Developing a Security Awareness Program

Mark Heckle

East Carolina University

ICTN 6823 Section 601

Dr. Phil Lunsford

Date: July 19, 2019

Abstract

In today's environment, technology has become a way of doing business. Because of technology, information security has become a necessary factor in how we use technology in our companies. There are certainly ways to help protect the technology with additional hardware and software, but the human component plays a vital role in reducing security risks. It is necessary to make the employees more security aware by developing security awareness programs. This research will show how to develop a security awareness program for your organization. It will also present ways to engage employees in such a plan for your organization. The security awareness program is the first step in protecting your organization from such events as ransomware, phishing attacks, spam, and many more.

Introduction

Organizations are facing a multitude of cybercrime attacks throughout their systems. These cyber crimes have increased every year with no sign of slowing down soon. The techniques have become more advanced, and the motivations vary to include ego, revenge, crime, money, and mischief, to name a few (Awawdeh and Tubaishat, 2014). Cybercrimes are being committed all over the world and can affect any organization. Users that are uneducated around cybersecurity are the most vulnerable for attacks. Hackers attack these users through many avenues, and these uneducated users are easy targets even though most organizations seem to be secure (Awawdeh and Tubaishat, 2014). Most employees don't intentionally create these errors that cause a security incident. Because most of these incidents are unintentional, it is imperative that education teaches us in organizations through a developed Security Awareness Program. One of the attacks that are seen all around the world with success is the phishing attacks. This paper will review phishing attacks and the growth seen over the last few years. Phishing attacks are costing organizations millions of dollars along with damaging their reputations. The information in this document will introduce a starting point to implement a Security Awareness Program for any organization. Awareness Programs are intended to change behavior and the culture in an organization. Changes will not happen overnight, but with continued effort, organizations will notice positive changes in the months ahead. This paper will examine good points to establish a robust program.

Phishing Attacks

Phishing attacks are one of the most used attacks in the world to steal bank information, social security numbers, user IDs, and passwords. It starts by the hacker, creating a fake website that resembles a legitimate site. A link is sent out to thousands of users to have them click on the

fake link and enter their personal information (Aloul, 2010). The look at the trends of phishing over the first quarter of 2019 it is essential to review the data that is distributed by the Anti-Phishing Work Group. The APWG data that was released states there are over 81,000 unique phishing web sites along with over 42,000 individual campaigns that have been reported by consumers in March 2019. These stats are up 20% since February 2019 (Docs.apwg.org, 2019). Whatever the eventual target, attackers are showing more essential skills when it comes to phishing. Some of us may laugh when we see some of these emails end up in our inbox, but the truth is that many people fall victim to these scams. The hackers understand this and continue to blast our inboxes with these emails (Art of Phishing, 2018). Of all the different threats, phishing is one of the hardest to defend with technology. Technology can certainly help, but the human element is where the majority of the time needs to be spent (Art of Phishing, 2018).

Security Awareness Program

According to the National Institute of Standards and Technology (NIST), "Awareness is not training. The purposes of the awareness presentations are to focus the attention of security. Awareness presentations are intended to allow individuals to recognize IT security concerns and to act accordingly" (Wilson & Hash, 2003). Implementing such a program is a necessary part of the overall security infrastructure that should be in place at any organization. These programs are designed not to train the individual but to change their behavior about security (Wilson & Hash, 2003). A Security Awareness Program should work in conjunction with the organizations IT hardware and software to help protect against threats to the company. It is crucial to state that an Awareness Program is for everyone, including all management, executives, and even IT staff. One of the first items to complete before the program is successful is to get buy-in from the

executive team. It should be supported from the top down to be successful and taken seriously by other departments.

The goals of any Security Awareness Program are to lower the attacks on your organization, empower the users to take responsibility of protecting the organization and enforcing any policies that are in place such as computer policies, internet, password, and remote access policies (Gardner & Thomas, 2014). As stated before, people are the weakest link in this information security. They don't choose this as people want to do a good job and provide the best possible customer service to their customers. Hackers seek to exploit the good human nature in these people. The only known protection against this type of attack is an active Security Awareness Program (Gardner & Thomas, 2014). Employees are going to want to see the expectation of them and who they will turn to if they have questions. The employees also need to understand that this program is supported, approved, and initiated from the top (Peltier, 2005). Another fundamental goal is that every employee gets the message. This message should start during the employee orientation, continue throughout the year, and even require annually mandated assessments (Peltier, 2005). One thing to understand is it must maintain and not fizzle out after the big kickoff. It is common for everyone to come together for the initial opening and then not meet again for months. The program will not be successful if this happens. It is crucial to keep the program in front of the employees during the entire year or more than likely, and it will fail. It isn't always enough to keep the message just in front of the employees. The good idea is to tie it back into your organization's strategic goals showing how a security breach could affect the overall goals (Peltier, 2005). The security program is meant to reduce company losses, whether accidental or intentional disclosure of information by the employees and established by raising awareness to the employees during the program.

Implementing the Security Awareness Program

Some guidelines to follow when implementing a Security Awareness Program. The NIST Special Publication 800-50 provides the guidelines for non-profit organizations (Kolb & Abdullah, 2009).

- Get Buy-In from the Top - It is mandatory that you get this top-level support. A champion will provide the needed authority for the security program. It will signify the importance of the program to the employees, and it could allow for the program to have valuable resources available.
- Assemble a Team- Another significant step in implementing the program is the assemble a team. This team shouldn't be all IT employees, but it should include expertise from Legal, IT, HR, and other key departments. The team will represent all aspects of the organization as this effort is widespread and not solely on the Information Security Department.
- Assess the Environment- Assess the current policies that your organization has in place. All policies should be reviewed by the awareness team to make sure each policy is current. If policies are absent, then new policies should be created by the organization. "Policies must have a scope, intended audience, a clear instruction, and a reasonable disciplinary action for violation of the policy" (Kolb & Abdullah, 2009).
- Survey Employees- To identify the knowledge of current employees around policies, a survey should be handed out. Here are some questions to ask the employees.
  - Do you know what a virus is?
  - Have you heard of Phishing?
  - Are you aware of spam emails?

- Do you know how spam emails harm a company?
- Have you read the security policies that are in place?

Again, these questions are to see if the intended audience has any knowledge around security.

- Educate the Employees- There should be an education session for employees talking about the upcoming Security Awareness Program, the survey results, the current security threats, the support from the organization, and policies that are already in place. It is almost always impossible to have a session with every employee attending, so one idea is to create this education session by video. Some organizations have this capability and can distribute this method to all employees. It is vital to make this education session mandatory.
- Monthly Awareness Campaigns- One education session isn't enough for an organization, so it is crucial that a monthly awareness meeting is scheduled and established. It is also essential to video the meeting if possible, so employees that can't attend will be able to view at a later time. Remind employees of the constant security threats in the world and acceptable behavior. Everyone will have their ideas of promoting the programs, but some thoughts are newsletters, posters that are put up around the organization, emails, or calendar invites (Kolb & Abdullah, 2009).

Methods on Delivery of the Message

People learn in many different ways and gather information from many various sources. It is imperative to understand the best way the audience likes to learn to deliver a message where people are focused on the topics. There are three methods to look at when deciding what is best for the audience. The three modes are reading from a book, watching a video, and have first-

hand demonstrations (Peltier, 2005). Another essential piece of information to obtain by the awareness program is how do most people gain knowledge for their data or news? According to a pew research study, 57% of Americans receive their information from TV, and 30% obtain it from online resources ("How Americans get their news," 2016). Since almost 90% of people learn from digital resources, it is safe to say that most people are visual learners. It is essential to use this information for the awareness program. Most of these types of learners like to see diagrams or pictures to visualize the discussion. Delivered to the current employees or even an outside resource will be a video of the meeting. Robust awareness programs will also take advantage of newsletters, brochure, and booklets. The effectiveness of these media types will depend on how well they have been put together (Peltier, 2005).

Presentation Topics

What do we look at for topics of our awareness program? There are many topics to discuss with security, but remember security is comprehensive. The audience will not be very technical, so it is crucial not to talk over their heads. It is essential to prioritize the message to the employees. One such resource to use would be a current risk assessment from the organization (Peltier, 2005). Many organizations have yearly security audits done where the organizations are provided a list of items for improvement. The security audit report is an excellent source that will provide many topics for the start of the security awareness program. After the identity of the topic(s), present the message, reinforce the word, and build up to the next objective.

Communication

Most of the items below are very straight forward, but they are items to remember when communicating to the audience.

Prepare for the presentation- Everyone should know this, but it is essential that the presenter is well prepared. The audience will quickly lose their attention if the presenter is stumbling around for words or papers.

Audience- It is vital to know the audience. Don't use too much technical jargon as these users will not understand that communication.

Present- Present the information instead of just reading from a piece of paper. It is crucial for the presenter to know the information. Anyone can read words from paper or PowerPoint presentation.

Time- Everyone's time is precious, and typically there aren't enough hours in the day. Keep the meeting at an hour or less.

Schedule- Try to schedule around the busier times of the week. The scheduling might become a difficult task, but maybe a Wednesday is better than a Monday. The meeting could be scheduled even at lunch if lunch is provided (Peltier, 2005).

Enforcing Methods

After presenting all of the information at the awareness program, it is necessary to enforce the teachings during the session. There are a few ways that come to mind testing the employees on the information that was covered. Again, it is crucial that the employees understand that they are to share the responsibility of security and be held accountable. It might be possible to have each employee sign a confidential agreement on an individual policy. Testing is undoubtedly used in these types of programs to understand if the employee has retained the information. One could also set up a reward program if the users complete their tests with a 100. Part of the employee's annual review could have a portion weighted from the Security Awareness Program ("Security Awareness: switch to a better programme," n.d.)

Costs and Benefits

A Security Awareness Program is one of the least expensive options around security that after implementation, the organization benefits swiftly. Like all implementations, there are a few costs that should be kept in mind.

Costs

- If you decide to bring in a professional to speak, there could be costs associated with that. Most vendors that currently work in the organization are usually more than willing to present free of charge.
- Any outside space rental that might be needed is space is tight at the organization
- Any materials that will be required, such as posters, bulletins, newsletters, or swag materials. Most larger organizations have a marketing department that could help with this process.
- Any outside training or courses required for the program will need to be purchased. An organization may have something in place already that can be taken advantage of, such as a learning center.
- The cost of the time away for the employees from their regular job duties ("Security Awareness: switch to a better programme," n.d.)

Benefits

- Improved compliance with laws and regulations (Healthcare example would be HIPAA)
- Overall security risks are lower because of the awareness program
- Less internal incidents occur. Employees are now more aware of what to look for, such as a phishing email. The users are more inclined to reach out to someone before just clicking on a suspicious email.

- The employees moral seems to get boosted Some users are embarrassed that they don't know a lot about security
- It helps with company reputation. A security breach can undoubtedly ruin a company's reputation, along with losing customers ("7 Benefits of Security Awareness Training [Updated 2019]," 2019).

Conclusion

With the ever-changing technology in the world today, hackers will continue to expose easy targets all around the world. There are many reasons for the hacks, but one conclusion is that hackers continue to detect easier targets in an organization. The hackers focus on users or employees of an organization. Some of the attacks are as simple as sending a phishing email where a user clicks on a specific link and enters personal data such as passwords, bank information, or even social security numbers. This paper has shown one reasonably easy step to take is to implement a Security Awareness Program. The awareness program is an inexpensive solution with great benefits to any organization. This paper discusses a focuses on fact, and that is security is not the entire responsibility of the IT Department. Security has to be the responsibility of the organization as a whole, and everyone must share this accountability. The Security Awareness Program must have the backing from Senior level management, or it will most likely fail. By having the buy-in from the top, it shows the employees the organization is stern around security. The benefits by far outweigh the costs of such a program. Some of the benefits mentioned in the paper include compliance with laws, boost employee morale, less internal incidents, and helps with company reputation. Security Awareness Programs might not require vast amounts of money, but they do require time and management of the program. It is essential that different avenues of delivery are used during the program and switch it up at times by bringing in outside speakers.

Everyone will need to believe in the program, including yourself. After a few awareness events, the employees will realize it is just part of the organizational culture and be happy to participate. If you haven't already implemented a Security Awareness Program, please look into developing one.

References

S. A. Awawdeh and A. Tubaishat, "An Information Security Awareness Program to Address Common Security Concerns in IT Unit," *2014 11th International Conference on Information Technology: New Generations*, Las Vegas, NV, 2014, pp. 273-278. doi: 10.1109/ITNG.2014.67

Kolb, N., & Abdullah, F. (2009). Developing an information security awareness program for a non-profit organization. International Management Review, 5(2), 103-107. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/195572110?accountid=10639

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. Washington, D.C: National Institute of Standards and Technology, Technology Administration, U.S. Dept. of Commerce. Retrieved from http://www.books24x7.com/marc.asp?bookid=10225

Manke, Ira Winkler, and Samantha. (2014). 6 steps to win executive support for security awareness programs. Retrieved from https://www.csoonline.com/article/2456290/6-steps-to-win-executive-support-for-security-awareness-programs.html

F. A. Aloul, "Information security awareness in UAE: A survey paper," *2010 International Conference for Internet Technology and Secured Transactions*, London, 2010, pp. 1-6.

URL: http://ieeexplore.ieee.org.jproxy.lib.ecu.edu/stamp/stamp.jsp?tp=&arnumber=5678046&isnumber=5678008

Docs.apwg.org. (2019). [online] Available at: https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf [Accessed 13 Jul. 2019].

The art of phishing. (2018). Computer Fraud & Security, 2018(11), 1. doi:10.1016/S1361-3723(18)30101-5

Gardner, B., (Bill G.), & Thomas, V. (2014). Building an information security awareness program. Retrieved from http://proquest.tech.safaribooksonline.de/9780124199675

Thomas R. Peltier CISSP, CISM (2005) Implementing an Information Security Awareness Program, Information Systems Security, 14:2, 37-49, DOI: 10.1201/1086/45241.14.2.20050501/88292.6

How Americans get their news. (2016, July 14). Retrieved from https://www.journalism.org/2016/07/07/pathways-to-news/

Security awareness: Switch to a better programme. (2006). Network Security, 2006(2), 15-18. doi:10.1016/S1353-4858(06)70337-3

7 Benefits of Security Awareness Training [Updated 2019]. (2019, February 11). Retrieved from https://resources.infosecinstitute.com/7-benefits-of-security-awareness-training/#gref