INDUSTRY BRIEFING

Security Awareness

Best Practices for Implementing Security Awareness Programs

Smart security awareness programs help organizations reduce threat risk by getting every employee rowing in the same direction.

Organizations of all sizes across the globe are being targeted and attacked by hackers and cyberterrorists. Multiple studies show that small and medium sized organizations are easy targets for cyber attacks such as Phishing. In order for organizations to become more secure, many are deploying or revamping cybersecurity employee awareness training, internal policies, monitoring technologies and full-time resources.

A Security Awareness Program is critical for any organization that is trying to reduce its risk by educating employees on the latest threats and attack techniques that the organization is facing.

How to Begin

The first step in increasing security awareness within an organization is to design and develop a formal security awareness program. The organization's leadership should assign the responsibility for developing, delivering, and maintaining the program to a cross-functional group of individuals from different areas of the organization.

At a minimum, two departments should be involved; the Information Security (or Information Technology if no Information Security department exists) and Human Resources departments.

Why Involve Multiple Departments?

When developing and implementing security awareness programs, multiple groups should be involved in the process since each brings a unique set of experiences and perspective into the process and program.

The Information Security (or Information Technology) department has security experience and/or expertise. Information Security groups are often the most informed employees on the latest attack techniques and threat types that the organization is facing, and can provide the content to update or create training resources and materials.

In organizations where no Information Security group or function exists, the Information Technology group is often the most educated or aware of security attacks and threats and can provide content and input on training and awareness materials and program resources.

A cross-functional security awareness team can ensure that an effective and current security awareness training program is delivered to the workforce, helping to reduce the organization's risk of breach or data loss.

cStor
We look beyond IT

Security Awareness Industry Briefing

The Human Resources department is a critical group to include when creating a security awareness program as this department in most organizations is the creator and enforcer of personnel and organizational policies, including employee training and development. The Human Resources group and personnel have experience managing and overseeing the process of employee training, tracking policy or regulatory compliance among the employee population and maintaining records of required training sessions.

Program Delivery

Security awareness program content distribution should not be limited to only a single population within the organization, but delivered to multiple groups, in order to create the biggest impact or reduction of risk, and a return on invested capital.

For example, the workforce might consist of full-time, and part-time employees. It might also consist of 1099 sub-contractors or workers that are sponsored or paid for through a 3rd party partner. Each of these workforce populations should receive the same general security awareness training content to ensure a basic knowledge and understanding of security attacks and threats is established within the workforce.

PROGRAM DESIGN

Security awareness training programs include common attributes such as:

- Security Awareness & Phishing Assessments
- Phishing Simulations
- Phishing Reporting
- General Security Awareness Training
- Compliance Awareness Training
- Training Completion Tracking & Reporting

Other attributes can include:

- Department Specific Training
- LMS Integration
- Incentive & Reward Programs

Security awareness training content delivery channels that can be used include formal training, computer based training, e-mails and circulars, memos, notices, bulletins, posters, and even Phishing simulations.

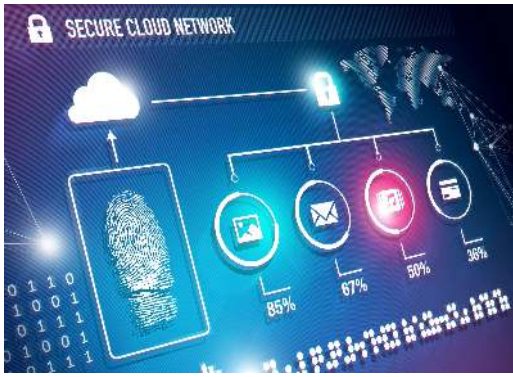
It is critical that security communication is distributed frequently and that a closed loop process is in place to enforce appropriate behavior. It might be difficult for an organization to provide formal training weekly to the workforce, but it can send weekly security emails on how to recognize and deal with the latest threats being launched at the organization. Enabling the workforce occurs through informing via security updates in a consistent and effective manner.

Security Awareness Program Topics

- Understanding impact of unauthorized access
- Security requirements for payment environments
- Who to contact and steps to protect Card Holder Data (CHD) and what steps to take to protect CHD
- The importance of strong passwords
- Secure e-mail practices
- How to recognize a Phishing e-mail
- Secure practices when working remotely
- Tips to avoiding malicious software
- Secure browsing practices
- Delegation of authority (how and when to transfer money, grant system access, share information)
- How to secure mobile devices
- Social media usage best practices
- How to report security incidents and identify incident response team personnel
- Avoiding social engineering attacks (in person, phone, e-mail, IM)
- A secure physical environment including visitor handling procedures
- Avoidance of shoulder surfing
- Secure disposal of documents, assets
- How to inspect point-of-sale (POS) devices for tampering (new requirement in PCI DSS 3.0)
- Challenge unauthorized personnel and report suspicious activities immediately
- Security training attendance tracking and/or security training individual test scores

Security Awareness Industry Briefing

Program Content is obtained from various resources, vendors and associations that publish standards and best practices. Training modules include the company's policies.



Sourcing Program Content

Below is a list of security training content sources to consider when developing security awareness programs:

- To cover PCI requirements 1 and 2, content for training materials could be obtained from the vendor documentation, the organization's policies, and the following industry standards and best practices for network and systems security: NIST, ISO, CIS, HIPAA.
- To cover PCI requirements 3 and 4, content for training materials could be obtained from the vendor documentation, the organization's policies, and industry standards or regulations related to the protection of consumers' private information: GLBA, SOX.
- To cover PCI requirements 5 and 6, content for training materials could be obtained from the vendor documentation, the organization's policies, and the following industry standards and best practices: PCI DSS, OWASP Top 10, CWE/SANS Top 25 most dangerous software errors, NIST, COBIT 5, CIS.
- To cover PCI requirements 7, 8 and 9, content for training materials could be obtained from the vendor documentation and the organization's policies.
- To cover PCI requirements 10 and 11, content for training materials could be obtained from the vendor documentation, the organization's policies, and industry standards or regulations related to sensitive data: NIST, ISO, GLBA, SOX, National Vulnerability Database, SANS CWE Top 25.
- To cover PCI requirement 12, content for training materials could be obtained from the organization's policies and industry standards or regulations related to background checks, privacy, and information security policies: FFIEC, SOX, HIPAA, NIST, ISO.

Why cStor Security Solutions Powered by Terra Verde

Security Awareness Programs offer a comprehensive solution to help address risk and vulnerabilities as well as help you:

- Deploy a repeatable, scalable set of standards, practices and a "program" for security alert monitoring, management and remediation.
- Reduce overall security and compliance risk.
- Reduce and eliminate capital expenditures for security technology and personnel.
- Deploy a new, or optimize an existing, Security Operations Center.

About cStor

cStor helps companies strategize, create, and implement security, data center and cloud solutions that address the business needs and demands of today's successful enterprise.

Powered By TERRA VERDE

cStor We look beyond IT

info@cStor.com
www.cStor.com
1.877.CSTOR.81
(1.877.278.6781)