CERT's PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Building Staff Competence in Security

Key Message: Practical specifications and guidelines now exist that define necessary knowledge, skills, and competencies for staff members in a range of security positions — from practitioners to managers.

Executive Summary

Given that people are often described as the source of up to 80% of security problems, they likely also can provide up to 80% of security solutions when properly educated and trained. There is now a rich body of knowledge that defines the necessary skills and competencies for security professionals. In addition, CERT has developed virtual training environments that can be used anytime, anywhere by individuals and teams to acquire these skills.

In this podcast, Barbara Laswell, CERT's Manager for Practices, Development, and Training, discusses means and resources for building staff competency in security.

PART 1: IDENTIFY AND MATCH REQUIRED COMPETENCIES TO ROLES

Identify Security Competencies

Understanding the need to protect intellectual capital and key information assets requires an enterprise-wide perspective, from system and network administrators to senior leaders and executives.

The organization must ensure that those working on critical systems have the necessary skills, competencies, and training.

So, where are some of these key competencies defined?

- Department of Defense Directive 8570.01-M: Information Assurance Workforce Improvement Program "provides guidance and procedures for the training, certification, and management of the DoD workforce" in information assurance positions. Three levels of technical and three levels of management descriptions are provided for those individuals working on computer network defense systems in critical infrastructures.
- For commercial organizations, this equates to systems necessary to support core business functions.
- For example, managers develop policy to protect critical data; system and network administrators implement practices and controls to ensure the policy is met.

Undergraduate and graduate degree programs in information assurance and information security are increasingly available.

The Department of Homeland Security and the National Security Agency have selected and designated National Centers of Academic Excellence. Hiring managers should consider graduates from these colleges and universities, both for technical and management-level positions.

Match Skills to Roles

Match staff skills and capabilities to the security requirements and criticality of the assets (systems, networks, information) being protected. This presumes that you know what your critical assets are. Less critical assets may require lesser staff skills, or may offer an opportunity to build skill on the job.

This ties some of the notions of risk assessment and risk management with competency development. Be selective about where you put your most capable staff members. Everyone does not need to know everything.

Build information protection strategies (assurance levels) in from the very beginning of a new product development, new service development, or software development life cycle. If you do this, then all parties involved address this from the beginning, not as an afterthought.

PART 2: WHAT SKILLS SHOULD A HIRING MANAGER LOOK FOR?

Certifications

DoD Directive 8570.01-M: Information Assurance Workforce Improvement Program includes a list of approved baseline certifications in Appendix 3, Table AP3.T1, page 64. The listed certifications are grouped by technical and manager levels I, II, and III. See the Resources section below for additional information on certifications.

Keep staff current in a changing environment:

- Make sure you have a continual learning development cycle for staff performing critical functions and protecting critical assets.
- Make staying current a cultural norm, an expected behavior.
- Recognize that staff typically cannot leave their current positions for off-site training, given the short supply of people with the right skills to keep critical systems up and running.
- Understand the need for globally distributed, asynchronous training methods for acquiring new skills and keeping up to date.
- Practice just-in-time learning for just-in-time application of new skills.

CERT's Virtual Training Environment (VTE) provides one solution.

- Available to anyone, anytime, anywhere
- Presents a wide range of topics in information assurance
- Contains lectures, demonstrations, and lab exercises
- Provides learning environments for individuals as well as teams

VTE presents complex, scenario-based, networked environments that reflect real production environments; as such, it is a safe place to experiment and learn.

Students can respond to the latest intruder attacks as an exercise, before seeing the real thing in a live setting.

A VTE user can acquire individual skills, but practicing as a team is essential — and VTE provides this opportunity.

PART 3: CREATING A CULTURE OF SECURITY; ACTIONS LEADERS CAN TAKE

In an information-based society, all users (including partners and suppliers) are developing intellectual capital for their organizations, clients, and customers.

Leaders have defined and communicated a structure and a means for classifying and categorizing information.

All users understand and actively consider:

- how critical information that requires protection is created, used, stored, and transmitted
- business requirements for the confidentiality, availability, and integrity (CAI) of information, and their role in ensuring these requirements are met
- the impact to the business if breaches of CAI occur, across the board and for specific customers

how to use a risk-based approach to select and prioritize what actions to take

Leaders need to:

- Make sure that required competencies and training plans are written into service level agreements with third parties.
- Make training expectations explicit with in-house staff, including what policies, procedures, and standards they are held to.
- Put processes in place to monitor, review, and enforce these expectations.

Take a look at The Committee on National Security Systems resources (under Issuances/Instructions) for role-based functional requirements for specific positions, such as information systems security officer and information systems security manager.

Use CNSS and 8570 resources and training standards as hiring guidelines as well as guidelines for training programs for in-house staff and service providers.

Resources

Department of Defense Directive 8570.01-M: Information Assurance Workforce Improvement Program, December 19, 2005.

The Committee on National Security Systems resources (under Issuances/Instructions)

Organizations Offering Certifications

- (ISC)2 (International Information Systems Security Certifications Consortium) offers CISSP: Certified Information Systems Security Professional and SSCP: System Security Certified Practitioner certifications.
- ISACA (Information Systems Audit and Control Association) offers CISM: Certified Information Security Manager and CISA: Certified Information Security Auditor certifications.
- SANS Institute offers a range of GIAC (Global Information Assurance Certification) certifications.
- CompTIA (Computing Technology Industry Association) offers security and network certifications.
- CERT-certified Computer Security Incident Handler

Additional Certification Resources

- Tittel, Ed. Certification Top 10 Lists Revisited, November 2006.
- IT Governance. Information Security Qualifications.
- SANS Institute. The SANS 2005 Information Security Salary & Career Advancement Survey.
