I Touch the Future, I Teach.

Crista McAuliffe
Computer Security

A Program for
Federal Government
Executives
Objectives

- Seven Basic Computer Security Facts
- Applicable Laws, Policy, Procedures, ETC.
- Current Computer Security Issues
- Risk Management Processes
- Accreditation Process
- Action Items
Seven Basic Facts

1. Agency Mission
2. Define Threat
3. Vulnerability
4. Protect Information
5. Risk Management
6. Awareness And Training
7. Effective Tool
FACT 1

COMPUTERS ARE CRITICAL TO FULFILL YOUR AGENCY MISSION!
FACT 2

THERE ARE DEFINED THREATS TO YOUR COMPUTER SYSTEM!
FACT 3

COMPUTER SYSTEMS ARE VULNERABLE!
FACT 4

COMPUTER SECURITY IS ESSENTIAL TO PROTECT YOUR SENSITIVE AND CLASSIFIED INFORMATION!
FACT 5

RISK MANAGEMENT IS AN EXECUTIVE RESPONSIBILITY!
FACT 6

COMPUTER SECURITY AWARENESS AND TRAINING PROGRAMS REDUCE RISK!
FACT 7

A COMPUTER SECURITY PLAN IS AN EFFECTIVE EXECUTIVE TOOL
YOUR ROLE?

Who?
What?
How?
When?
Where?
Role of the Executive

- Establish Computer Security Policy
- Assign Responsibility
- Accept Risk
- Provide Resources
- Evaluate Results
Where Do You Fit?

- Security Plan
- Mission and Need Statement
- Risk Assessment
- Policies, Procedures, Directives
- Guidelines, Standards and Regulations
- Policy and Executive Order
- Laws
Level 1 Executive

• **Responsibility**
  – Interpret Law and Establish Policy
  – Evaluate Mission
  – Assign Organizational Responsibility
  – Evaluate Certification System and Accept Risk
  – Justify, Defend and Provide Resources

• **Rank:** SES Mid-Level or Higher

• **Reports To Board of Governors/ Directors or Head of Federal Agency**
Level 2 Executive

• Responsibility
  – Translate Policy to Operational Need
  – Assign Unit Responsibility
  – Evaluate Risk Assessment Statement
  – Recommend Security Safeguards
  – Dispense and Evaluate Resource Allocations

• Rank: Lower to Mid-Level SES
• Reports to Executive Level 1
Level 3 Executive

- **Responsibility**
  - Implement Policy
  - Supervise Unit Responsible for Action
  - Implement Security Safeguards
  - Utilize Allocated Resources

- **Rank:** Lower Level SES or GS/GM 15

- **Reports to Executive Level 2**
Statutory and Executive Baseline

Security Plan

Mission and Need Statement Risk Assessment

Policies, Procedures Directives

Guidelines, Standards and Regulations

Policy and Executive Order

Laws
Applicable Computer Security Statutes

Public Law 97-255
Federal Managers Financial Integrity Act of 1987

Public Law 98-473
Comprehensive Crime Control Act of 1984

Public Law 99-474
Computer Fraud and Abuse Act

Public Law 99-508
Interception or Disclosure of Wire, Oral or electronic Communications

Public Law 100-235
Computer Security Act of 1987

Public Law 100-503
Computer Matching and Privacy Protection Act
Applicable Policy and Executive Orders

OMB Circular A-130
Management of Federal Information Resources

OMB Circular A-123 & 127
Internal Control/Financial Management Systems

OMB Bulletin 89-22
Computer Matching and Privacy

OMB Bulletin 90-08
Agency Security Plans

Executive Order 12333
United States Intelligence Activities

Executive Order 12356
National Security Information

DCI Directive 1/16
Security Policy for Uniform Protection of Intelligence Processed in AIS’s and Networks
Guidelines, Standards and Regulations

- National Institute of Standards and Technology (NIST) Technical Publications, Training Assistance and Newsletter
- National Computer Security Center (NCSC) Rainbow Series, Technical Reports
- Office of Personnel Management (OPM) Training Requirements for all USG Employees
- General Accounting Office (GAO) Reports on AIS Deficiencies and Remedies
- General Services Administration (GSA) Provides Training Services for Users
Agency and System Documentation

- Policies, Procedures, Guidelines and/or Directives
  - Obtain These From Your Federal Agency
  - These are Agency-wide Computer Documents
  - They Will be Specific to Your Organization
Agency and System Documentation

• Mission and Risk Assessment Statements
  – Baseline Documentation For Operation Of Computer System/Network. This Plan Is System Specific
  – “Working/Living” Document
Agency and System Documentation

• Mission and Risk Assessment Statements
  – These are Derived From Agency Policies And Procedures
  – These Two Statements Are System Specific
Current Issues

Confidentiality
Integrity
Availability

Biographical Data
Payroll Data
Health Data

Packet Switch
Bridge
Gateway
File Server

Other Networks

Sensitive Data
Biographical Data
Payroll Data
Health Data
Current Issues
Confidentiality, Integrity, Availability

Confidentiality

Integrity

Availability
Current Issues
Data Aggregation and Sensitivity

Biographical Data

Payroll Data

Health Data
Current Issues
Inter-connectivity

- Video
- Bridge
- Packet Switch
- File Server
- Gateway
- Other Networks
Current Issues
Common Misconceptions

• Computer Security Deters Only Criminals
• Implementation and Costs are Prohibitive
• Applies Only to Classified Systems
• Virus Protection is the Only Reason
• Once Secure — Always Secure
• Encryption Is The Solution
• “The Great Computer Chip”
Developing Certification Package

Evaluation

Risk Assessment

Risk Mission

Security Plan

Copyright 1993 All Rights Reserved
EVALUATION

Evaluation Involves Technical Assessment Of:

- The Hardware,
- The Software and
- The Procedures Which Meet A Specific Policy.
Risk = Threat $\times$ Vulnerability — Security
LIST OF POSSIBLE ASSETS

• Hardware
  – Physical Items
  – Firmware Updates

• Software
  – Operating System
  – Application

• Personnel
  – Operators & System Maintainers
  – Users - Direct/Indirect

• Data & Information
  – Collection
  – Storage
  – Stages of Process
  – Replacement Value
  – Current Worth
    » Short Term
    » Long Term
Risk Management

Risk = Threat \times\ Vulnerability — Security Safeguard
THREATS TO COMPUTER SYSTEMS

• Threats By People
  – Unintentional Employee Action 50-60%
  – Intentional Employee Action 15-20%
  – Outside Actions 1-3%

• Physical & Environmental Threats
  – Fire Damage 10-15%
  – Water Damage 5-10%
  – Electrical Fluctuations 1-5%
  – Natural Disaster 1%

• Other 5-10%
Risk Management

Risk = Threat \times Vulnerability — Security Safeguard
PC VULNERABILITIES

- Increasing Number Of Systems
- Physical Awareness
- Lack of Built-in Security Mechanisms
  (Access Control)
- Available Operating System Code
- Easily Transportable
- Lack of User Training and Awareness
- Local Area Network Accessibility
Risk Management

\[ \text{Risk} = \text{Threat} \times \text{Vulnerability} \quad \text{— Security Safeguard} \]
SECURITY SAFEGUARDS
When Is Risk Management Important?

Life Cycle Phases

- Design and Development
- Fabrication and Production
- Acquisition and Procurement
- Test and Evaluation
- Shipping and Delivery
- Operations
- Maintenance
- Obsolescence and Removal
Risk Management

• Why risk management is important should be obvious.
  – The purpose is to keep classified or sensitive information - Confidential, with full Integrity and Available at all time.

• When does Risk Management occur?
  – From the beginning of the system design (a twinkle in the engineer’s eye) to the time the system is thrown out and destroyed.

• Security must be an integral part of the entire Life Cycle
  – You will save money and time if SECURITY IS NOT RETRO-FITTED
Security Plan

• The Plan Must
  – Identify All Actions Needed To Implement Security Safeguards
  – Cite All Applicable Laws, Policies and Regulations
  – Describe Degree of Compliance With Regulations
  – Provide For A Review and Revision Process
Security Plan

I. Introduction
   A. General
   B. Security Management
   C. System Overview

II. Computing Facility
    Description/Configuration

III. System Description
    A. System Configuration
    B. Hardware Description
    C. Software Description

IV. System Accesses and Ops.
    A. System Access
    B. System Preparation
    C. Data Process
    D. Mode Termination

V. System Audit
   A. Manual
   B. Automated

VI. Media and Hdw Control
    A. Control and Accountability
    B. Sanitization
    C. Maintenance

VII. A. Concept of Ops.
     B. Duties
     C. Virus Protection

VIII. Policy
      A. Introduction
      B. Applicable Documents
      C. Compliance

IX. Documentation & Training
    A. Documentation
    B. Security Training
Certification

Certification Package

• Certification Memorandum
• Evaluation Report
• Risk Analysis Document
• System and Network Security Plan
  – System Interconnect MOUs
  – Security Certification Documents
    (Physical, Tempest, COMSEC, Personnel)
Accreditation

• The Official Management Decision To Operate A System
DAA Accreditation Decision
Risk Management

\[ \text{Risk} = \text{Threat} \times \text{Vulnerability} \quad \text{— Security Safeguard} \]
Accreditation Process

Executive Role

Risk Assessment

Security Plan

Evaluation
Executive Action Items
Level 1 Executive Action Items

- Validate Number and Function of Systems
- Appoint Accreditor To Each System/Network
- Advise Certifier
- Appoint Security Officer To Each System/Network
- Assign Responsibility and Deadline for Certification
  Package of Each System
Level 2 Executive Action Items

• Appoint Program Manager
• Determine Boundary For Each System/Network
• Assign Responsibility For Evaluation
• Develop Security Policy For Each System/Network
• Assign Organizational Responsibility To:
  – Security Tasking
  – Configuration Management Tasking
  – Mission and Function Tasking
Level 3 Executive Action Items

• Prepare Program Management Plan  
  (Include Security Plan)
• Implement Security Policy
• Verify And Validate Dates for Certification  
  Package And Assign Personnel
• Develop And Implement Risk Analysis
• Evaluate and Monitor Resource Expenditures
Computer Security

A Program for Federal Government Executives
I Touch the Future, I Teach.

Crista McAuliffe

These Materials Were Produced
For
The Federal Information Systems Security Association
by
The Center for Decision Support
Idaho State University

For Additional Information Contact
Dr. Corey D. Schou
Chairman, Computer Information Systems
Idaho State University
P.O.Box 4043
Pocatello, Idaho 83205-4042
(208) 236-3040