Security is Everyone's Business: Role-Based Training for the System Development Life Cycle

Margaret Spanninger
Booz, Allen & Hamilton

Abstract

This paper is based on the premise that the integration of security into organizational business processes, especially the system development life cycle (SDLC), is a fundamental requirement for Federal Information Security Management Act (FISMA) compliance and attaining security performance goals. Now, more than ever, security role-based training is key for achieving security integration into enterprise business processes and the cultural change that is required to sustain long-term organizational benefits and improvement in enterprise security programs.

Organizations must identify the stakeholders in each life cycle phase and educate them about their roles. This education must help personnel distinguish between performance and compliance issues, and the roles responsible and accountable for "doing" security versus "ensuring" security. Role-based training will address these stakeholders and their roles and teach them what is required to pass the "security baton" from one phase to the next.

By integrating security into the SDLC and providing role-based training to personnel with significant security responsibilities, organizations can be better prepared to meet the challenges of FISMA compliance. It is clear that IT systems cannot be adequately protected unless all personnel understand their roles and responsibilities for safeguarding the information and information resources. Training can promote cultural change and shift the workforce from being observers who show interest in security to becoming participants who demonstrate commitment to security.

This paper focuses on developmental activities of the SDLC, security activities that must be integrated into the SDLC, and the players or stakeholders in each SDLC phase. It is only through the understanding of these security roles and their relationships among each other that total security integration can occur.

Biography
Margaret (Marge) Spanninger is an Associate at Booz Allen Hamilton Inc. where she leads the Security Workforce Development Services group of Booz Allen's Global Resilience Team. She was graduated from West Virginia Wesleyan College with a B.S. in Accounting and from The George Washington University with an M.B.A in Information Systems Technology. Mrs. Spanninger has over 25 years of experience in

technical and security training design, development, and delivery. She has conducted security training for government clients that include Department of Veterans Affairs, Department of Energy, Department of Education, General Services Administration, and several agencies of the Intelligence Community.

Mrs. Spanninger is the author of the following papers—

Developing Security Competencies Through Information Assurance Undergraduate and Graduate Programs, presented at the National Colloquium for Information System Security Educators (NCISSE) Conference, September 2001.

Security Awareness and Training: The Neglected Countermeasures, presented at the Federal Information System Security Educators Association (FISSEA), March 2003.