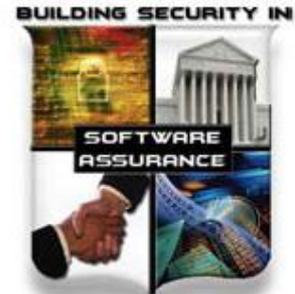

Lessons Learned in Implementing Software Assurance



Presented by Carole Dicker
Director, Information Security at
Compusearch Software Systems, Inc.
March 10, 2009

Scope and Approach:

What is the Perspective?

- Small well established product company - COTS Acquisition Management software for the Federal Government
 - Formal security program - covering both internal security and product assurance
 - Top down – information assurance promoted by executive management
-

Scope and Approach:

What is the Implementation Challenge?

- Budgeting security in
- Application security has not yet permeated software development community at large
- How to include software assurance in the existing process (change management activity)
- How to think like a hacker (training activity)

Change throughout the Organization

What is Sufficient SwA?

- Risk management approach
 - As a COTS product company, consideration given to:
 - Customer requirements
 - Target deployment environment of the product
 - Data that the product contains
 - Legal/liability concerns
-

Implementing Software Assurance Activities

- Establishing policy
 - Finding the best opportunities to educate and train - threat modeling, secure code standards, testing methods, and tools
 - Defining where security activities fit into the organization's development process
 - Assisting management and team leads to understand their roles
-

Leveraging Technology (and Tools) for Implementation

- Information Resource Tools
 - OWASP Top 10
 - CWE Top 25
 - Industry Experts
 - Technology
 - Industry Experts (manual)
 - Automated testing – dynamic and static code review
-

Recognizing Success: Anecdotal

- Last year, I am the initiator of passing around various security informational articles to Executive Management
 - This year, the COO is sending me articles on “building security in” and the CTO is sending me articles on “Protection Poker” to develop a collaborative process for threat modeling
-

Recognizing Success: Anecdotal

- Last year, I invited a variety of security consulting and tool vendors to demonstrate/discuss security product for our organization
 - This year, Compusearch budget units are requesting pricing so they could include these costs in their budgets
-

Carole Dicker

Director, Information Security

Compusearch Software Systems, Inc.

21251 Ridgetop Circle, Suite 100

Dulles, VA 20166

571-449-4184

cdicker@compusearch.com

<http://www.compusearch.com>
