8-2 Short Paper: Security Awareness Communication

Michael Singletary

IT-335, 17EW6, SNHU

Introduction

As part of any security policy document design and implementation process, it is important to include security awareness communications as part of the roll-out. A policy on communicating security awareness information to an employee base will help ensure that employees at all levels of the organization are both involved in the process and understand the importance of these policies. Simply providing policy documents to employees is not enough to ensure that these policies are read, understood, appreciated, and practiced consistently in order to provide an improved security posture. There are many methods available for communicating this information to employees, which are detailed below.

Methods for Communicating Security Awareness

The first step to communicating security awareness information to employees is to let them know that this information is going to be available, is important, and is a requirement of their job along with their regular responsibilities. This initial communication may take the form of an informational email or memo sent to employees describing the importance of security awareness and its benefits to both the company and its employees.

Next, employees should be informed in greater detail about these security awareness efforts and any changes that come as a result of them. This more structured communication may take the form of an in-person meeting with those responsible for implementing the change and designing the awareness information. This brief meeting would give the instructors time and an appropriate place to highlight the importance of security awareness including common pitfalls and the results of failing to maintain a secure environment, which has been shown to increase the attention of audience members (Fitzpatrick, 2010). Questions and answers may also be fielded during this session.

As a complement or alternative to an in-person meeting, another effective method of communicating this information would be through video conference or recordings. This method would allow employees unable to attend an in-person training session the ability to receive the same security awareness information as those that were able to attend the session. As an added benefit, an in-person meeting itself might be recorded and made available for later playback so that the benefits of the question and answer section may be realized by those unable to attend physically.

Another effective method for communicating security awareness would include designing eye-catching and quick to read flyers that could be distributed and hung in common areas of the workplace. These flyers should be varied but include crucial and easy to absorb security awareness information that would reinforce knowledge and practice of selected principles. While also communicating useful information, these flyers would serve to stress the importance of the information by making it obvious and visible frequently throughout the workplace.

Quizzes can also serve as a means for communicating security awareness to employees. Having managers deliver occasional security quizzes to employees can serve as a method to not only check knowledge but to also re-inform employees about important security awareness information. Once a question is answered, for example, the correct answer can be confirmed and a short, written, example of a real-world situation can provide relatable information that helps to reinforce the knowledge demonstrated. Additionally, gaps in understanding can be identified that may signal the need for additional communications or training.

Penetration testing (like simulated phishing attacks via email) is another method for communicating security awareness information in an organization. While the test itself does not qualify as a direct communication, sending the results of the penetration test to all employees will communicate necessary information while also showing them examples of how security awareness is a part of their job and impacts the company. These results can be delivered via email or a posted announcement in the office, and would detail any failures recognized, its impact to the company if it were a real attack, and provide information on how employees could prevent this in the future.

Finally, games are another method that can be used to communicate security awareness. These engaging activities would serve as a way to capture the attention of employees while also providing useful information that can be applied to protect themselves against attacks. Gamification has been shown to increase security awareness while also working to modify the behaviors of employees (Wood, 2014). This can serve as a great way to encourage participation in a topic that some may find dry or unengaging.

Conclusion

Security awareness is an important aspect of any company and is a crucial part of the security policy development and implementation process. By utilizing many methods of communication and analyzing the effectiveness of each one, critical information that can be used to protect the company and its employees can be more effectively communicated.

References

Fitzpatrick, V. (2010, April 26). Effective Communication Leads to Understanding. *SANS Technology Institute*. Retrieved from https://www.sans.edu/cyber-research/management-laboratory/article/fitzpatrick-mgt421

Wood, L. (2014, July 16). Boost your security training with gamification – really! *ComputerWorld*. Retrieved from http://www.computerworld.com/article/2489977/security0/boost-your-security-training-with-gamification-really.html