



INFORMATION SECURITY AWARENESS TRAINING

EXPERTISE FOR THE NEW AGE OF INFORMATION RISK MANAGEMENT

COURSE CURRICULUM

Our Security Awareness Training program is designed to educate your employees on general information security principles. These training modules are available to you and your staff online 24 hours a day, from any location with an Internet connection. In addition to a rich, multimedia virtual classroom training, we include online testing (the results of which can be used to demonstrate due diligence and provide an audit trail for regulatory compliance).

SA301: INTRODUCTION TO INFORMATION SECURITY

This course is designed to provide an introduction to concepts such as: information asset classification, information security policy, ISO17799 security framework, cyber crime, the layered security approach, and other topics that will familiarize students to a corporate environment that places high value on their information asset protection program.

SA302: SOCIAL ENGINEERING AND COMPROMISE

This course introduces the dangers of social engineering and compromise used in malicious attacks against information assets in an enterprise. Introducing concepts such as "dumpster diving", "dialing for dollars" and data mining, the course is designed to assist in recognizing social engineering attempts and to develop appropriate countermeasures.

SA303: ELECTRONIC PRIVACY IN THE CORPORATE ENVIRONMENT

This course deals with the difficult, and often misunderstood, issues and concepts of electronic privacy in a corporate environment. The course covers applicable laws and regulations, combined with typical corporate policy that deals with these issues. Understanding the methods of surveillance, the concept of expectations of privacy, and other similar topics help individuals be more effective in adhering to a corporate information security policy.

SA304: ACCESS CONTROL - IDENTIFICATION, AUTHENTICATION AND ACCOUNTABILITY

This course provides an introduction to access control and the major key stones of access control systems including identification, authentication, and accountability. Focusing on the different methods of access control available such as biometrics, tokens, single sign-on and passwords, the course outlines the best practice methods for applying access control to all information and network assets, based on the pre-determined rights of individual users.

SA305: PHYSICAL SECURITY OF INFORMATION ASSETS

This course provides an introduction to the importance of safe-guarding corporate information assets from physical compromise. Dealing with issues such as laptop security, access control, piggy backing, unattended assets, and social engineering techniques, the course provides an understanding of the risks to information assets from physical compromise and the proactive methods for prevention.

SA306: MALICIOUS CODE - WORMS, TROJANS AND VIRUSES

This course provides an introduction to the concept of malicious code, the different types of malicious codes, the methods of delivery, the impact to information assets that they can create, and the signs for identification of an infection. The course also covers, at a high level, preventive controls that can be deployed by users to minimize infections.

SA307: DISCLOSURE OF INFORMATION

This course provides a best practice approach on disclosure of information assets according to levels of classification, sensitivity, and security policy. This course is designed to provide insight on other related security concepts such as accidental disclosure, intentional disclosure, reporting disclosure events, labeling, common types of classifications, and the importance of information classification.

SA308: INFORMATION ASSET DISPOSAL

This course is designed to provide an introduction to the best practices for proper handling and disposal of information assets in contemporary organizations. The course also covers, at a high level, the various types of information assets pervasive in contemporary organizations, the proper methods of disposal and the implications of improper disposal of information assets in terms of disclosure and regulatory compliance.

SA309: INCIDENT RESPONSE TEAMS

This course provides an understanding of how corporate incident response teams function, their structure, their authority, sphere of influence and the responsibilities of an incident response team. This course is designed to provide an introduction to the various types of incidents, the concept of virtual teams, the weaknesses associated with virtual team models, the issues such as crime scene handling and forensics investigations, as well as the impact an improper approach can have on corporations.

SA310: REGULATORY COMPLIANCE

This course is designed to provide an introduction to the impact of regulatory compliance on the handling of information assets. The course provides, at a high level, an introduction to the more common regulatory laws and how they can affect an information security policy and program, and the implications of non compliance.

For More Information Call 678.845.0209