CERIAS Workshops for the K-12 Technology Coordinator

Intended Audience

Technology coordinators and/or school administrators who are responsible for information security, including policy development, in a school or school system.

General Abstract

An unfortunate perception about information security is that it is just about protecting computers. Many factors affect information security, and not all of them concern the technical aspects of computers and networks. In fact, the practice of information security transcends many aspects of an organization and is actually on of the most critical policy and structure decisions in any school system.

To ensure the security of a school's information, the availability of services critical to learning, and the safety of a school's constituents, administrators and technology staff need to stay apprised of fundamental security concepts and procedures, current and emerging security practices, and the theory that serves as the foundation for sound security decisions.

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

Workshop 1: Security Foundations & Risk Analysis

Description

This one- or two-day course will provide you with an overview of the foundational principles and goals of a sound information assurance and security program. In order to understand the policies, procedures, guidelines, training, and technology that your school needs to protect your information assets, you need to understand these fundamental principles. This course also demonstrates how to use cost effective risk analysis techniques to identify and quantify the threats to your organization, the origin of the threats, necessary countermeasures to reducing or eliminating the threat, and associated costs.

Objectives

- Recognize the purpose & value of information security.
  Understand and prioritize information security goals.
- Use basic information security terminology.
- Understand the purpose of information security risk analysis and its relationship to risk management.
- Recognize the benefits, types, and scales of risk analysis.
- Understand and practice the steps of risk analysis.

Workshop 2: Creating & Auditing School Security Practices

Description: Many people perceive information security to be a technology problem, when in fact technical solutions alone cannot achieve information security; information security decisions impact organizational policy and culture, and thus need to address the human components of a program. The cornerstone of an effective security architecture is well-written policy. This one- or two-day course demonstrates how to develop effective policies, practices, guidelines, and procedures that mitigate your school's information security risks. After completing this course, your school should be better prepared to establish a program that protects your information resources and guides personnel behavior.

Objectives:

- Use results of a risk assessment, in conjunction with security best practices, to develop an information security policy.
- Create and audit information security practices in order to determine the effectiveness of the information security program in place in the local school system.
- Identify the people, technology, and processes model for information security practices.
- Apply the people, technology, and processes model to the local school system.
- Describe and apply steps for evaluating security practices.

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

Workshop 3: Developing and Implementing a Security Training and Awareness Program

Description: Have you ever heard the phrase "employees are your best firewall?" This statement strikes at the heart of the information security problem; too often, information security programs fail because they address only the technological issues. This one-day course will highlight how to conduct security awareness training and initiatives that impact user behavior and makes your school's computer users one of the most effective countermeasures in your information security program.

Objectives:

- Conduct a gap analysis to identify poor security practices common to computer users.
- Identify practices and issues relevant to the K-12 population.
- Analyze successful and failed awareness and training programs.
- Develop goals for an awareness and training program.
- Select appropriate training and awareness interventions for your computer users.

Workshop 4: Intrusion Detection Systems

Description

While many technology coordinators and system administrators are comfortable with implementing firewall technology, there are many unanswered questions about an equally important security technology, intrusion detection systems. Intrusion detection systems include technological mechanisms, written security policies, and procedures used for detecting unauthorized system use. This one-day course will demystify intrusion detection systems by explaining the underlying basics of intrusion detection, providing further insights into the technology, and describing current limitations so that technology coordinators and system administrators will be able to effectively purchase and implement the intrusion detection system that is right for their school.

Objectives

- Describe the basic functions, goals, and uses of an intrusion detection system (IDS).
- Compare an IDS to other security technologies, including a firewall.
- Describe the types of IDSs.
- Weigh the advantages and disadvantages of implementing and maintaining types of IDSs.
- Understand/decrypt IDS vendor terminology.

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu