Chapter 4
Awareness

ABSTRACT

Awareness is a term used to describe an individual's knowledge of a topic. One would expect that awareness of the cybersecurity threat is well understood because of the continual reports of cyber incidents and attacks impacting individuals, organizations, and cyber-attacks on communities and states. The CIAS found it was true that people understood cyber incidents and attacks were happening. They also understood they needed to protect their assets and information, and they needed to be able to respond and recover from incidents that might occur. The significant gap was they did not understand all the impacts that could occur from a cyber incident, and they didn't understand the cascading impacts that could domino from a single attack. The lessons learned regarding awareness are incorporated into the awareness dimension of the CCSMM and include what each member of a community needs to know based on their role in the community.

INTRODUCTION

A security awareness program can be a valuable tool to ensure everyone understands the cyber threat and to reduce the amount of weaknesses that can be exploited by an attacker. Everyone needs to be aware of common threats, so that, at the very least, they do not become a victim of easier scams and phishing attempts. When addressing more sophisticated attacks, users can at least apply the knowledge acquired during training to mitigate the effects of the attack, gather the info necessary for security professionals to act and

DOI: 10.4018/978-1-7998-4471-6.ch004

know who to notify through the right channels. End users are an incredibly important aspect of a security program to reduce risks and to prevent cyber threats.

Security awareness programs often get scrutinized when determining their worth. The greatest argument against the awareness program is no matter how much training users receive; breaches that target end users are still occurring and continue to have a high success rate because people continue to be the weakest link in the cyber security chain. Often, it is also pointed out that there is a disconnect between the users' performance and ability to recognize threats in their behaviors and responses in a real-life environment. When designing a security awareness program and implementing a cybersecurity culture, the important aspect to focus on is not whether security awareness is worth it, but whether the program implemented is effective and really addresses the needs of the community.

Questions to think about include:

- Is the effort supported by leadership?
- Are awareness topics relevant to the individual based on their role in the community?
- Have we educated people on data breach prevention and response?
- Do people know who to contact if they discover a security threat?
- Do people know what constitutes a security threat?
- Do people understand the real value of data?
- Do we have regular training to keep the most current cyber threats known within the community?
- How do we know the awareness program is effective?

BACKGROUND

The community cybersecurity exercises, discussed in previous chapters, were used as a tool to not only assess the preparedness of the community in terms of how they would respond to a cybersecurity event, but it was also used as a mechanism to provide relevant awareness to the stakeholders in the community. Using the exercise as the catalyst, CIAS was able to introduce cybersecurity terminology, various types of cyber-attacks, show how each attack could impact a particular organization or sector, and the exercise injects were used to show the cascading effects a single cyber-attack could have on the greater community.