tracesecurity

Practical, worry-free cybersecurity.

WHITE PAPER

Information Security Awareness Training

Effective Curriculum Development

Nathan Turner

TraceSecurity Information Security Analyst

Executive Summary

Information Security is a general term used to describe the measures an organization takes to protect the confidentiality, integrity and availability (CIA) of sensitive or confidential information. Information security awareness training is an essential element of any organization's information security program. Its purpose is to equip staff with the knowledge necessary to help protect the organization's assets, including client and personnel information. However, some information security awareness training programs barely provide the necessary information to be considered an effective means of ensuring employees understand not only how to protect the organization's information but why it is important to protect that information. According to a Forrester Research, Inc. report "Reinvent Security Awareness To Engage The Human Firewall" published December 17, 2014, "One false step by a single employee can have devastating effects on an organization." The report continues to say lackluster and informal security awareness programs today are commonplace, and only 22% of information workers are concerned about security at their companies.

This white paper provides an overview of how organizations can develop effective curriculum for information security awareness training programs.

Information Security Awareness

Some organizations are beginning to recognize the value of information security awareness training, and as a result, are implementing formal training programs that include sound curriculum and ongoing training for all employees. These programs typically incorporate topics not only related to physical security but also technical security. Basic topics are often assigned to all employees, while supplementary topics are assigned to specific staff members based on their roles and responsibilities within the organization. For instance, in addition to standard information security training, employees with security-related roles, such as information security officers and compliance officers, generally receive compliance and regulatory training and certifications.

While many organizations understand the importance of information security awareness training, others disregard the value in administering a formal training program. These organizations may only provide security awareness training to new employees as part of their orientation, or perhaps only pick a topic or two to disseminate to staff on occasion, but refrain from offering training on an ongoing basis.

Then there are those organizations that simply fail to offer any type of information security awareness training. While these scenarios are less than ideal and may be due to the organization's opinion of necessity, a lack of knowledge within the organization as to what it takes to provide effective information security awareness training could be the culprit as well.

Training may not be the silver bullet to preventing information security incidents, but it can certainly help employees understand their role in protecting information assets and preventing the unauthorized exposure of sensitive information.

Designing Effective Training

The first step to creating an effective training curriculum is to determine the content. Implementing a sound information security awareness training program requires organizations either create or locate courses that cover several common or basic information security awareness topics. For example, social engineering attacks, email and messaging threats, Web browsing threats, social networking threats, mobile device security tips, secure password tips, and physical security tips, among others. In most cases, it is not necessary for all employees to receive the same training; however, most, if not all, employees should participate in the basic training courses. How much training an employee receives should be determined based on their role within the organization and their ability to provide physical and technical access to sensitive information. For example, facility maintenance and cleaning staff are often overlooked when it comes to training, but physical access capabilities combined with a lack of training could potentially make these individuals soft targets for social engineering attacks.

Additional security awareness training courses should be assigned to employees with critical roles and responsibilities related to protecting sensitive information. This includes employees with access to the data and those responsible for securing the physical and technical environments where the data is housed. These employees should participate in additional training that

covers topics such as data security tips, data destruction tips, and any regulated data handling requirements. Of course, this group should also include the IT staff responsible for implementing and managing the secure configuration of systems and the network environment.

As previously stated, special training that includes compliance and regulatory certifications should be provided to employees in security-related roles. In addition to receiving training for information security credentials, these individuals should also receive training on new and trending information security threats. If designated and certified individuals are not on staff, the organization should consider hiring someone with these credentials or designating and training at least one employee to fulfill these roles. The purpose of security-related roles is to help create and maintain a firm information security program as well as create or locate an effective training curriculum tailored to the organization's specific needs. If the organization chooses not to or is unable to create an information security awareness training program that includes engaging and relevant content, a third-party vendor should be selected to perform onsite training or deliver an online training program.

In addition to general information security awareness training courses, a review of the organization's information security policies and procedures should be included in the curriculum. The purpose of information security policies and procedures is to establish guidelines for handling sensitive information and identify the minimum safeguards that will be utilized to protect sensitive information and the corresponding technical and physical environments from unauthorized access, disclosure, corruption or destruction. At a minimum, the organization's security requirements should conform to the compliance and regulatory requirements associated with the data. Basic policies and procedures, such as the Acceptable Use Policy, Code of Ethics, and Incident Response, should be reviewed by all employees. Review of additional, more advanced policies and procedures should be assigned based on job function within the organization.

Once the information security awareness topics have been established, the next step to creating an effective training curriculum is to determine when and how often to administer training. Employees should be provided with security awareness training material during the initial hiring period and exposed to ongoing training that addresses new threats and includes reminders of common threats. Routine training helps keep security awareness topics and the organization's security requirements and processes top-of-mind for employees. It is recommended that organizations implement a formal security awareness training program that, at a minimum, includes annual training.

Conclusion: Close the Education Gap

While a small group may argue the necessity of information security awareness training, most agree the importance of such training should not be dismissed. Information security breaches due to employee error are common and demonstrate the critical role training plays in defending against data security threats. Some examples of human error related threats include data theft due to lost or stolen mobile electronic/computing devices that do not include recommended security configurations, system or network breaches due to spear phishing and other social engineering attacks, and information disclosure due to insecure data disposal. Establishing a sound information security awareness training curriculum requires that organizations identify training topics, find training resources, and establish training schedules tailored to job function. Finally, by reinforcing training with periodic and timely updates throughout the year, organizations can help ensure employees are better equipped to not only recognize security threats but take appropriate steps to minimize the risk of a security breach.

About TraceSecurity

TraceSecurity is a leader in cloud-based cybersecurity solutions that help organizations of all sizes reduce the risk of cyber breaches and demonstrate compliance. TraceSecurity's award-winning TraceCSO is a revolutionary solution that dramatically streamlines the management of IT governance, risk and compliance (GRC) programs. It accomplishes this by tightly integrating and automating all eight critical IT GRC components: Risk Management, Compliance Management, Audit Management, Vendor Management, Incident Response Management, Vulnerability/Patch Management, Policy Management and Training Management. Most important, it provides built-in security and compliance expertise that most organizations lack. Because of its unique architecture and cloud delivery, TraceCSO deploys rapidly and reduces the cost of GRC management by as much as 80%.

With market experience that spans over 2,000 customers, TraceSecurity offers the insight, products, professional services and partners to support the security and risk management efforts of organizations of all sizes across all industries.