SECURITY COMPLIANCE REQUIREMENTS

Overview

The purpose of this document is to provide an overview of the various standards and legislations that require security awareness programs.

ISO/IEC 27001 & 27002

§8.2.2 - *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.*

- Best-known standard in the family providing requirements for an information security management system (ISMS).
- An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

PCI DSS

§12.6 - *Make all employees aware of the importance of cardholder information security.*

- *Educate employees (for example, through posters, letters, memos, meetings and promotions).*
- *Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures.*

Federal Information Security Management Act (FISMA)

§3544.(b).(4).(A),(B) - *Securing awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities; and their responsibilities in complying with agency policies and procedures designed to reduce these risks.*

Gramm-Leach Bliley Act

§6801.(b).(1)-(3) - *In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical and physical safeguards:*

- *To insure the security and confidentiality of customer records and information;*
- *To protect against any anticipated threats or hazards to the security or integrity of*
- *such records;*
- *To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.*

Health Insurance Portability & Accountability Act (HIPAA)

§164.308.(a).(5).(i) - *Implement a security awareness and training program for all members of its workforce (including management).*

Red Flag Rules

§16 CFR 681.1(d)-(e). Employees should be trained about the various red flags to look out for, and/or any other relevant aspect of the organization's Identity Theft Prevention Program.

CobiT

§PO7.4 Personnel Training - *Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organizational goals.*

§DS7 - *Management of the process of Educate and train users that satisfies the business requirement for IT of effectively and efficiently using applications and technology solutions and ensuring user compliance with policies and procedures is: […] 3 Defined when a training and education program is instituted and communicated, and employees and managers identify and document training needs. Training and education processes are standardized and documented. Budgets, resources, facilities and trainers are being established to support the training and education program. Formal classes are given to employees on ethical conduct and system security awareness and practices. Most training and education processes are monitored, but not all deviations are likely to be detected by management. Analysis of training and education problems is only occasionally applied*

NERC CIP

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standard. §CIP-004-3(B)(R1) - *The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:*

- *Direct communications (e.g., emails, memos, computer based training, etc.);*
- *Indirect communications (e.g., posters, intranet, brochures, etc.);*
- *Management support and reinforcement (e.g., presentations, meetings, etc.).*

US State Privacy Laws

Many states in the United States have their own individual privacy laws. You can find a listing of most of those state privacy laws at the Morrison & Foerster's Privacy Library. Many of these privacy laws require some type of awareness training, or at a minimum that the privacy requirements are communicated to employees in that state.

EU Data Protection Directive

The European Union has directed all European member countries to develop and define laws regarding the protecting of personal privacy of the citizens of their respective country. While each country's implementation of this directive is different and unique, many of them require security awareness training to educate people on how to protect individual privacy.

References

- http://en.wikipedia.org/wiki/ISO_27001
- http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
- https://www.pcisecuritystandards.org/security_standards/documents.php
- https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf
- http://en.wikipedia.org/wiki/FISMA
- http://en.wikipedia.org/wiki/Gramm-Leach-Bliley_Act
- http://en.wikipedia.org/wiki/Hipaa
- http://en.wikipedia.org/wiki/Red_Flags_Rule
- http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
- http://www.NERC.com/files/ CIP-004-3.pdf
- http://www.mofo.com/privacy--data-security-services/