The need for Security Awareness

Today, you need to protect not only against traditional security threats like hacking and exploitation of software vulnerabilities, but also against risks related to data breaches caused by internal negligence, and damage resulting from outside attacks targeted at your mobile devices. The best method of defense against these security threats is security awareness training. In addition, compliance and governance regulations, like the Sarbanes-Oxley Act and the Payment Card Industry Data Security Standard, mandate such training.

Negligent employees are the most common causes of data breach. The average consolidated total cost of a data breach is $3.8 million, representing a 23% increase since 2013. The cost incurred for each lost or stolen record containing sensitive and confidential information increased six percent from a consolidated global average of $145 to $154.¹ A top preventative measure aimed at reducing this is employee training and awareness programs.

Major Causes of Data Breaches ²

The need for proper training, IT policy development, and continuous education is amplified by evolving technology trends and the resulting security threats. For example, companies are seeking the proper balance between social media's advantages and the dangers posed by increased exposure of potentially sensitive information. Organizations that allow employees to utilize social media in the workplace need to develop comprehensive best practices and an IT policy to protect employee privacy as well as company data. A poorly trained workforce significantly increases the risk of loss and disclosure of vital data such as social security numbers, bank account details, and corporate IP. The immediate costs of these losses—the size of fines and compensation to individuals—grab the headlines. But the largest impacts are the loss of reputation and trust, damage to an organization's brand, and erosion of its customer base. Security-conscious companies realize that an effective security awareness program that touches all employees is as important as your firewall in defending against data breaches. Because such breaches can be addressed with training in appropriate security behavior, most government standards, regulations, and laws covering corporate governance, privacy, and security best practices mandate that organizations provide employee security awareness training and show evidence thereof for compliance audits.

Symantec™ Security Awareness Program overview

Symantec supports a risk management approach to help organizations mitigate risk through an effective security awareness program. The program:

- Promotes proactive employee behavior to better protect information
- Meets regulatory requirements specific to employee security awareness training

¹ Ponemon Institute, LLC 2015 Annual Study, “2015 Cost of Data Breach Study”
Web-based Training

The Symantec™ Security Awareness Program provides a programmatic approach that includes comprehensive web-based training and communication tools to help companies meet regulatory requirements specific to employee security awareness training. This can help reduce vulnerabilities by creating an informed corporate culture, to influence employees to protect an organization’s critical information assets from exploitation, cyber-attacks, unauthorized access, and fraud. The program is designed not only to increase security knowledge and understanding, but also to influence appropriate employee behavior at all levels.

The web-based training describes the importance of information security, promotes the understanding of information security principles, the awareness and reality of threats and vulnerabilities, and the application of security best practices to your environment.

Lessons in the web-based training include:

**Lesson 1**: Information Security, Responsibilities, and Principles—Defines information security, explains why it’s important, who is responsible, and how to classify and respond to incidents.

**Lesson 2**: Threats, Vulnerabilities, and Countermeasures—Provides an awareness of the threats and vulnerabilities to which information is subject, along with the countermeasures, objectives and techniques used by hackers to gain information.

**Lesson 3**: Securing Your Working Environment—Identifies security best practices and how to apply them in the workplace and in home offices. Also covers securing passwords and emails, and exchanging information securely.

**Lesson 4**: Security While Traveling—Describes how to secure communications when on the road, including what to do before you leave, how to maintain security while on the move, and in offsite locations.

**Lesson 5**: Protecting Information on the Internet—Demonstrates how to protect information in the cloud, increases awareness of advanced persistent threats and provides web browser best practices.

**Lesson 6**: Social Media Awareness—Explains the benefits and risks of social media and how to use it safely.

**Lesson 7**: Mobile Device Security—Covers mobile device threats, safety and best practices, as well as “bring-your-own-device” threats, safety and policies.

The following modules are available separately:

**PCI-DSS**—Describes the Payment Card Industry Data Security Standard requirements that must be enforced when a Primary Account Number (PAN) is stored, processed, or transmitted, regardless of the media. Most organizations that handle credit cards for payment will need to adhere to this standard.

**HIPAA and HITECH**—Introduction to the security and privacy requirements of medical patient information, including procedures for protecting patient data, types of violations and reporting requirements, and resources to assist with HIPAA- and HITECH-related privacy and security matters.

**Information Privacy**—Defines personal information, describes how personal information is collected and used, and illustrates best practices for maintaining the security of personal information.

Each web-based training module concludes with an assessment to measure employee understanding. The trainings are available in Shareable Content Object Reference Module (SCORM) compliant training modules that are ready to be published to an organization’s SCORM 1.2 compliant Learning Management System (LMS) for tracking, reporting, and audit purposes.
Communications materials

An effective security awareness program requires on-going communications to help reinforce knowledge received from the trainings. Communication materials provided within the Security Awareness Program include:

- Ready to print posters (11”x17” and 2’x3’ sizes)
- Ready to print reminder cards
- Email templates to remind employees of the security best practices
- Short animated videos

Customization services

Symantec provides flexible content customization services to tailor the content to your organization’s specific needs, including branding the content with your logo. Customers can modify the additional resource link in the training modules to reference their own security policies and procedures and other relevant information.

Why Symantec™ Education for security awareness training

A successful security awareness program influences attitudes and behavior. It instills and reinforces security best practices so that they become habitual in daily tasks and interactions. It must:

- Promote employee awareness that they are responsible for organizational security.
- Teach the security principles for which employees are responsible.
- Raise employee awareness of the threats to which the organization is vulnerable.
- Teach how to apply the security principles to everyday tasks.
- Remind, refresh, and update the security principles and best practices learned.

As a recognized global leader in security intelligence and security training, Symantec is uniquely positioned to help organizations raise security awareness.

Why Symantec

Symantec's position as the industry leader in security is the result of 25 years of research, development, and delivery of market-leading technologies in use by 99 percent of the Fortune 500. Symantec is recognized as a technology and market share leader in over a dozen categories by Gartner, Forrester, and IDC. Symantec holds over 1,200 patents in its global patent portfolio. Symantec’s Global Intelligence Network:

- Holds more than 66,400 vulnerabilities in the Symantec vulnerability database
- Has five million decoy accounts in the Symantec Probe Network
- Gathers data from 8.4 billion emails per month
- Has more than 57.6 million attack sensors in 157 countries

Symantec’s unmatched global intelligence of the evolving security threats and trends serves as the foundation for its products and services.

More Information

Visit our website www.symantec.com/training
Or email: americas_education@symantec.com

To contact Product Specialist outside the U.S.

For specific country offices and contact information, please visit our website.

Europe, Middle East, Africa –
edu_sales_emea@symantec.com

Asia, Pacific, Japan –
apj_education@symantec.com

About Symantec

Symantec protects the world’s information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: www.symantec.com/social

Symantec World Headquarters
350 Ellis St. | Mountain View, CA 94043 USA
www.symantec.com