Chapter XX
Creating a Security Education,
Training, and Awareness
Program

Nick Pullman
Citigroup, USA

Kevin Streff
Dakota State University, USA

ABSTRACT

Security training and awareness is often overlooked or not given sufficient focus in many organizations despite being a critical component of a layered defense. Organizations often purchase expensive hardware and software to help secure their organization, but fail to allocate resources to train employees who will install and configure the product. Similarly, organizations will devote many hours developing policies and procedures to protect sensitive information, but fail to allocate the appropriate resources to ensure awareness of those policies and procedures. This chapter discusses how to design, create, and implement a formal security education, training, and awareness (SETA) program as a component of a layered defense strategy.

OVERVIEW

Kevin Mitnick, one of the world’s most famous hackers, wasn’t particularly skilled at exploiting technology, but was notoriously effective at social engineering; he tricked and persuaded individuals into disclosing sensitive information. Mitnick took advantage of individuals’ trusting nature by impersonating “trusted” individuals to perform reconnaissance for later attacks. The adage goes that a chain is only as strong as its weakest link, and many security experts would agree that the human element is the weakest link in information security (Hansche, Berti, & Hare, 2004). These
Creating a Security Education, Training, and Awareness Program

threats due to human failures are significant with the theft of intellectual property accounting for a loss of $59 billion a year from American companies (National Security Institute, 2007). A security education, training, and awareness program aims to mitigate the human risk in securing organizations and their assets. The core issue with organizations today, however, isn’t whether or not to perform security training and awareness, many organizations have some form of training and awareness, but how to implement a program that it is effective and efficient in providing the additional level of security that was intended.

A security education, training, and awareness (SETA) program is designed to mitigate threats due to human factors such as employees not being properly trained on a specific technology or not being aware of a security policy. There are many facets to information security and organizations tend to try and solve security issues with a technical bias; however, the reality is that humans are typically the first and last line of defense in protecting the organization. Technical-only solutions are insufficient as these defenses are installed and managed by individuals who if not properly trained could leave a system vulnerable to attack. In addition, employees use systems and applications on a daily basis so they are the most likely the first to identify issues or security breaches.

There are three pieces to understand with regard to security education, training and awareness:

• creating an overall security program,
• understanding SETA fundamentals, and
• creating the SETA program.

First, before beginning to create the SETA program, the organization must develop a comprehensive information security program. The overall security program details the approach that the organization will use to secure its assets. Next, the organization must understand the fundamentals behind a SETA program such as which topics are appropriate and what the best methods are for delivering the learning material. Finally, after the organization has an understanding of the appropriate topics, materials, and distribution methods, they can create the SETA program. This includes determining what the needs of the organization are, ensuring that there is an appropriate plan for designing and executing the SETA program, and following appropriate methods to implement and evaluate the SETA program. It is important for an organization to understand its overall security needs so that the SETA program can be developed to meet those needs. In addition, following a defined process for implementing and evaluating the SETA program will ensure that the program is effective, efficient, and continuously improving.

PEOPLE BASED SECURITY BREACHES

Information assurance is the process of protecting the confidentiality, integrity and availability of electronic systems and the information it stores, processes and transacts (McCumber, 2005). There are many different types of security incidents as it relates to compromising information, such as loss or theft of data, unauthorized changes, disclosure of sensitive information, and loss of system availability and these incidents could originate for a number of reasons such as viruses, hackers, insider abuse, and natural disasters. Technical attacks, such as remote exploits and malware, are important to defend against, but equally or more important are the human aspects of information security.

All individuals within an organization need to do their part in defending against information security attacks. Further, because many of the information security breaches are conducted or aided by internal personnel, all individuals need to be on the lookout for anything unusual that could