Security Awareness Paper

Jared Broyhill

University of Advancing Technology

Author Note

This paper was prepared for NTS435, taught by Professor Michael Vasquez.

Abstract

The purpose of this paper is to create and outline a plan for a fictional organization in order to establish and encourage a sense of awareness as it relates to that organization's security.

Security Awareness Paper

A security awareness plan’s goal is to inform relevant parties of active security risks against them and/or the organization they represent, and how best to address those risks and safeguard themselves against them. The outline will cover security from all aspects of the organization: physical and cyber. Additionally, the key parts that the plan addresses will be covered, as well as the benefits and drawbacks of creating a plan.

Key Elements and Questions

The primary ideas security practitioners must contend with one conceptualizing a security plan is what level of awareness they want employees to be at and what level of awareness is realistic for the employees to be at. Employees need to play a part in awareness if the organization is to be kept safe from threats, but at the same time it is unrealistic to put the expectation on employees for them to have the same awareness and concerns as a security expert. Additionally, the security concerns the average employee would be addressing would likely be limited compared to the total amount of concerns present. For example, a security plan would likely encourage employees to be vigilant of their fellow employees and whether or not they carry a proper identification badge or card. What a plan would not do (realistically) is to train employees on how to recognize whether or not the application another employee is using is malware or a hacking tool in disguise.

Key questions regarding a security plan would regard not only the contents of the plan but how the plan will be implemented in regard to training employees. Will employees simply be sent a one-time email upon employment? Will they be trained? If so, how regular will training be? These questions are vital and essential when addressing the security awareness level of any organization, and the security plan would have to include a level of planning as to how common the teaching of it will be towards employees. Additionally, the organization in charge of the plan would have to address when and how often to update the plan. Updating it often would leave some confused as to what is a risk this time around and what is not, while updating it rarely could cause it to fall behind and become outdated when trying to address the security risk of the modern day.

Issues Addressed

The security awareness the plan would seek to bring about would be typical of what is expected of a somewhat high-security organization. Employees would be trained to recognize basic social engineering tactics, when someone is not badging in at entry points, lacking an identification badge, etc. The other physical threats employees would be made aware of is when others are trying to get them to reveal classified information.

Cyber threats employees would be made aware of through the security awareness plan would be things such as recognizing malicious software, phishing attempts (all types), fake and suspicious websites, emails, addresses. They would also be taught to recognize techniques such as shoulder surfing, access with unauthorized devices (plugging in USBs and similar devices into machines without proper authorization), etc.

Benefits and Drawbacks

The clearest benefits of creating a security awareness plan for an organization is that it simply increases the organizations security; employees become more aware or risks, how to address them, and what they are. Drawbacks of the plan primarily revolve around logistics: how and when to update it, and decisions regarding what to include. Overall, the presence of a security awareness plan far outweighs the drawbacks.

References

No citations were used in this paper.