Awareness Training as a Requirement for Security Regulation Compliance

Awareness Training & Compliance

Training is as necessary as Firewalls and Antivirus

Employee Security is a Requirement for all Companies.

Here is an abbreviated list of security regulations and the requirements for security awareness training (including phishing). Training is not just a good idea for all companies to ensure the forgotten weakest link (employees), but a requirement for anyone that is regulated.

HIPAA

45 CFR § 164.308(a)(5)

(5)(i) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).

GLBA

Training under GLBA is required via its Safeguards Rule, 16 CFR 314.4. "Train staff to recognize and respond to schemes to commit fraud or identity theft, such as guarding against pretext calling; Provide staff members responsible for building or maintaining computer systems and local and wide-area networks with adequate training, including instruction about computer security; and Train staff to properly dispose of customer information."

Payment Card Industry Data Security Standard (PCI-DSS)

PCI-DSS 12.6 – Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
PCI-DSS 12.6.1 – Educate personnel upon hire and at least annually.
PCI-DSS 12.6.1.a – Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web based training, meetings, and promotions).
PCI-DSS 12.6.1.b – Verify that personnel attend awareness training upon hire and at least annually.
PCI-DSS 12.6.2 – Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy.

Federal Information Security Management Act (FISMA)

FISMA, 4 U.S.C. § 3544, requires federal agencies to establish a security awareness training program. The program must include contractors and "other uses of information systems" that support the agency. The program must address information security risks and each employee's responsibilities in complying with agency policies and procedures to minimize security risks.

Why eSecurity Solutions?

- Security Experts for over 14 Years
- Complete Compliance Level Solutions
- Compliance Certifications
- Top tier vendors Partners
- Broad customer base

Contact us for a quote or information today:

886-661-6685

sales@esecuritysolutions.com
www.esecuritySolutions.com
Managed Services Line

ISO/IEC 27002

Section 8.2.2 Information Security Awareness, Education, and Training

All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

NIST Special Publication 800-53 (Revision 4)

AT-1 SECURITY AWARENESS AND TRAINING POLICY & PROCEDURES

1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
3. Reviews and updates the current:
4. Security awareness and training policy [*Assignment: organization-defined frequency*]; and
5. Security awareness and training procedures [*Assignment: organization-defined frequency*].

AT-SECURITY AWARENESS TRAINING

Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

1. As part of initial training for new users;
2. When required by information system changes; and

AT-3 ROLE-BASED SECURITY TRAINING

AT-4 SECURITY TRAINING RECORDS

AR-5 PRIVACY AWARENESS AND TRAINING

Banks & Credit Unions (FFIEC/FDIC)

Section II.C Risk Mitigation subsection II.C.7(e) User Security Controls-Training

Training ensures personnel have the necessary knowledge and skills to perform their job functions. Training should support security awareness and strengthen compliance with security and acceptable use policies.

Training materials for most users focus on issues such as end-point security, log-in requirements, and password administration guidelines. Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through e-mail or removable media, or unintentional posting of confidential or proprietary information on social media. As the risk environment changes, so should the training.

It is clear that all companies need security training including all regulated companies. Call us today to discuss how we can help with your employee security awareness training needs.

Contact us for a quote or information today:

886-661-6685

sales@esecuritysolutions.com
www.esecuritySolutions.com
Managed Services Line