SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

3 November 2009

DoD-DHS-NIST Software Assurance Forum Where is Academia Going & How can the SwA Forum Help? Panel Briefing

Facilitator: Carol Woody, SEI/CERT

Mini-Keynote: Wm. Arthur Conklin, PhD

Participants

- Facilitator: Carol Woody, SEI/CERT
- Mini Keynote: Wm. Arthur Conklin, PhD
- Panelist: Tammy Alexander, University of Memphis
- Panelist: Stephen Boyer, MIT Lincoln Labs
- Panelist: Dan Shoemaker, University of Detroit Mercy

Academia Contributes to Software Assurance

- SwA Working Group

- Education
  - Publications
  - Teaching content
  - Curriculum

- Research Initiatives
  - Facilitate Workshops
  - Defining the Ontology
  - Promote Standards
  - Building and Piloting Methods, Practices, and Frameworks

Workforce Education and Training

- *Software Assurance: A Curriculum Guide to the Common Body of Knowledge*. PDF is available for download from the Build Security In Web site.

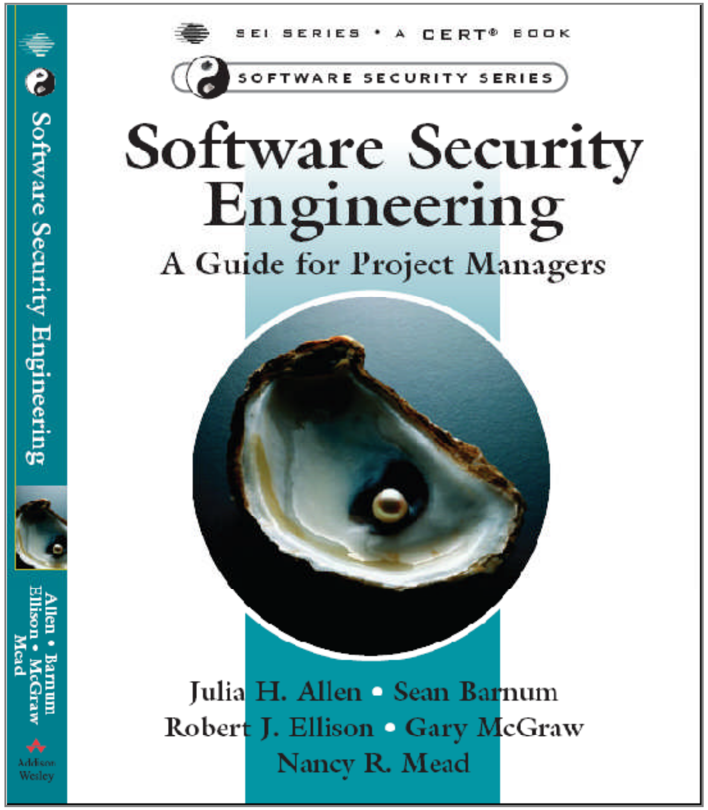
- Backgrounder on *Software Assurance: A Curriculum Guide to the Common Body of Knowledge*

- *Toward an Organization for Software System Security Principles and Guidelines*, version 1.0, by Samuel T. Redwine, Jr. Institute for Infrastructure and Information Assurance, James Madison University, IIIA Technical Paper 08-01, February 2008.

SEI Education Examples

Software Security Engineering: A Guide for Project Managers

- Published May 2008
- Contains an introduction to software security engineering and guidance for project managers
  - Derives material from DHS SwA “Build Security In” web site
  - Provides a process focus for projects delivering software-intensive products and systems



SEI SERIES • A CERT® BOOK

SOFTWARE SECURITY SERIES

Software Security Engineering

A Guide for Project Managers

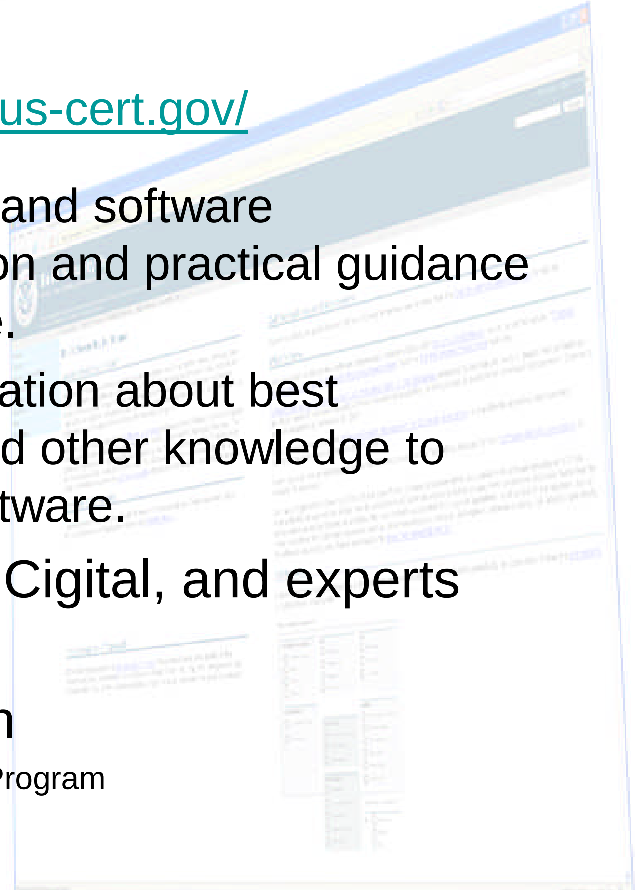
Julia H. Allen • Sean Barnum
Robert J. Ellison • Gary McGraw
Nancy R. Mead

Software Security Engineering

Allen • Barnum
Ellison • McGraw
Mead

Addison Wesley

Education Material: Build Security In



- Build Security In web site: https://buildsecurityin.us-cert.gov/
  - BSI is intended for use by software developers and software development organizations who want information and practical guidance on how to produce secure and reliable software.
  - BSI contains or links to a broad range of information about best practices, tools, guidelines, rules, principles, and other knowledge to help organizations build secure and reliable software.
- Contributing authors include CMU SEI CERT, Cigital, and experts from the SwA community
- Expanding to include current doctoral research
- Sponsored by U.S. Department of Homeland Security, Software Assurance Program

Software Assurance Curriculum Development in support of DHS NCSD

- Development of graduate curriculum reference model for Master’s in Software Assurance, and software assurance specialization(s) within other master’s degrees. Delivery 2Q2010

- Development of annotated undergraduate course outlines in software assurance, to fit into a variety of existing curricula. Delivery 1Q2010

SEI Research Examples

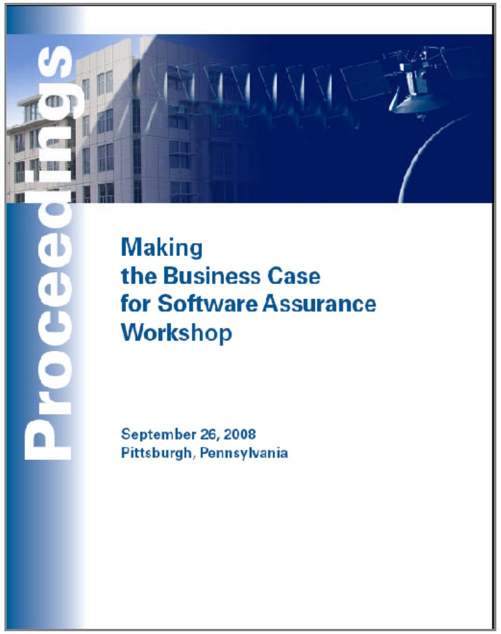
SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Workshop: Making the Business Case for SwA

- Held September 26, 2008 at Carnegie Mellon
- Invited speakers, refereed paper presentations, facilitated discussions; 70 researchers and practitioners
- Topics:
  - Measurement
  - Process and decision making issues
  - Legal issues
  - Globalization
  - Risk issues
  - Organizational development issues

- http://www.sei.cmu.edu/community/BCW_Proceedings.pdf



Proceedings

Making
the Business Case
for Software Assurance
Workshop

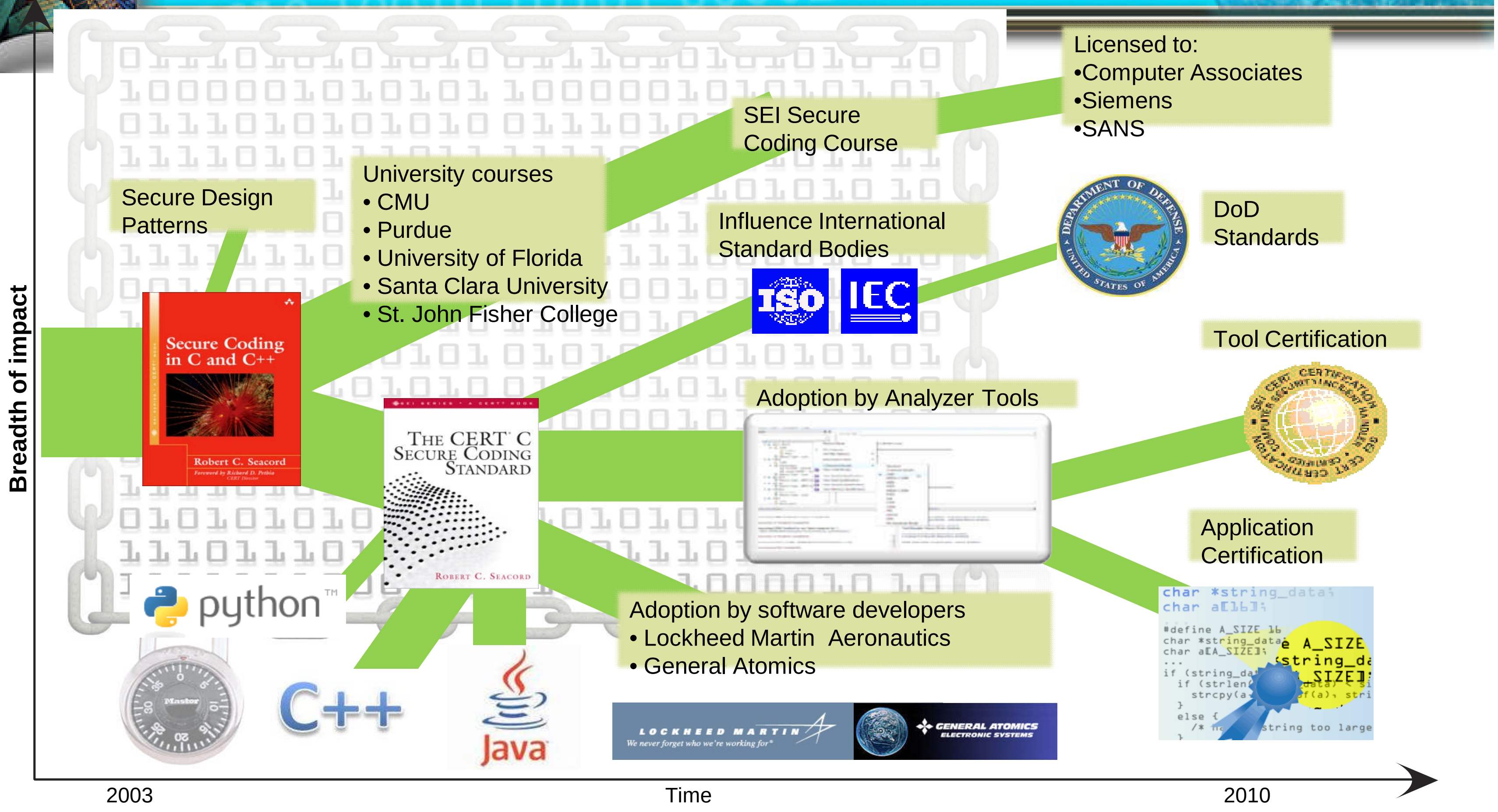
September 26, 2008
Pittsburgh, Pennsylvania

Ontology: Software Assurance Landscape Project

- Build a framework to understand how participating organizations and technologies contribute to software assurance
  - Use an iterative discovery, multi-phase approach
  - Leverage multiple analysis and modeling methods oriented to complex, social and technical environments

Starter Set of Questions to Address with a Framework
Who are the participants?
What are the technologies and other elements of value exchanged among participants?
What are the roles of participants, technologies, and other mechanisms in enabling achievement of software assurance?
How do technologies and organizational structures work together to achieve software assurance?
How is the achievement of assurance results accomplished within the DoD today?
What patterns of possible inefficiencies can be identified?
What are candidates for improvements, and what is their likely impact?

Standards: Secure Coding Initiative



Secure Design Patterns

University courses

- CMU
- Purdue
- University of Florida
- Santa Clara University
- St. John Fisher College

SEI Secure Coding Course

Licensed to:

- Computer Associates
- Siemens
- SANS

Influence International Standard Bodies

DoD Standards

Tool Certification

Adoption by Analyzer Tools

Application Certification

Adoption by software developers

- Lockheed Martin Aeronautics
- General Atomics

Methods & Practices (1)

- **Security Quality Requirements Engineering (SQUARE)**

- Method for identifying software security requirements

Who is involved ?

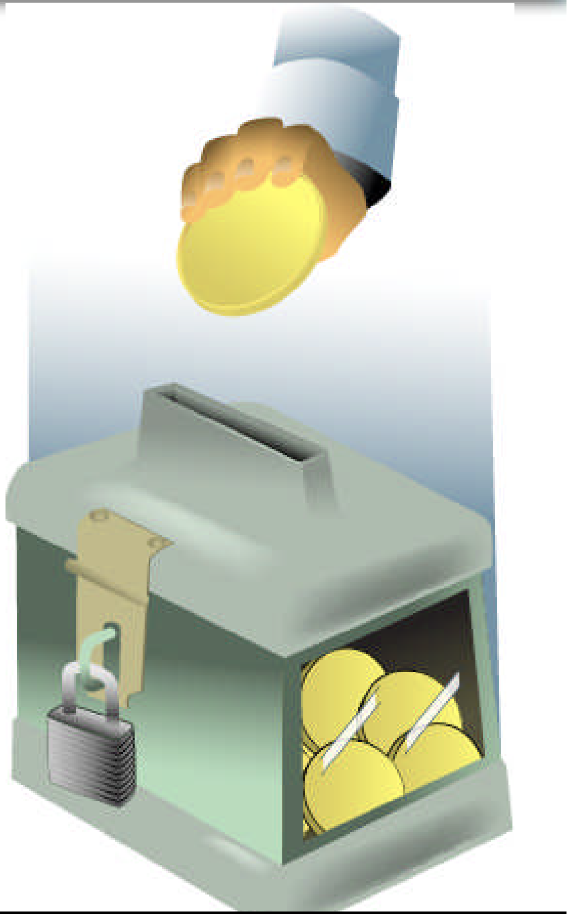
- stakeholders of the project
- requirement engineers with security expertise

In the SQUARE approach, security requirements are

- treated as add-ons to the system's functional requirements, *but*
- carried out in the early stages
- specified in similar ways as software requirements engineering and practices
- carried out through a process of nine discrete steps

Methods & Practices (2)

- **Security Investment Decision Dashboard (SIDD)**
- Make security investment decisions in the same fashion as other business investment decisions
- Use business-based criteria
- Engage leaders in establishing criteria priorities
- Track investment priorities, performance, and results over time
- *Ensure that investments in security directly support business objectives.*



Methods & Practices (3)

- **Supply-Chain Risks and Acquisitions**
- Management of supply-chain risks should be part of the normal acquisition process
  - When should supply-chain risks be addressed?
  - What level of risk is acceptable (if any)? And at what cost?
  - What decisions are required and who makes them?
  - What do we need to know about software suppliers, or the software development environment, in order to be able to thwart such threats?
  - What are the sources of such information?
  - For many acquisitions, a significant portion of supply-chain risk management has to be delegated to the prime contractor.
    - How should a prime contractor manage supply-chain risks with sub-contractors?
    - What visibility should the Program Office have into those relationships?
- Consideration of supply chain risk should begin as early in the acquisition life cycle as possible

How Can the SwA Forum Help?

- Can SwA Forum participants
  - further education and research efforts?
  - tap education and research to address their needs?
  - contribute lessons learned?
- Can the SwA Forum provide a venue for sharing research to enhance its value?
- Other ideas?

Contact Information

Carol Woody, Ph.D.

Senior Technical Staff

CERT

Telephone: +1 412-268-9137

Email: cwoody@cert.org

U.S. mail:

Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

World Wide Web:

www.sei.cmu.edu

www.cert.org

Customer Relations

Email: customer-relations@sei.cmu.edu

Telephone: +1 412-268-5800

Participants

- Facilitator: Carol Woody, SEI/CERT
- Mini Keynote: Wm. Arthur Conklin, PhD
- Panelist: Tammy Alexander, University of Memphis
- Panelist: Stephen Boyer, MIT Lincoln Labs
- Panelist: Dan Shoemaker, University of Detroit Mercy

Mini-Keynote

- Where is Academia Going?
- How Can the SwA Forum help?

Where is Academia Going?

- Academia is not a business
- Academia is not government
- Academia is Academia

How Can the SwA Forum help?

- Objective: Teach Johnny to Code
- Mechanism: Change their Instructional Outcome
- Who, What, How, When

How Can the SwA Forum help?

- Change the game: Instructional material for non-believers
- Attack Surface: Target based on volume
- Environment: Raise the water level

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

3 November 2009

DoD-DHS-NIST Software Assurance Forum ACT Online Overview Panel Briefing

Panelist:
Tammy Alexander
University of Memphis
Center for Information Assurance

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

act online
www.act-online.net

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security

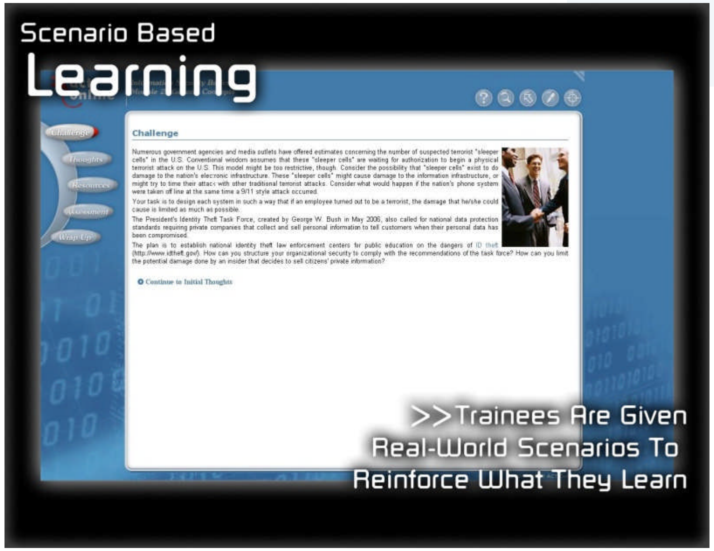
Participants

- Facilitator: Carol Woody, SEI/CERT
- Mini Keynote: Wm. Arthur Conklin, PhD
- Panelist: Tammy Alexander, University of Memphis
- Panelist: Stephen Boyer, MIT Lincoln Labs
- Panelist: Dan Shoemaker, University of Detroit Mercy

Introduction

- Overview
  - Program
  - Stats
  - Feedback

IA General/Non-Technical	IA Technical/IT Professional	IA for Business Professionals
Information Security for Everyone TEI Course Number: AWR-175-W	**Information Security Basics** TEI Course Number: AWR-173-W	**Business Information Continuity** TEI Course Number: AWR-176-W
Cyber Ethics TEI Course Number: AWR-174-W	**Secure Software** TEI Course Number: AWR-178-W	**Information Risk Management** TEI Course Number: AWR-177-W
Cyber Law and White Collar Crime TEI Course Number: AWR-168-W	**Network Assurance** TEI Course Number: AWR-138-W	**Cyber Incident Analysis & Response** TEI Course Number: AWR-169-W
	Digital Forensics Basics TEI Course Number: AWR-139-W	



Challenge

Numerous government agencies and media outlets have offered estimates concerning the number of suspected terrorist "sleeper cells" in the U.S. Conventional wisdom assumes that these "sleeper cells" are waiting for authorization to begin a physical terrorist attack on the U.S. This model might be too restrictive, though. Consider the possibility that "sleeper cells" exist to do damage to the nation's electronic infrastructure. These "sleeper cells" might cause damage to the information infrastructure, or might try to time their attac‹ with other traditional terrorist attacks. Consider what would happen if the nation's phone system were taken off line at the same time a 9/11 style attack occured.

Your task is to design each system in such a way that if an employee turned out to be a terrorist, the damage that he/she could cause is limited as much as possible.

The President's Identity Theft Task Force, created by George W. Bush in May 2006, also called for national data protection standards requiring private companies that collect and sell personal information to tell customers when their personal data has been compromised.

The plan is to establish national identity theft law enforcement centers for public education on the dangers of ID theft (http://www.idtheft.gov/). How can you structure your organizational security to comply with the recommendations of the task force? How can you limit the potential damage done by an insider that decides to sell citizens' private information?

Continue to Initial Thoughts

>>Trainees Are Given Real-World Scenarios To Reinforce What They Learn

Global Reach: Over 5000 participants in all states and U.S. Territories

THE UNIVERSITY OF MEMPHIS. Center for Information Assurance

act online www.act-online.net

Homeland Security

Outreach

- Challenges
- How can you help?

http://www.act-online.net

http://cfia.memphis.edu

Tammy Alexander, Project Manager

901-678-1521 or tammy.alexander@memphis.edu

Participants

- Facilitator: Carol Woody, SEI/CERT
- Mini Keynote: Wm. Arthur Conklin, PhD
- Panelist: Tammy Alexander, University of Memphis
- Panelist: Stephen Boyer, MIT Lincoln Labs
- Panelist: Dan Shoemaker, University of Detroit Mercy

STEPHEN BOYER

MIT LINCOLN LABS

Participants

- Facilitator: Carol Woody, SEI/CERT
- Mini Keynote: Wm. Arthur Conklin, PhD
- Panelist: Tammy Alexander, University of Memphis
- Panelist: Stephen Boyer, MIT Lincoln Labs
- Panelist: Dan Shoemaker, University of Detroit Mercy

A Problem of Understanding

- No common understanding of what constitutes the SwA process
  - Tendency to confuse “doing it right in the first place” with additional things you need to know in order to produce secure software

- No accrediting bodies for the BOK
  - Which creates a serious validity problem

- No public awareness of the issue, let alone best practice

What We Are Doing About That

- Describing the discipline
  - Compiling and indexing everything published on the topic of secure software assurance (currently 1,691 cites)

- Validated the conceptual model for secure software assurance
  - Using a Delphi process to obtain structured understanding/agreement from government, industry, academic and standards experts

- Mapping specifically where secure software assurance content fits into the curricula of the various disciplines (CC 2005)

What We Are Doing About That

- Developing “snap-in”” courseware in areas that do not duplicate current disciplinary content
  - **Risk Management** (as it pertains to Software Assurance)
    - Threat modeling to manage risk during specification and design
  - **Operational Assurance Processes**
    - Ethical Hacking/Forensics (ad-hoc discovery of vulnerabilities)
    - Operational Sensing (monitoring of changing environment)
    - Configuration Control
  - **Secure Coding Methodologies**
  - **Strategic Assurance Processes**
    - Secure Acquisition
    - Secure Project Management
    - Secure Supply Chain Management

What We Are Doing About That

- Developing learning methodologies consistent with the delivery of the courseware
  - Customizing instructional delivery approaches for each discipline
- Developing learning milieu consistent with current generation of learners
  - Visual, asynchronous and web-enabled
- Developing delivery vehicles other than traditional instruction
  - Such as visual i-pod university