disadvantages of using password management tools in general. There are also advantages and disadvantages of using cloud based password management tools versus those local to the computer, phone, or other device. These advantages and disadvantages outlined in the literature review should be considered by a company or organization prior to making any recommendations in a security awareness program. This is because each individual company or organization must first accept the risk before encouraging users to utilize these types of tools. Further, prior to adding any of this information into a security awareness program, the company's policies should first be reviewed to determine what password management tools, if any, are allowed.

The final topic on passwords is important to include in all security awareness programs. This is the topic of password sharing. The Webroot (2010) study that was reviewed showed that 54% of the individuals in the study shared their passwords with someone else. They offer that

passwords should not be shared with anyone, including a spouse. This 54% is an alarming number, because once the password has been shared, the security of that password is out of the account owner's control. Based on the literature reviewed, it is recommended that a security awareness program include that passwords should not be shared with anyone for any reason.

Public Wi-Fi security awareness. The literature reviewed revealed that a large number of people connect to open, public Wi-Fi. These individuals admitted to using the public Wi-Fi to send and receive company email and conduct other types of company business (Kelleher, 2013). This action should be avoided due to the inherent risks of being connected to an open, public Wi-Fi. The example discussed in the literature review regarding *Firesheep* revealed that the tool could be used to steal a person's web site authentication that is on the same open Wi-Fi as the attacker, without the attacker needing the user's credentials (Shirriff, 2010). One solution that could be offered to individuals using company equipment offsite is the usage of a personal, encrypted Wi-Fi device. Another solution may be the usage of a VPN in order to open an encrypted tunnel between the user and the corporate network. Although, if the tunnel is created through an open Wi-Fi, there may still be some data passed in the clear before the encrypted tunnel is created. This means that others may be able to capture and read that data sent in the clear before the tunnel is created. A security awareness program should strongly recommend that public Wi-Fi be avoided, and that if absolutely necessary, the user should assume that everything they send and receive over the Internet may be viewed by someone else.

Email security awareness. The importance of email safety should be included in a security awareness program. The literature reviewed showed that a high percentage of organizations had malware on their networks due to a root cause of email (Osterman Research, 2014). Examples of malicious email messages should be included, in an interactive format,

allowing the user to pick out everything that appears suspicious. Various sophistication levels of phishing emails can be used across multiple examples, in order to show the user that it is not always easy to spot a malicious email. The following security methods should be offered as a part of the awareness program on how to spot a malicious email:

- Hover over links to see where they actually go.
- Be cautious of links and attachments. A link may lead to malware, and an attachment may contain malware, such as a backdoor.
- Do not click a link to browse to a URL unless absolutely sure it is legitimate.
- Look for signs of phishing domains that look similar to the real domain, but are slightly different.
- Look for spelling and grammatical errors.
- Be aware of email that is attempting to acquire personally identifiable information.
- Look for message that state that an action must be taken within a short amount of time.
- Consider changing the settings in the email client to always view email as plain text.
- If an email appears suspicious, report it.

It is also important to include in the security awareness program that although the above tips may help identify a malicious email, attackers will likely come up with new ways to create malicious email that won't be identified by any of the tips above. It is important for the user to stay vigilant. Lastly, it is important to include information as to how and where to report suspicious email. This is especially important in an executive security awareness program, which will be further discussed in the *methods in delivering security awareness to executives* section below.

Social engineering security awareness. The literature revealed that social engineering is a way for an individual to acquire information through social interactions (US-CERT, 2013).

These interactions can be done physically in person, over the phone, or through phishing email messages. The tips discussed above on how to spot a malicious email also apply in detecting social engineering through email. A good defense against social engineering, that should be included in a security awareness program, is to make sure the individual asking for information is properly vetted. Simply believing a person is who they say they are is dangerous and could lead an individual to fall for social engineering attacks. In order to make sure that an individual on the phone is who they say they are, it is important to get as much information about them as possible, including their name, company, email address, and return phone number. Once that information is received, the caller should be told that they will be called back. That gives the phone call recipient time to verify that the information that was given by the caller is legitimate. For instance, the phone number can be researched to make sure it matches the company that the individual said they were calling from.

In a situation where the contact occurs in person, there are multiple ways that the individual could be vetted. The first aspect that should be considered is personal safety. If an individual does not feel safe confronting someone that may not belong in the work place, they should have a security contact they can get in touch with, and this contact information should be published to all employees. If the company adopting a security awareness program has a policy in place in regards to possible unauthorized physical access, this policy should be included in the awareness program.

Social media security awareness. Duggan et al (2015) discovered in the survey that 71% of adults use Facebook. Considering all of the other social media outlets available, one can deduct that a large number of adults actively use social media. Due to this, social media can be used as a channel of attack. Social media can be used for reconnaissance by an attacker to gather

information, including answers to security questions that could be used to reset passwords. The literature reviewed also revealed that attackers use social media to find out when a family is going to be out of town in order to determine the best time to burglarize the family's house (Shullich, 2011). A security awareness program should include this information along with the following tips to prevent reconnaissance and other attacks through social media:

- Lock down security settings on all social media sites to only allow known family and close friend's access to view information.
- Do not post anything that everyone should not be able to see.
- Always assume that the world is able to view the social media profile, regardless of the security settings.

Recent news stories should also be included in the security awareness program to show examples of individuals that have had trouble due to what was posted on their social media accounts.

EXIF data should also be considered in a security awareness program when discussing social media. EXIF data stores information within a digital photograph, including GPS information from the time the picture was taken (Ullrich, 2010). When these images are posted to social media sites, an attacker can use this GPS data to determine exactly where the picture was taken and can use that information to find out where their victim lives, works, goes to school, etc. The security awareness program should include this information and suggest that EXIF data be stripped from images prior to posting anything to social media.

Physical security awareness. The literature reviewed revealed some important physical security topics that should be included in a security awareness program. These topics include having a clean desk, properly disposing information, identification and company badges,

tailgating, and electronic device locking. The findings on each of these topics are reviewed below.

A security awareness program should stress the importance of keeping the work area clear of any sensitive or company proprietary information. This includes, but is not limited to, passwords, email addresses, phone numbers, and sensitive documents. As Gulati (2003) explained, custodial staff is not typically expected as an adversary, although The CERT division of the Software Engineering Institute at Carnegie Mellon University (2011) found that multiple cases of insider threats involved a custodial staff member as the culprit. Due to this, the following tips should be included in a security awareness program:

- When not in use, keep the desk or work area clear of any sensitive information including documents, cell phones, USB drives, and other storage devices.
- When custodial staff or other individuals are near an employee's work area and should not have access to the sensitive information being worked on, this information should be put away, out of plain view.

The literature reviewed explained that "dumpster diving" is a method where an attacker goes through the trash that is left outside for disposal, looking to gather sensitive information (Houchins, 2002). The following tips should be included in a security awareness program regarding proper disposal of sensitive information:

- Dispose of sensitive documents in a cross cut shredder.
- Dispose of sensitive media through permanent destruction.

A company's policies should be reviewed to determine if there is any policy or procedure on document and media destruction. If policies are discovered, they should be included in the awareness program as well.

Also to be considered in the physical security section of a security awareness program is the usage of company badges and identification. The literature showed that attackers can take a picture of someone's identification badge and use it to forge a fake badge (The Security Awareness Company, 2012). For this reason, the following security tips should be included in a security awareness program:

- Employees should only wear their badges while inside the walls of their work place.
- Employees should remove badges when leaving their work place.
- Employees should not allow themselves to be photographed at any time while wearing their identification badge, even while at work.

Another topic that should be discussed in the physical security section of a security awareness program is tailgating. The literature reviled that tailgating occurs when an individual allows someone to follow them into an access controlled environment without authenticating their access as well (Hassfield et al., 2014). An awareness program should stress that tailgating should be avoided at all times, and that everyone should be forced to authenticate their access. This could easily tie into the previous section of employee identification badges by explaining that if an attacker makes a fake badge, they will have to rely on tailgating to gain access to an access controlled area. Requiring everyone to swipe their badge to gain access to the area would thwart an attacker with a fake badge.

The final section that should be included in the physical security section of a security awareness program is the locking of electronic devices. As discovered in the literature reviewed, leaving a computer unattended without first locking it leaves the information contained on the computer accessible to anyone that happens to walk by (Prout, 2015). The same scenario holds true for cell phones, tablets, or any other electronic devices. For this reason, a security awareness

program should explain the importance of locking all electronic devices when not in use. This even includes locking the computer when leaving for only a few moments to get coffee from the break room, or use the restroom.

Importance of Executives Having an Understanding of Security Awareness

The Ponemon Institute LLC (2014) study showed that a data breach could cost a company over five million dollars. Further, a PricewaterhouseCoopers survey revealed that companies without a security awareness training program for new employees had an average annual loss of $683,000 (Mickelberg, Pollard, & Schive, 2014). These facts, coupled with the point that senior level executives are highly targeted, shows the importance of executives having a strong understanding of security awareness. Without an understanding of how their actions could open a hole for adversaries to walk through, executives may not have a strong security posture.

In the 2014 survey conducted by PricewaterhouseCoopers, it was discovered that 42% of those that responded to their survey indicated that "security education and awareness for new employees played a role in deterring a potential criminal, among the highest of all policies and technologies used for deterrence" (Mickelberg, Pollard, & Schive, 2014, p. 14). Beaver pointed out that many executives do not follow their organization's security policies. The reason for this, he offered, is because people do not like trying to enforce these policies on their management (Beaver, 2015). For this reason, many executives may be exempt from participating in their organization's security awareness program. Since the literature showed that education helped thwart attackers over other methods, it is critical for executives to gain an understanding of security awareness. For this reason, a security awareness program crafted specifically for senior

level executives should be created, and the importance of the program as discussed in this section should be relayed to the executives in order to get their buy in and support of the program.

Methods in Delivering Security Awareness to Executives

As shown, the main topics and content of a typical security awareness program should be included in an executive security awareness program. The delivery of the program is where the main differences will fall, and are what will separate an executive security awareness program from a typical security awareness program for all other employees. These methods will be discussed below.

The literature reviewed shows that executives need to be shown why they are being targeted. Further, they should be shown real life examples of security events that occurred due to other executives' accounts being compromised that had elevated rights (Hayden, 2012). Many breaches involving larger companies are fully detailed after the fact by security researches, and reports are typically made available to the public. These types of reports can be a great resource for finding examples of intrusions involving executives. Examples such as these should be included in each possible section of the security awareness program in order to assist the executives in understanding the importance of having a strong security posture.

Hayden (2012) also pointed out the importance of executive assistants in having the same understanding of security awareness. This is due to the fact that the assistants have a close, direct relationship with the executive and likely has access to much of the sensitive information that the executive does. Families of executives may also be targeted as an indirect way to gain access to the executives' corporate network. It is recommended that this is explained to the executives and that they are encouraged to discuss security awareness with their assistants and even their families. This will also be beneficial to the executives because the more they discusses the

content of the awareness program, the more it will be in the forefront of their thoughts, and they may become even more vigilant.

The literature also points out the importance of establishing a means for executives to communicate suspicious activity to the proper individuals, and that these communication channels should be specific to the executives and have a priority response. This reason for this is to ensure a quick response to a suspicious contact submission, as a slow response could discourage the executive from submitting future suspicious contacts (Hayden, 2010). It is recommended that these communication channels be established prior to rolling out an executive awareness program. These communication channels should include a hotline phone number as well as an email address. The email address and phone number should be directed to the proper security personnel for immediate response. If the organization has an on call incident response team, the email and phone number should be set up to go through to the individual or group that is on call. It is recommended that an immediate response be provided to the executive submitting the suspicious contact, if only to advise them that the submission has been received and is being actively investigated. This contact information should be clearly communicated to the executives. A magnet or flyer with the special contact information could be made for the executive to stick in their office as a constant reminder. The contact information should also be included in any regular reports created for executives. The more that they see and become familiar with these communication channels, the more likely they will be to remember them and use them when encountering suspicious activity.

A study by the Ponemon Institute LLC (2013) stated, “The majority of the security professionals are not able to effectively articulate the security risk or demonstrate clearly that security is aligned with the goals of the business” (p. 47). Companies and organizations will all

have differences in their business goals. Therefore it is important for those implementing an executive security awareness program to gather an understanding of these goals and implement the awareness program to fit in line with them. Further, an executive security awareness program would be an excellent avenue for discussing these security risks to senior executives, and explaining how they tie in with the goals of the company.

The study also revealed that IT staff does not properly relay information to senior level executives in layman's terms that non cyber security personnel would understand (Ponemon Institute LLC, 2013). For this reason, it is important that an executive awareness program be delivered in a non-technical manner so that senior level executives can understand. Executives are likely business professionals rather than cyber security professionals. If technical terms must be used in the program, these terms should be clearly defined and explained well.

Another aspect that must be considered when implementing an executive security awareness program is the timeframe in which the program should be delivered to the executive, and how long each portion of the program should last. The literature revealed that Presidents and Vice Presidents of a company or organization work more hours each week than other job titles. Due to senior executives having such a busy schedule, an executive awareness program must be strategically implemented to deliver a clear and precise message without taking much time. This could be done by splitting up the program into small segments that can be delivered over an extended period of time, specifically based on the executives' schedules. Seeing as different executives have different time constraints, the executive security awareness program timeframe should be decided by each individual organization adopting the program. It is recommended that a program be continual, lasting throughout the entire year.

The literature also revealed that the majority of respondents in a study conducted by the Ponemon Institute do not "meet with senior executives routinely about cybersecurity risks" (Ponemon Institute LLC, 2013, p. 47). This disconnect could cause a large security failure for multiple reasons. If senior executives are not kept abreast of current risks, they may not have a good understanding of the importance of cyber security programs, and may not provide proper funding. Further, without knowledge of current threats, they may fall victim to attacks themselves, putting the company at a large risk of data loss, financial loss, and public embarrassment. An executive security awareness program is a great way to ensure the continual communication with senior executives in order to keep them informed on current threats, improve their security posture, and help them make informed decisions on funding for cyber security programs.

Comparison of Findings

This study revealed what appears to be a common problem; many executives may not participate in their organization's security awareness program, and also may be exempt from the security policies of the company they work for. The literature showed that this is because senior level executives are at the top of the command chain and individuals that work under them do not feel comfortable forcing the executives to follow the company's security policies. A new way of approaching this problem would be the creation of an executive security awareness program that includes all of the typical security awareness topics, but focused to capture the interest of senior level executives. The creation of this program should be preceded by discussions with the senior level executives to discover what security awareness topic areas they know most and least about, and what they feel the main goals of the company are. This will allow an organization to further tailor the awareness program to its own executives.

Limitations of the Study

Three main limitations became apparent throughout the course of this study. The most significant limitation was the lack of available information specific to executive security awareness programs. A plethora of information was discovered in regards to typical security awareness programs that many companies and organizations utilize to increase the security posture of their employees, and multiple articles and blog posts were discovered with individuals' opinions on education of executives on cyber threats, but very little was discovered in the area of actual studies on executive cyber security awareness programs. In order to overcome this, research was conducted on the security awareness topics for typical employees, which are just as important for senior level executives to understand. Research was then conducted on how executives learn, what peaks their interest, and what their typical time constraints are. This allowed for recommendations as to what should be included in an executive security awareness program, as well as recommendations on delivery.

Another limitation of the study was that no interviews were conducted with senior level executives. Interviewing a large number of executives on their preferred methods for learning new information could be very useful in the creation of an executive security awareness program. Further, interviewing a large number of executives to determine their current understanding of the cyber security awareness topics could lend a great deal to this study. Knowing how much the average senior level executive understands current cyber security awareness topics would allow for a deeper focus in the executive awareness program for the areas least understood by the average executive. This may also assist in creating an outline of which topic areas should be discussed first.

The final limitation is that an actual security awareness program containing slides, printable handouts, videos, and interactive activities was not created. In part, this was due to time constraints. Another reason for this was that each company is unique, and an executive security awareness program should be specifically tailored to their own executives. A one size fits all executive security awareness program does not appear to be the best solution, due to uniqueness of each company and senior executive.

RECOMMENDATIONS & CONCLUSIONS

Importance of Executive Security Awareness

Based on the research conducted in this study, it has been shown that a security awareness program can be a critical part in enhancing a company's security posture. It can assist by reducing successful intrusions, and by empowering employees with the knowledge of how to detect and report suspicious activity. It also helps employees gain a stronger understanding of how to be safe when using both company, and personal computers and other electronic devices.

The research also revealed that senior level executives contain valuable knowledge and have access to large amounts of information about the company they work for. Unauthorized access to their accounts could cost the company they work for large amounts of money and embarrassment (The Ponemon Institute LLC, 2014). Further, an adversary with access to a senior level executive's account could use it to craft phishing attacks against other individuals in the company. These phishing attacks would more likely be trusted by the target due to the account that they came from. Due to this, it is imperative that senior level executives gain a strong understanding of the security awareness topics previously discussed.

Gap Areas in Executive Security Awareness

There appears to be a large gap across all industries in the lack of senior level executives that participate in their company security awareness program. Senior level executives are at the top of the command chain. For this reason, cyber security staff may feel uncomfortable attempting to make the executives abide by company security policies (Beaver, 2015). For this reason, a creation of an executive security awareness program is recommended, and could greatly assist in closing this security gap. This program should include all of the security awareness topics discussed in this report, along with any additional topics that are relevant to the

organization creating the program. This could vary from industry to industry and company to company. Further, as time moves forward, additional topics may arise that do not currently exist.

Executive Security Awareness Program

Preliminary steps. Prior to the creation and implementation of an executive cyber security awareness program, specific work and research should be conducted. It is recommended that those charged with creating the program set aside time to meet with the senior level executives on an individual basis to gather some information. During these meetings, the executives should be asked what they feel the company's goals are. This will assist with keeping the program in line with these goals. For example, an executive may feel that one main company goal is customer service. When creating the various sections of the program, it can be shown that the program will assist with protecting the customer's data in order to ensure the best customer service possible. One reason for this is to get the executives to buy in to the program. The executives are the target audience of this awareness program and without their support the program will likely fail. Another reason to meet with the executives is to gather an assessment of their current security knowledge. With an understanding of this, the executive security awareness program can be specifically tailored to have a stronger emphasis on the subject areas that are least understood by the executives.

Creating an executive security awareness program. When ready to create an executive security awareness program, it should not be forced on senior level executives, but rather should be crafted strategically to capture an executive's attention. This should be done by including recent news regarding other companies or organizations that have been breached due to an executive's poor security actions, and then presenting the security awareness techniques to the executives in order to show what could have been done to prevent the intrusion. These example

breaches could include companies that have suffered data loss, financial loss, or the compromise of company integrity. It is important to always try to relate to the executives when creating this program. Referring back to the initial meeting with the executives is a great way to keep this on track.

When creating the executive security awareness program, it is important to keep in mind that executives typically are not cyber security professionals. It is easy to get caught up in technical terminology, especially for those that use the technical terms every day, so explaining technical ideas in a non-technical fashion may be difficult. However, using technical terminology and security jargon could lose the executive's attention. If a technical term must be used, it should be clearly defined and explained in laymen's terms.

Delivery of an executive security awareness program. Executives are very busy and may have little time to devote to security awareness training (Bailey, 2015). Due to this, it is recommended that the segments be broken out into short snippets, but spread throughout the entire year. Security awareness training should not be a one-time training, it should be continual. This does not necessarily mean that every week an executive must set aside a few minutes to sit down with security staff to learn security awareness. Security awareness tips can be distributed a number of ways, including but not limited to regular email campaigns, included in regular reports to the executives, or even placed on flashy graphical posters posted in the workplace. The more that the security awareness tips are seen by executives, the more it will be in the forefront of their thoughts.

Direct line reporting. One last action that should be taken prior to rolling out an executive security awareness program is the creation of various methods for executive staff to report suspicious activity, or to contact cyber security professionals. This should include a

dedicated phone number and email address that is only published to the executives. These methods of communication should be closely monitored and made a priority for response. If an executive is forced to wait an extended period of time before getting a response, they may be less likely to report suspicious activity in the future (Hayden, 2012). Due to this, it is also recommended that as soon as suspicious activity is reported by an executive, they should be advised that the security team has received their information and will be actively investigating.

Recommendations for Further Research

These conclusions could have also been arrived at through conducting interviews of a large number of executives. If executives were interviewed as a part of this research, they could have specifically been asked how much time they felt they would be able to allocate on a regular basis for security awareness training. They could have also been asked their preferred method for learning. It is likely that these answers would vary based on the size of the company, industry, and even personality of each executive interviewed. However, if enough interviews were conducted, an average response may have been discovered. It is recommended that this method of information gathering from executives be conducted in future studies on the topic of executive security awareness programs.

Conclusions

As shown through the research conducted, senior level executives, spanning all industries, are amongst the most targeted individuals at a company or organization. This appears to be due to a number of reasons, including the amount of information about the company or organization that an executive knows, what an executive has access to, and what an attacker could do with an executive's credentials. The research also showed that there appears to be a lack of security awareness education for senior level executives. This proves to be a large gap

area across all industries due to the amount of access and information that executives have, coupled with the fact that they are highly targeted.

A way to close this gap is for companies and organizations to create an executive security awareness program that is specifically tailored towards their executives, and also captures their attention. The purpose of this project was to create a primer that could be used as starting point for any company or organization wanting to create their own executive security awareness program. In order to do this, an attempt was made to discover the major topic areas that should be included in any security awareness program. The idea being that the content of an executive security awareness program would be similar, if not exactly the same, as a regular security awareness program for all other employees. The differences are in the delivery, timing, and methodologies for capturing an executive's attention in order to get their buy in to the program. It was recommended that all of the topic areas discussed in this research be included in an executive security awareness program. The main topic areas discovered and researched were:

- Cell phones
- Passwords
- Public Wi-Fi
- Email
- Social engineering
- Social media
- Physical security

Research was then conducted on the importance of security awareness. One main reason for this research was to discover information that could be shared with senior level executives in order to get their support of an executive security awareness program. One study utilizing

surveys showed, “Security education and awareness for new employees played a role in deterring a potential criminal, among the highest of all policies and technologies used for deterrence” (Mickelberg, Pollard, & Schive, 2014, p. 14). It was also discovered that security awareness programs can save a company or organization large amounts of money.

Based on the research, it was recommended that individuals that plan on creating an executive security awareness program schedule a preliminary meeting with each of their executives individually prior to creating the program. During the meeting, the executive’s knowledge of the various security awareness topics should be assessed, along with the discovery of the time constraints that each executive has. Further, during the meetings, the executives can specifically be asked what methods of being educated do they prefer the most. This meeting could be a key part in specifically tailoring a security awareness program to the executives.

Methods on educating senior level executives were researched next. One of the main methods discovered during the research was the importance of not using technical jargon. This is because executives are typically business oriented, and are not cyber security professionals. Another important method discovered was the usage of current events where other executives were targeted and a breach occurred. The reason behind this is to show the executives why they are being targeted, and what could have been done differently by the executive to prevent the breach. This will also help capture the executive’s attention and help to show the significance of security awareness. One of the other main methods discovered was that each security awareness session with an executive should be completed in a clear and concise fashion, broken into small segments of time. It was determined that each company or organization creating an executive security awareness program must determine their own executives’ time constraints and tailor their program based on their own executives.

As shown, a way to close the gap area in the lack of executive security awareness is for companies and organizations to create their own executive security awareness programs that are specifically tailored towards their executives. The research and recommendations in this paper can be used as a primer for companies and organizations across all industries to use when attempting to create and implement their own executive security awareness programs.

REFERENCES

2014 Deloitte-NASCIO Cybersecurity Study (2014). Retrieved from http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf

Bailey, M. (2015, January 19). *Four reasons executives should participate in security awareness and training*. Retrieved from http://info.wombatsecurity.com/blog/4-reasons-executives-participating-in-security-awareness-and-training

Beaver, K. (2015). *Five reasons your employees are violating your security policies*. Retrieved January 30, 2015, from https://www.tnwinc.com/products-services/ethics-compliance-elearning/security-awareness-training/

Better Business Bureau. (2014, December 19). *Scam alert -- fake confirmation emails trick holiday shoppers*. Retrieved from http://www.bbb.org/council/news-events/bbb-scam-alerts/2014/12/scam-alert-fake-confirmation-emails-trick-holiday-shoppers/

CERT. (2011, May 10). *Insider threat and physical security of organizations*. Retrieved from http://www.cert.org/blogs/insider-threat/post.cfm?EntryID=71

Consumer Reports. (2014, April 17). *3.1 million smart phones were stolen in 2013, nearly double the year before.* Retrieved from http://pressroom.consumerreports.org/pressroom/2014/04/my-entry-1.html

Dodd, D. (2012, March 4). *Post exploitation using Metasploit pivot & pivot forward*. Retrieved from http://www.sans.org/reading-room/whitepapers/testing/post-exploitation-metasploit-pivot-port-33909

Duggan, M., Ellison, N., Lampe, C., Lenhart, A., & Madden, M. (2015, January 9). *Social media update 2014*. Retrieved from http://www.pewinternet.org/files/2015/01/PI_SocialMediaUpdate20144.pdf

Google. (n.d.). *Stronger security for your Google account*. Retrieved February 11, 2015, from https://www.google.com/landing/2step/#tab=how-it-works

Gott, A. (2014, July 11). A note from *LastPass*. Retrieved from https://blog.lastpass.com/2014/07/a-note-from-lastpass.html/

Gulati, R. (2003). *The threat of social engineering and your defense against it*. Retrieved from http://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232

Harley, D., & Abrams, R. (2009, August). *Keeping secrets: Good password practice*. Retrieved from http://www.eset.com/us/resources/white-papers/EsetWP-KeepingSecrets20090814.pdf

Hassfield, G., Larkin, B., White, J., Dodson, J., Duprey, K., Stamberger, J., ... Pigna, E. (2014, November 13). *Security tailgating (aka piggybacking)* (D. Catterton, J. Stamberger, E. Erickson, P. Thomas, P. Trapanese, & E. Corzine, Eds.). Retrieved from http://www.alliedbarton.com/Portals/0/SRC/WhitePapers/Security Tailgating - Best Practices in Access Control.pdf

Hayden, E. (2012, October). *How to begin corporate security awareness training for executives*. Retrieved from http://searchsecurity.techtarget.com/tip/How-to-begin-corporate-security-awareness-training-for-executives

Houchins, T. (2002, August 1). *Security's biggest threats: Social engineering and your employees*. Retrieved from http://www.giac.org/paper/gsec/2149/securitys-biggest-threats-social-engineering-employees/103657

Internet Crime Complaint Center. (2015, January 22). *Public service announcement* (Alert Number: I-012215-PSA). Retrieved from http://www.ic3.gov/media/2015/150122.aspx

Kelleher, K. (2013, September 19). *95.6% of commuters in the US put company data at risk over free public Wi-Fi [survey]*. Retrieved from http://www.gfi.com/blog/survey-95-6-of-commuters-in-the-us-put-company-data-at-risk-over-free-public-wi-fi/

Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Bauer, T. V. L., Christin, N., ... Lopez, J. (2012). *Guess again (and again and again): Measuring password strength by*

simulating password-cracking algorithms. Retrieved from https://www.ece.cmu.edu/~lbauer/papers/2012/oakland2012-guessing.pdf

Kharpal, A. (2014, November 10). *'Dark Hotel' hacks target business travelers: Report*. Retrieved from http://www.nbcnews.com/tech/security/dark-hotel-hacks-target-business-travelers-report-n245266

Kovacs, E. (2014, November 14). *Feedback Friday: Executives targeted in 'Darkhotel' attacks – industry reactions*. Retrieved from http://www.securityweek.com/feedback-friday-executives-targeted-darkhotel-attacks-industry-reactions

Li, Z., He, W., Akhawe, D., & Song, D. (2014). *The emperor's new password manager: Security analysis of web-based password managers*. Retrieved from http://devd.me/papers/pwdmgr-usenix14.pdf

Mandell, A., & Weise, E. (2014, December 6). *Sony hit again, employee families threatened, files released*. Retrieved from http://www.usatoday.com/story/life/movies/2014/12/05/sony-hacked-again-this-time-employee-families-threatened/19970141/

Mickelberg, K., Pollard, N., & Schive, L. (2014). *US cybercrime: Rising risks, reduced readiness (Key findings from the 2014 US State of Cybercrime Survey)*. Retrieved from http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

Microsoft. (n.d.). *Check your password-is it strong.* Retrieved from https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx

Nield, D. (2014, January 2). *Remove location data from your photos before sharing them*. Retrieved from http://fieldguide.gizmodo.com/remove-location-data-from-your-photos-before-sharing-th-1593773810

Osterman Research. (2014, January). *Best practices in email, web, and social media security*. Retrieved from

http://www2.trustwave.com/rs/trustwave/images/Best_Practices_in_Email_Web_and_Social_Media_Security_Trustwave.pdf

Pace Productivity. (2010, October). *Hours worked by job*. Retrieved from http://getmoredone.com/2010/08/hours-worked-by-job/

Ponemon Institute LLC. (2013). *The state of risk-based security management*. Retrieved from http://www.tripwire.com/it-resources/the-state-of-risk-based-security-2013-full-report/showMeta/2/?dl=C4FEDC6D-CA1F-B5BC-8816561E822ACABE

Ponemon Institute LLC. (2014, May). *2014 cost of data breach study: United States*. Retrieved from http://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03017usen/SEL03017USEN.PDF

Prout, B. (2015). *Basic security measures we sometimes forget: Lock your computer*. Retrieved from http://www.sophos.com/en-us/security-news-trends/security-trends/basic-security-measures-we-sometimes-forget-to-use-part-1.aspx

Roberts, P. (2015, January 21). *Research exposes attacks on military, diplomats, executives.* Retrieved from https://securityledger.com/2014/12/research-exposes-attacks-on-military-diplomats-executives/

Schmidt, J. (2011, December 20). *How to manage the weak link in cybersecurity: Humans*. Retrieved from http://www.crn.com/blogs-op-ed/channel-voices/232200743/how-to-manage-the-weak-link-in-cybersecurity-humans.htm

Security Awareness Company. (2012, October). *Security awareness news: The security awareness newsletter for security aware individuals*. Retrieved from http://www.tn.gov/homelandsecurity/docs/SAC_SpecialEdition_2012October.pdf

Security Awareness Program Special Interest Group PCI Security Standards Council. (2014, October). *Information supplement: Best practices for implementing a security awareness program*. Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Shirriff, K. (2010, October). *Inside the Firesheep code: How it steals your identity*. Retrieved from http://www.righto.com/2010/10/firesheep-how-it-steals-your-identity.html

Shullich, R. (2015, December 5). *Risk assessment of social media*. Retrieved from https://www.sans.org/reading-room/whitepapers/privacy/risk-assessment-social-media-33940

Siegrist, J. (2011, May 4). *LastPass security notification*. Retrieved from https://blog.lastpass.com/2011/05/lastpass-security-notification.html/

Sparkes, M. (2014, December 1). *Hackers target 'top pharmaceutical executives' to gain trading advantage*. Retrieved from http://www.telegraph.co.uk/technology/internet-security/11265539/Hackers-target-top-pharmaceutical-executives-to-gain-trading-advantage.html

Sundhar, S. (2014, November 8). *The evolution of a phish: Phishing delivery mechanisms.* Retrieved from http://info.phishme.com/l/46382/2014-11-08/23tmc/46382/25150/Evolution_of_a_Phish_whitepaper.pdf

Symantec. (2012). *The Symantec smartphone honey stick project*. Retrieved from http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide_honeystick

Trustwave. (2010). *Security awareness education training.* Retrieved January 26, 2015, from https://ssl.trustwave.com/security-awareness-education.php

Ullrich, J. (2010, February 10). *Twitpic, EXIF, and GPS: I know where you did it last summer*. Retrieved from https://isc.sans.edu/diary/Twitpic EXIF and GPS I Know Where You Did it Last Summer/8203

University of Rochester. (n.d.). *Security tip of the week archive*. Retrieved February 18, 2015, from http://www.rochester.edu/it/security/securitytipofweek_archive.html

US-CERT. (2013, February 6). *Security tip (ST04-014): Avoiding social engineering and phishing attacks*. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-014

Valente, E. (2009). *Two-factor authentication: Can you choose the right one?* Retrieved from http://www.sans.org/reading-room/whitepapers/authentication/two-factor-authentication-choose-one-33093

Vengerik, B., Dennesen, K., Berry, J., & Wrolstad, J. (2014). *Hacking the street? FIN4 likely playing the market*. Retrieved from http://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf

Verizon. (2014). *2014 data breach investigations report*. Retrieved from http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf

Webroot. (2010, October 12). *New Webroot survey reveals poor password practices that may put consumers' identities at risk*. Retrieved from http://www.webroot.com/us/en/company/press-room/releases/protect-your-computer-from-hackers