Chapter 33

Security Education, Training, and Awareness

Albert Caballero
HBO Latin America, Surfside, FL, United States

1. SECURITY EDUCATION, TRAINING, AND AWARENESS (SETA) PROGRAMS

Security Education, Training, and Awareness (SETA) is a program that targets all users in an organization to help them become more aware of information security principles as is appropriate for their jobs. Without a SETA program an organization runs the risk of easy infiltration by simple virtue of their employee's ignorance on how to securely perform basic IT tasks. A SETA program not only has the bottom-line effect of raising the difficulty for attackers to infiltrate an organization, but can also decrease cyber-risk insurance premiums, help meet regulatory standards, and set the tone for the secure business practices of an entire industry. All users have a responsibility to help secure the business and should therefore be given an opportunity to learn how to better protect themselves and their company's assets with appropriate information security training. It is important for every employee to understand their role in security, so the goal of a SETA program should be participation and motivation.

If implemented well, a SETA program is a continuum of training that begins with the most general for all users and becomes more targeted and in-depth depending on the role of each individual or group. The most basic level of a SETA program, and likely the most important, starts with awareness. Security awareness is the general information security training that is delivered to all users. The goal is to create a culture of security awareness across the entire organization and should therefore speak to all users focusing on individual accountability so that everyone maintains a certain level of skepticism when finding themselves in a situation that is unorthodox or out of the ordinary. It is these special exceptions and social manipulations that are typically leveraged by attackers to gain a foothold and some level of access from which to pivot and expand unauthorized access further into an organization. For example, something as simple as letting someone into the building without proper ID, clicking on a mail attachment that is not expected, or sharing your password with a coworker could end up being the demise of an entire business costing tens of thousands of dollars or more in recovery efforts. Fig. 33.1

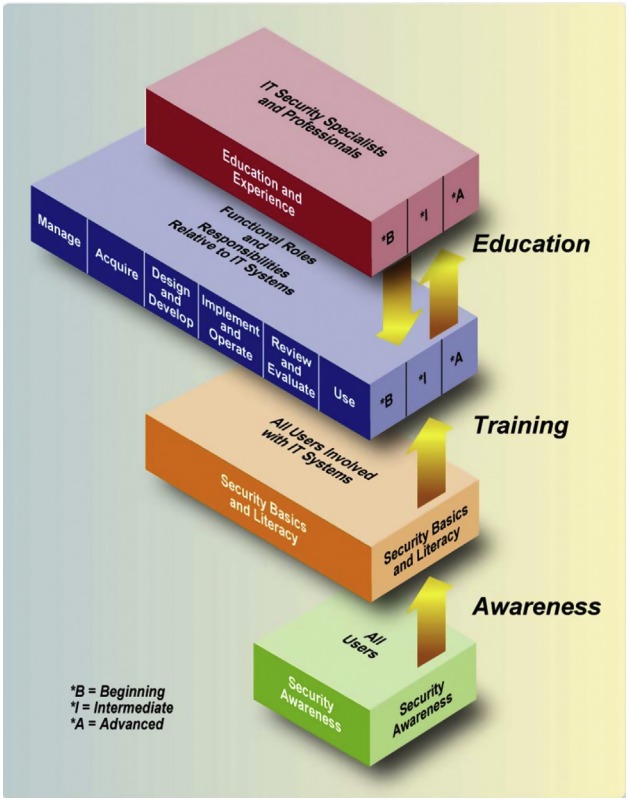

FIGURE 33.1 The IT security learning continuum.

Computer and Information Security Handbook. http://dx.doi.org/10.1016/B978-0-12-803843-7.00033-8

below describes the IT Security Learning Continuum according to the National Institute of Standards and Technology (NIST) [2].

The next level in a properly implemented SETA program is training. Security training is more targeted and tactical typically based on the responsibility of each employee and helps develop more advanced skills, increasing the understanding on how to securely perform their specific job functions. There are two methodologies by which to effectively deliver this type of security training: functional and skill-based. Functional information security training is specialized training based on the role of an employee. For example, a network firewall administrator will likely require training on the type of firewalls that are in production by any particular company such as Checkpoints, Palo Alto, or Cisco; whereas, an infrastructure administrator will likely need security training in Windows Active Directory and ITIL Change Management procedures—all critical aspects of running a safe computing environment. Skill-based training will take into account the current skill level (beginner, intermediate, or advanced) of the employee when delivering technical training. An individual that has been a firewall administrator for several years will likely benefit much from an advanced course in firewall hardening tactics whereas a person that may have had a security education but no real world experience will need to start at a beginner class that addresses basic management and implementation of the specific firewalls being administered. Ultimately, the higher the level of risk that individuals manage the higher the level of awareness and training they must be provided as depicted in Fig. 33.2 [2].

Many times this type of training requires a level of technical expertise that is not available within a typical organization so it is necessary to go outside of the company to institutions like SANS.org and ISC2 for advanced and highly technical information security training that can be delivered to small groups or individuals that need it, not to the entire organization as security awareness would be. Today, a Security Education is possible by enrolling in a formal curriculum that is purpose built to teach all the fundamental concepts required to build a career in information security. Many universities and colleges have begun to create curriculums that will offer bachelor's and master's degrees on information security. These degree programs are good for students that are fresh out of high school or adults which would like to retrain in this fast-growing field; however, many of these programs do little to expose students to real world information security practices. The most important aspect of developing a proper security education program should be to map to real world scenarios and job functions in areas that are in high demand. Some of these fundamentals areas of study should include:

- Information security and risk management
- Network communication analysis, design, and security
- Software development and embedded operating system (OS) security
- Ethical hacking and application security
- Social engineering and SETA
- Mission-critical infrastructure
- Identity and access management
- Digital and mobile forensics
- Data security standards and regulatory compliance
- Malware analysis and reverse engineering

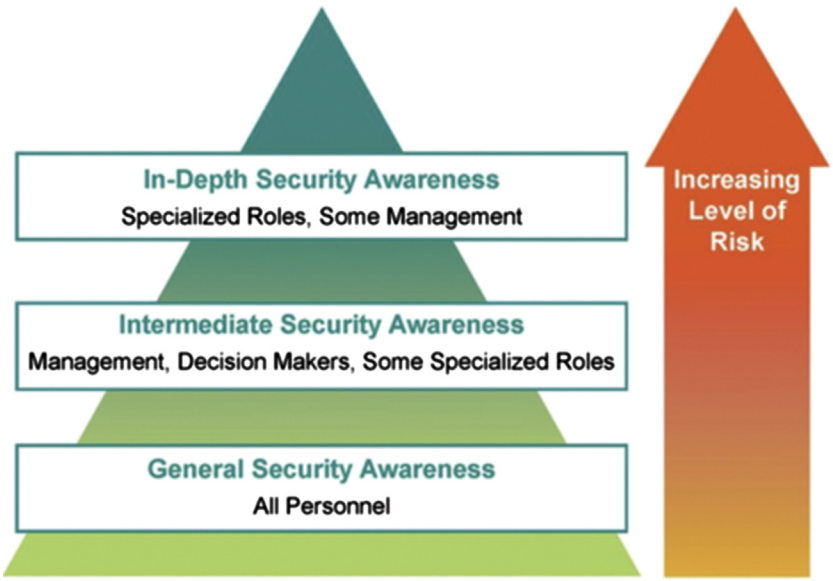

FIGURE 33.2 Depth of security awareness, training, and education.

2. USERS, BEHAVIOR, AND ROLES

Users in every organization are critical to the defense and protection of sensitive data and secure operations. No matter what technical controls are implemented from firewalls to intrusion detection systems it only takes one user clicking on the wrong link or tripping over the wrong wire and a true disaster or outbreak can occur. This is why all users need to have clearly defined roles and their behavior must be modified so as to think twice before taking an action that may lead to nefarious consequences. This can only be done with SETA. It is increasingly important throughout the SETA program to maintain user engagement high in order to raise morale and reward the appropriate behavior while discouraging risky behavior.

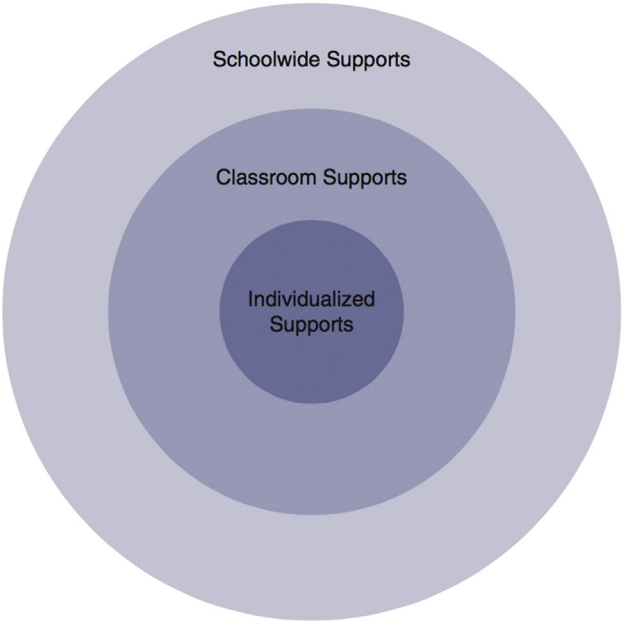

FIGURE 33.3 Behavior management planning.

Understanding user behavior and motivation is key to a successful SETA program. As a security professional it is necessary to be both an evangelist and a leader. To be an effective leader there is a need to implement proven techniques and strategies in modifying user behavior whenever possible. Although there are certain innate qualities present in most leaders there is also a training management process that should be understood and practiced to enhance leadership skills to more effectively influence the way users behave under certain circumstances. Behavioral management is an important aspect of this and needs planning that should occur at three levels. First, at an individualized level where support is provided one on one, which is most effective with users that have a high level of responsibility within the organization by way of managing other users (such as managers and executives) or by their administrative duties (such as network and system administrators). Next, there is classroom or group support, which can also be referred to as business units or departments depending on the organization. For example, the Human Resources department may have quite different security awareness needs than the Operations or Legal department. There should be customized training sessions based on these user groups that address their specific needs. Finally there is school-wide or organization-wide support, which addresses general security awareness topics that are common across the entire organization. Fig. 33.3 shows the levels to consider when planning a behavior management strategy in a classroom or business environment [4].

Defining roles and responsibilities is part of the best practices needed to understand how to best design and develop a SETA program that will engage the right people and encourage the desired behavior. As part of these best practices the Payment Card Industry Data Security Standards (PCI DSS) has defined the roles described in Fig. 33.4 below. This maps somewhat to the traditional

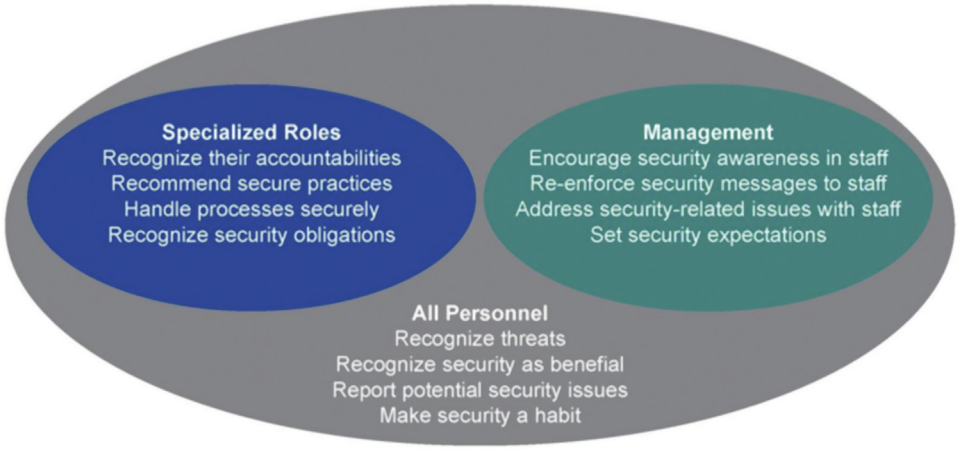

FIGURE 33.4 Security awareness roles for organizations.

behavioral management techniques used in higher education institutions. All personnel need to be able to recognize security threats and potentially risky behavior. Management needs to reinforce and support these initiatives, while security professionals need to understand what they are held accountable for and recognize their security obligations [6].

3. SECURITY EDUCATION, TRAINING, AND AWARENESS (SETA) PROGRAM DESIGN

The ultimate purpose of a SETA program is to change the behavior of users (and, this cannot be done without engaging them in a way that is memorable and effective), it is important that the design of the program be well thought out. For users to be engaged there needs to be a variety of training opportunities that are both interactive and innovative with a campaign that is all inclusive, in other words, does not leave anyone out. From managers and executives in any organization to temps and interns, security awareness is essential for designing and developing an effective SETA program.

Designing and developing a SETA program requires thought, organization, and planning making sure to keep the mission and culture of the organization in mind. To be successful it needs to support the business needs while making the users feel relevant and connected to the subject matter. During the design process the needs of the organization are identified and an effective, organization-wide program is developed. Without organizational buy-in, proper funding, and established priorities it becomes extremely difficult to implement a valuable program. While designing the program there are three major components to consider: policy, strategy, and implementation. Policy is extremely important and is typically centralized with requirements being established organization-wide and applying to all users. Depending on the organization there may be a need to have either a distributed or centralized strategy for implementation depending on the size of the organization, budget allocations, and geography of the users.

The training strategy typically benefits from customization based on the different groups needing training although there should be some consistency in the actual training material covered. Ideally, implementation will be highly customized and take into consideration not just the organizational culture but also that of the employee's region, department, and function. There are several different strategies available when creating a SETA program. One of these is a centralized training strategy where there is a top-down effect that can be effective, especially if there is support from upper management. If a centralized strategy is too difficult to implement due to organizational, cultural, or geographical differences then it would make sense to simply write a general policy for the entire organization and let each logical division handle the design and delivery of the material. This is most common where there are language barriers such as a multinational organization or multiple business units that have different core businesses such as a holding company. See Fig. 33.5 for an

FIGURE 33.5 Fully decentralized strategy and implementation.

example of a fully decentralized SETA program where each organizational unit has a high level of input into the design of the program [2].

Regardless of the strategy selected for implementation there always needs to be a central authority that authorizes, supports, and establishes executive support for the program. That being said, there is also the consideration that these types of training programs are not the core competency of most information security groups. The delivery of these types of programs are best designed and developed by the departments that are in charge of developing other training programs such as Human Resources, Risk and Compliance, or Employee Training, if they exist. There is also a large impact on an organization at the highest level if a committee or council of key stake holders is put together to support the initiatives put forth by the central authority. Having a team of individuals that have the power to implement significant change within an organization is crucial in maintaining strategic support and defining a direction that aligns with the goals of the organization. Information security training should follow the frequency defined below [1]:

- New hire orientation
- Initial security briefing within 3–6 months
- Refresher briefing every 3–6 months
- Termination briefing

4. SECURITY EDUCATION, TRAINING, AND AWARENESS (SETA) PROGRAM DEVELOPMENT

Once the design of the program has been approved the content will need to be developed and this will indeed involve more security staff. There is a significant amount of topics that can be selected for information security training but to overwhelm users is quite easy so the organization should typically begin with a short list of pertinent topics that apply to all users. Remember that security awareness is organization wide and it's not until we refer to security staff and some other types of technical personnel that we do not need to define the training and education piece or the program. Also, the security awareness portion because it needs to be general and applicable to every user it requires less in-depth expertise than other types of training and can usually be developed in house. Among the initial topics that are commonly chosen for developing material for are:

- Password security
- Email phishing
- Social engineering
- Mobile device security
- Sensitive data security
- Business communications

As part of the development of the program it is important to define the content that will be delivered but also develop some of the materials and collateral that will be used to help communicate the content. There are many different techniques that can be used to deliver an engaging security awareness program. The most effective is usually a combination of different techniques whereby creating a security awareness campaign that delivers propaganda and content in ways that are innovative, engaging, and all-inclusive. Some of the different materials and techniques that can be used include:

- Computer-based training
- Phishing awareness emails
- Video campaigns
- Posters and banners
- Lectures and conferences
- Regular newsletters
- Brochures and flyers
- Corporate events

5. IMPLEMENTATION AND DELIVERY

Implementing and delivering a SETA program effectively is critical to the security of every organization. As mentioned it only takes one user that is not aware of how to handle a malicious email or a social engineering phone call to cost an organization a tremendous amount of damage and money. How well a SETA program is implemented and delivered depends largely on the design and development of the program. Both design and development are key steps in the proper building of an effective program and if there are misfires in executive support, program design, or content development it can significantly hamper how much users learn. It is valuable to spend a good amount of time and emphasis on the corporate policy to make sure it is well-written and communicated correctly. Immediately after having figured out the language on the policy it helps to perform a needs assessment. A needs assessment before the implementation of the SETA program will likely bring to light some unexpected needs and improve the results of the program after and during implementation. Some of the steps involved in implementing any training program include:

1. Identifying program scope, goals, and objectives.
2. Identify the training staff and target audiences.
3. Motivate management and employees.
4. Administer, maintain, and evaluate the program.

When it is finally time to implement, communication is key. There should be a communication plan that is mapped to the overall strategy. When implementing the SETA program and communication plan it is important that it is delivered not just by topic but also by business unit, department, and geolocation. Regardless of the implementation techniques

Metric	Training Effectiveness Indicator
Operational Metrics	
Reduced system downtime and network or application outages	Consistent, approved change-management processes; fewer malware outbreaks; better controls
Reduction in malware outbreaks and PC performance issues related to malware	Fewer opened malicious e-mails; increased reports from personnel of malicious e-mails
Increase in reports of attempted e-mail or phone scams	Better recognition by personnel of phishing and other social-engineering attempts
Increase in reporting of security concerns and unusual access	Increased understanding by personnel of risks
Increase in the number of queries from personnel on how to implement secure procedures	Better awareness by personnel of potential threats
DLP scanning and network traces are active but not detecting cardholder data outside the CDE	Better understanding by personnel of potential threats
Vulnerability scans are active and detect high or critical vulnerabilities	Decrease in time between detection and remediation
Vulnerabilities are addressed or mitigated in a timely manner	Better understanding by personnel of potential threats and risks to sensitive information
Training Program Metrics	
Increase in number personnel completing training	Attendance tracking and performance evaluations
Increase in number of employees with privileged access who have received required training	Attendance tracking and performance evaluations
Increase in personnel comprehension of training material	Feedback from personnel; quizzes and training assessments

FIGURE 33.6 Metrics defining training effectiveness.

chosen, it is important to deliver the material in ways that take into consideration the following key aspects:

- Ease of use
- Scalability
- Accountability
- Industry support

After implementation there should be ways that feedback can be returned to the program managers. These feedback mechanisms can consist of traditional surveys during the delivery of the content, evaluation forms, focus groups, or a number of other methods. Defining key metrics that will help measure the effectiveness of the training is the final stage of implementation and can provide valuable information to keep the security program up to date and current. The table shown in Fig. 33.6 below is a good template that can be used as a starting point to define some powerful metrics for a SETA program [6].

6. TECHNOLOGIES AND PLATFORMS

In the effort to enable an effective SETA program, there are several technologies that can be leveraged to help in the process. One of the most effective ways of training personnel is with a behavioral management tool (see Fig. 33.7) such as ThreatSIM by Wombat Security, Phishme, or other Learning Management Systems (LMS) available from other vendors. ThreatSIM is a platform that allows administrators to measure and monitor the delivery of emails to users and can be used to craft fake phishing

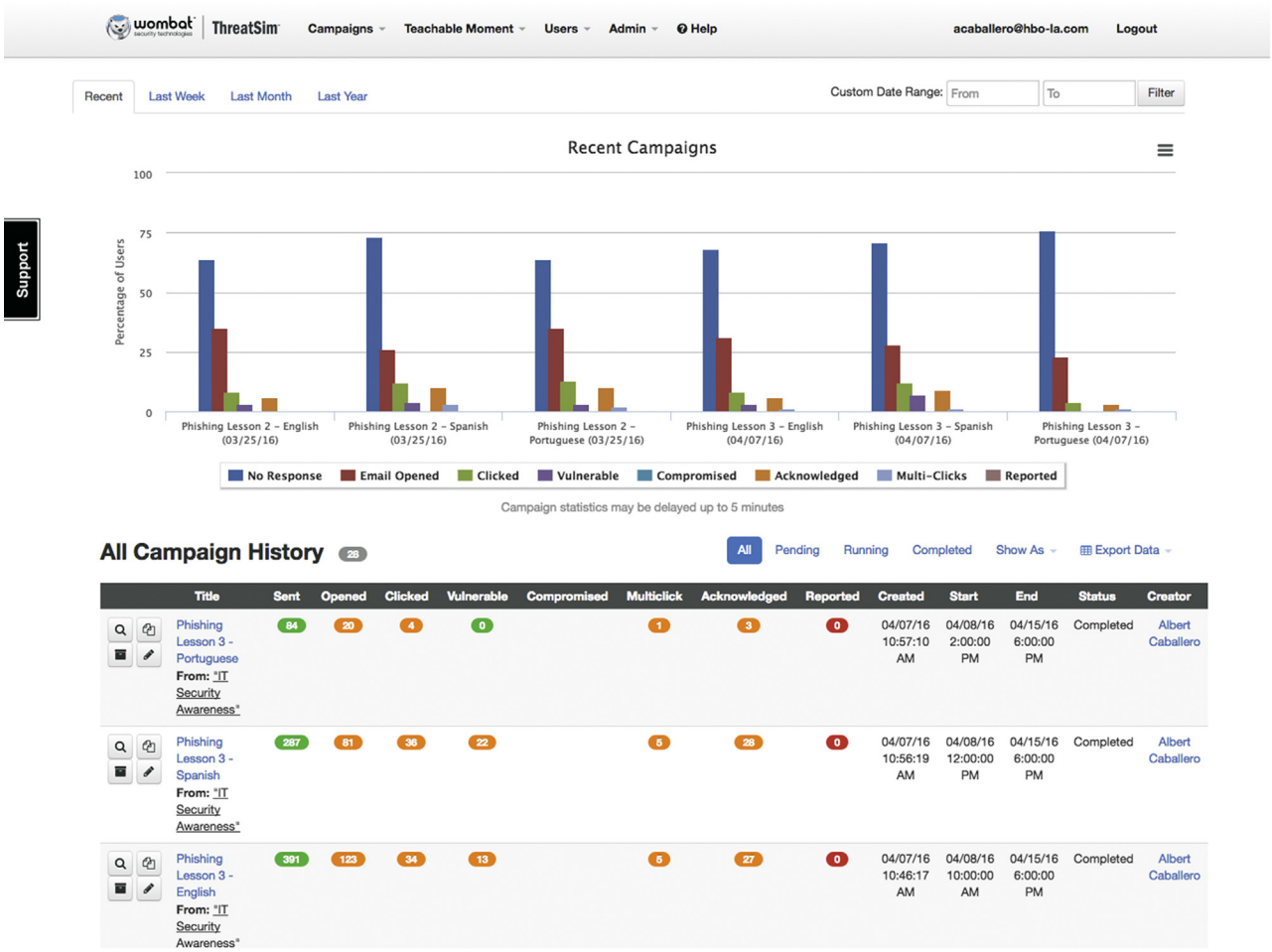

FIGURE 33.7 Behavioral management training platform.

emails that can be customized by department or region. This allows you to evaluate vulnerability to different threat vectors based on user groups and regions. It is also possible to deliver standard or customized teachable moments to employees who fall for mock attacks. This allows for brief, focused, just in time teaching with messages that focus practical guidance in avoiding future threats [7].

7. SUMMARY

A SETA program targets all users in an organization with programs specific to their positions, roles, and level of expertise to minimize the likelihood and impact of a security breach. Security education is the concept that information security personnel require higher education to be competent at their positions and to achieve a common body of knowledge that prepares them to enter the workforce. Security training is tactical and helps technology and operations staff receive highly specialized, formal training that helps everyone manage their roles and responsibilities better as well as be more effective at understanding their own accountability. Security awareness gets the word out to all personnel and helps everyone focus on building a security culture and a mature information security practice. The principal goal of a SETA program is that technology leaders, executive management, and all personnel get the appropriate security knowledge based on their roles and responsibilities (see checklist: " An Agenda for Action Plan for Other Important Goals of a Security Education, Training, and Awareness (SETA) Program").

Every aspect of security is a process, indicating that a one-time security briefing or training session will not suffice when attempting to implement real security. Ongoing and continuous training is part of any major endeavor. At the pace with which security breaches are increasing in number and sophistication it is necessary to adopt these methods when it comes to security training. Fig. 33.8 below describes an ongoing process that when implemented properly will help build a continuous training methodology that will be effective for a long time to come [7].

Now, let's move on to the real interactive part of this Chapter: review questions/exercises, hands-on projects, case projects, and optional team case project. The answers and/or solutions by chapter can be found in Appendix K.

An Agenda for Action Plan for Other Important Goals of a Security Education, Training, and Awareness (SETA) Program

Some of the other important goals of a SETA program should include at least the following key activities (check all tasks completed):

_____**1.** Increase awareness of the need to protect people, assets, and resources.
_____**2.** Develop the skills and knowledge necessary to perform jobs more securely.
_____**3.** Hold employees accountable for their actions by communicating security policy to all users.
_____**4.** Provide better protection of assets by helping employees recognize real and potential security concerns.
_____**5.** Improve morale by providing information that is personally useful, such as how to avoid scams, phishing, and identity theft.
_____**6.** Save money by reducing the number and extent of security breaches.
_____**7.** Motivate employees to improve their behaviors and incorporate security concerns into their decision-making.
_____**8.** Protect customer and corporate information by building a security culture.

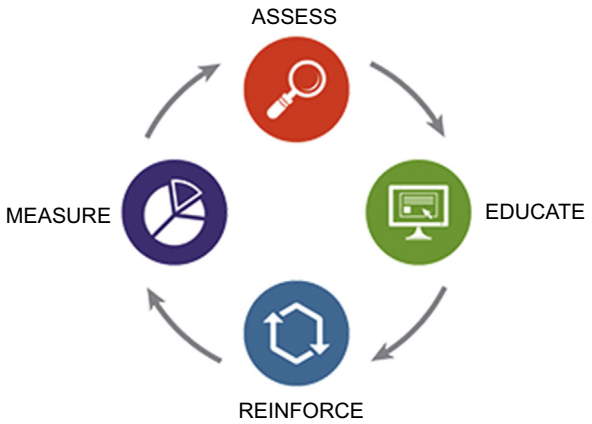

FIGURE 33.8 Continuous training methodology.

CHAPTER REVIEW QUESTIONS/ EXERCISES

True/False

1. True or False? Security Education, Training, and Awareness (SETA) is a process by which all users of an organization have an opportunity to enhance their knowledge of information security in an effort to protect themselves and organizational assets.
2. True or False? Security education is an informal curriculum created for the purpose of educating individuals in a broad array of security topics that will build a body of knowledge essential for a career in information security.
3. True or False? Understanding user behavior and motivation is key to a successful SETA program.
4. True or False? Because the ultimate purpose of a SETA program is to change the behavior of users (and, this can be done without engaging them in a way that is memorable and effective), it is important that the design and development of the program be well thought out.
5. True or False? Implementing a SETA program can only be as effective as the planning put into the design and development of the program.

Multiple Choice

1. One of the techniques used to deliver an engaging security awareness program includes?
   A. Username
   B. Password
   C. Validations
   D. Security systems
   E. Computer-based training
2. Regardless of the techniques chosen to deliver the material, which feature is maintained throughout each of the methods or techniques implemented?
   A. Attack
   B. Choking
   C. Ease of use
   D. Security
   E. Questionnaire
3. What platform allows administrators to measure and monitor the delivery of emails to users and can be used to craft fake phishing emails that can be customized by department or region?
   A. Devices
   B. ThreatSIM
   C. Data
   D. Backups
   E. All of the above
4. What concept is required by information security personnel that requires higher education to be competent for their positions and to achieve a common body of knowledge that prepares them to enter the workforce?
   A. Security education
   B. Private plan
   C. Secure plan
   D. Virtual plan
   E. All of the above
5. What gets the word out to all personnel and helps everyone focus on building a security culture and a mature information security practice?
   A. Monitoring
   B. Securing
   C. Governing
   D. Security awareness
   E. All of the above

EXERCISE

Problem

How do you go about developing a security education training and awareness (SETA) program?

Hands-On Projects

Project

Where can you find existing security awareness training that your employees can take?

Case Projects

Problem

What type of cyber security training is available in order to brush up on your security knowledge and skills?

Optional Team Case Project

Problem

How can you improve the SETA program in your organization?

REFERENCES

[1] Department of Homeland Security Management Directive System, Security Education, Training, and Awareness Program Directive, 2004. https://www.dhs.gov/sites/default/files/publications/mgmt_directive_11053_security_education_training_and_awareness_program_directive.pdf.

[2] M. Wilson, J. Hash, Building and Information Technology Security Awareness and Training Program, National Institute of Standards and Technology, 2003. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

[3] Deleted in review.

[4] R.C. Martella, J.R. Nelson, N.E. Marchand-Martella, M. O'Reilly, Comprehensive Behavior Management: Individualized, Classroom, and Schoolwide Approaches, SAGE Publications, Inc., 2012, pp. 2–5.

[5] Deleted in review.

[6] Security Awareness Program Special Interest Group – PCI Security Standards Council, PCI Data Security Standard (PCI DSS) 1.0, 2014. https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf.

[7] Wombat Security Technologies Website, 2016. https://www.wombatsecurity.com/.