Security Awareness and Training—The Neglected Countermeasure

Federal Information System Security Educators Association

16th Annual Conference

March 5, 2003

Prepared by:
Marge Spanninger
Booz Allen Hamilton
(703) 289-5471
spanninger_margaret@bah.com

Booz | Allen | Hamilton

Today's Presentation

- Introduction
- Security Training Requirements Are Not New
- Federal IT Security Assessment Framework (ITSAF)
- NIST Self-Assessment Questionnaire
- OMB FY 2001 GISRA Findings
- OMB FY 2002 GISRA Findings (TBD)
- Security Awareness and Training Has Been Neglected
- Achieving ITSAF Level 5
- NIST 800-50 Provides a Blueprint
- A Model for Success
- Security Awareness and Training Is the Neglected Countermeasure

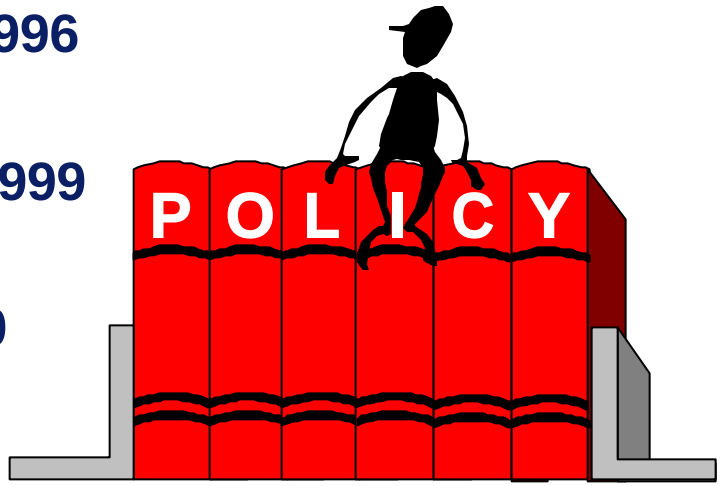
Introduction

This presentation is based on the premise that Security Awareness and Training are a countermeasure that is often neglected for more glamorous and tangible hardware and software security solutions.

- **All agencies within the Federal government are charged with ensuring the security of their information and information resources**
- **Management, IT professionals, security professionals, and system users have a responsibility for safeguarding the information and information resources of their agency**

Security Training Requirements Are Not New

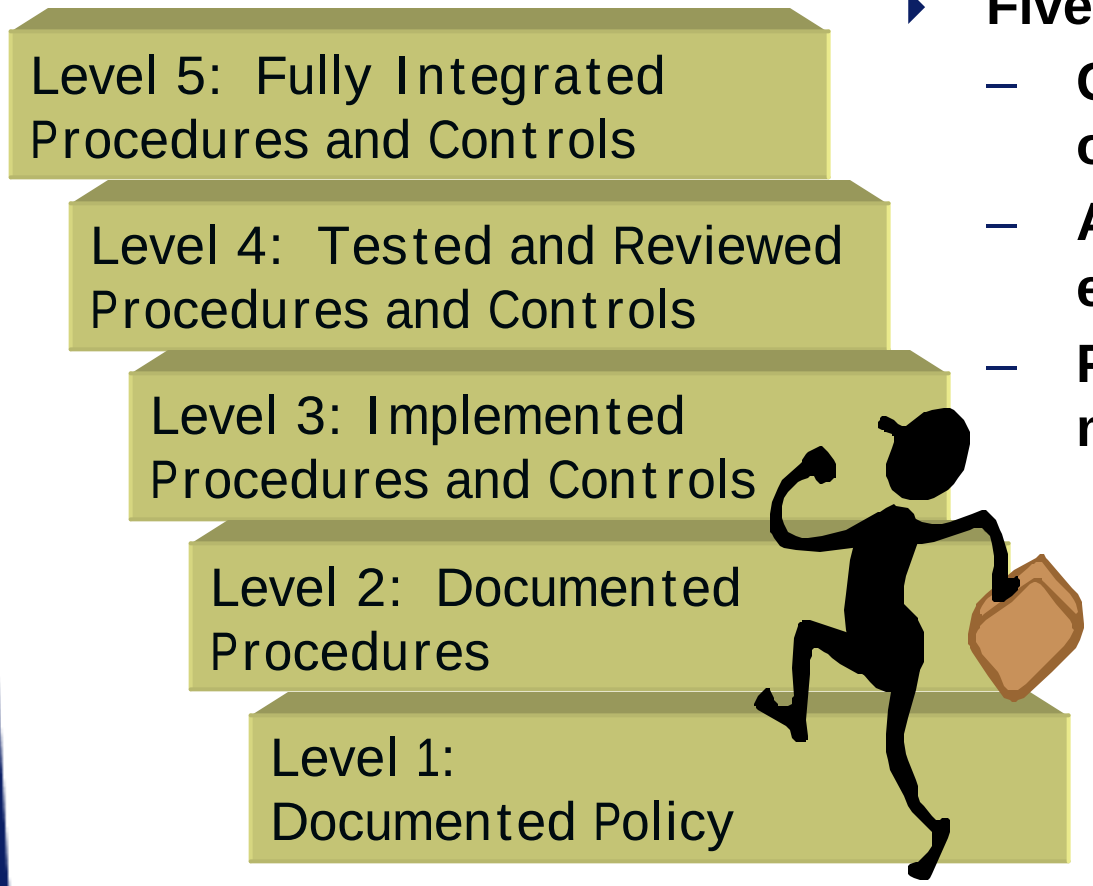
- Federal Managers Financial Integrity Act (FMFIA) of 1982
- OMB Circular A-123, Management Accountability and Control, 1995
- Computer Security Act of 1987
- OMB Circular A-130, Management of Federal Information Resources, 1996
- GAO Federal Information System Control Audit Manual (FISCAM), 1999
- Government Information Security Reform Act (GISRA) October 2000
- Federal Information Security Management Act (FISMA), 2002



Federal IT Security Assessment Framework

- The Framework provides a method for agency officials to
  - Determine the current status of their security programs relative to existing policy, and
  - Where necessary, establish a target for improvement
- It ***does not*** establish new security requirements
- The Framework is used to assess the status of security controls for a given asset or collection of assets

Federal IT Security Assessment Framework



- **Five levels to**
  - **Guide agency assessment of their security programs**
  - **Assist in prioritizing efforts for improvement**
  - **Provide a basis to measure progress**

Each level represents a more complete and effective program

NIST Self-Assessment Questionnaire

- The Self-Assessment Guide supports the IT Security Framework
- It blends requirements and guidance from GAO's FISCAM and several NIST documents
  - ***Critical elements*** are derived from OMB A-130
  - It has a hierarchical approach that is similar to FISCAM
- It identifies specific ***control objectives*** for standardizing and measuring IT security

NIST Self-Assessment Questionnaire

Management Controls	Operational Controls	Technical Controls
1. Risk management 2. Review of security controls 3. Life cycle 4. Certification & accreditation 5. System security plan	6. Personnel Security 7. Physical Security 8. Production input/output controls 9. Contingency planning 10. Hardware and system software maintenance 11. Data integrity 12. Documentation 13. Security awareness, training & education 14. Incident response	15. Identification & authentication 16. Logical access controls 17. Audit trails

Security Awareness & Training Control Objectives

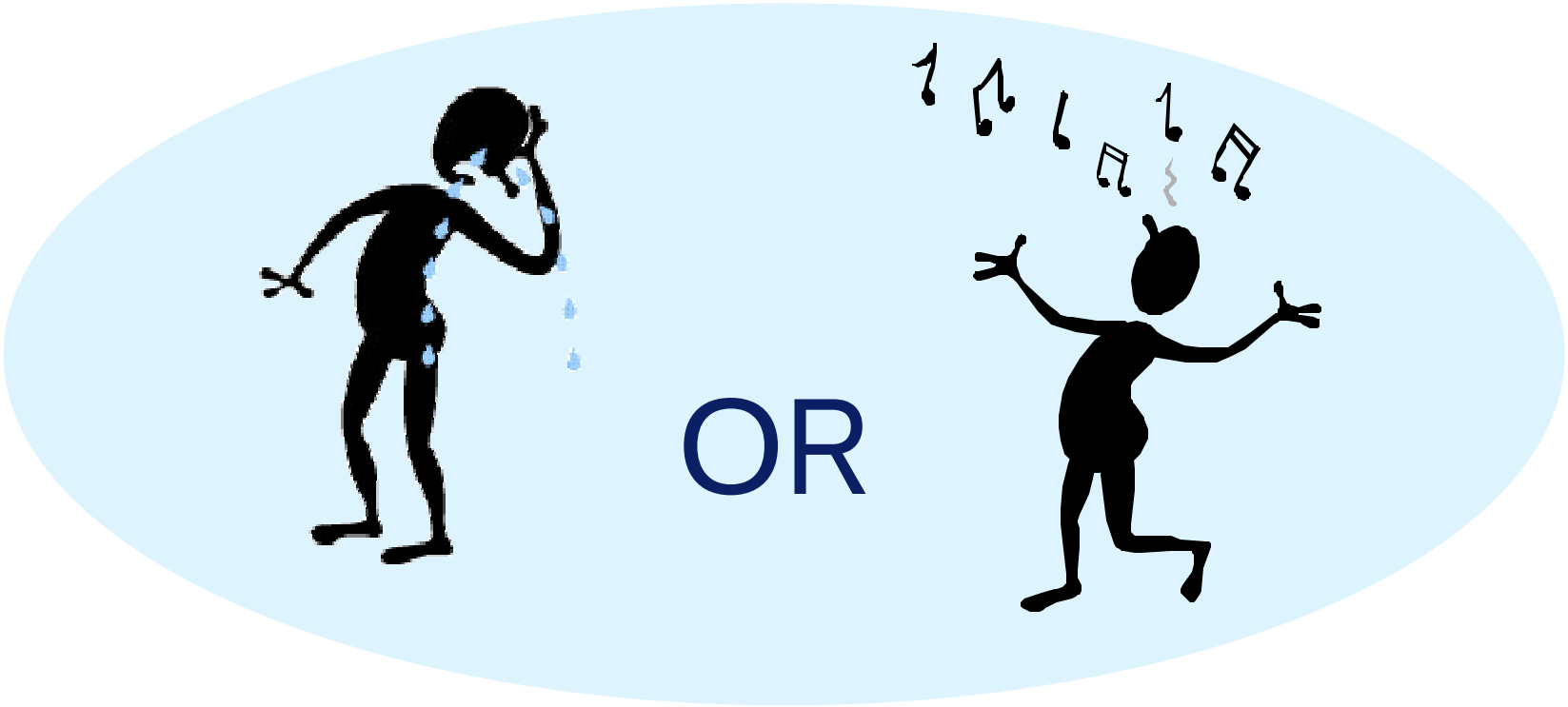
Security Awareness, Training and Education	OMB A-130, III
Critical Element 1: Have employees received adequate training to fulfill their security responsibilities?	
Have employees received a copy of the Rules of Behavior?	NIST SP 800-18
Are employee training and professional development documented and monitored?	FISCAM SP-4.2
Is there mandatory annual refresher training?	OMB A-130, III
Are methods employed to make employees aware of security, I.e., posters, booklets?	NIST SP 800-18
Have employees received a copy of or have easy access to agency security procedures and policies?	NIST SP 800-18

OMB FY 2001 GISRA Findings

OMB's review of over 50 agency reports identified six government-wide security problems—

1. **Senior management attention**
2. **Measuring performance**
3. **Security education and awareness**
4. **Funding and integrating security into capital planning and investment control**
5. **Ensuring that contractor services are adequately secure**
6. **Detecting, reporting, and sharing information on vulnerabilities**

OMB FY 2002 GISRA Findings (TBD)



Security Awareness and Training Has Been Neglected

- GISRA FY 2001
  - Study 6, CIO Performance Measures reported on Measures of performance used by the agency to ensure the CIO has effectively implemented and maintained security programs, and trained employees
  - Study 7, Security Training reported on how the agency ensures employees are sufficiently trained
- Congressman Horn Security Report Cards

Achieving ITSAF Level 5

- Requirements
  - A comprehensive security program that is an integral part of an agency's organizational culture
  - Decision-making based on cost, risk, and mission impact
- Criteria that describe a fully integrated security program
  - A cost-effective enterprise-wide security program
  - Integrated IT security practices within the asset
  - Security vulnerabilities are understood and managed
  - Threats are continually re-evaluated, and controls adapted to changing security environment
  - Additional or more cost-effective security alternatives are identified as the need arises
  - Costs and benefits of security are measured appropriately
  - Status metrics for the security program are established and met

NIST 800-50 Provides a Blueprint

- Introduction
- Components: Awareness, Training, Education
- Building a Strategy
- Developing Awareness and Training Material
- Implementing the Awareness and Training Program
- Post-Implementation

A Model for Success

Cyber Security Awareness Program for all employees and contractors

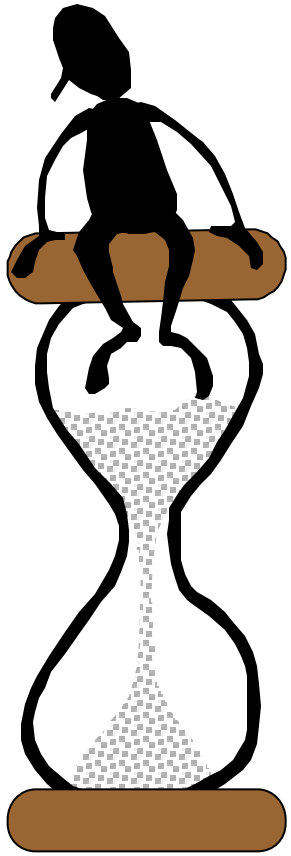
Cyber Security "Essentials" for System Users

Cyber Security "Fundamentals" for Management, IT, and Security Personnel

Management Controls Training	Operational Controls Training	Technical Controls Training
• Managing an Enterprise-wide Security Program • Capital Planning • Risk Management • Security Plans • Certification and Accreditation • Security and Life Cycle Planning • Independent Review of security controls	• Personnel Security • Physical Security • Input/Output Controls • Contingency Planning • Maintenance Procedures • Documentation – Policy – Procedure Guides • Awareness and Training • Incident Response	• Identification and Authentication • Logical Access Controls • System Monitoring Tools • System Auditing Tools • Anti-Virus • Encryption • Firewalls • LAN/WAN Security • Host Security • Server Security

A Time for Change

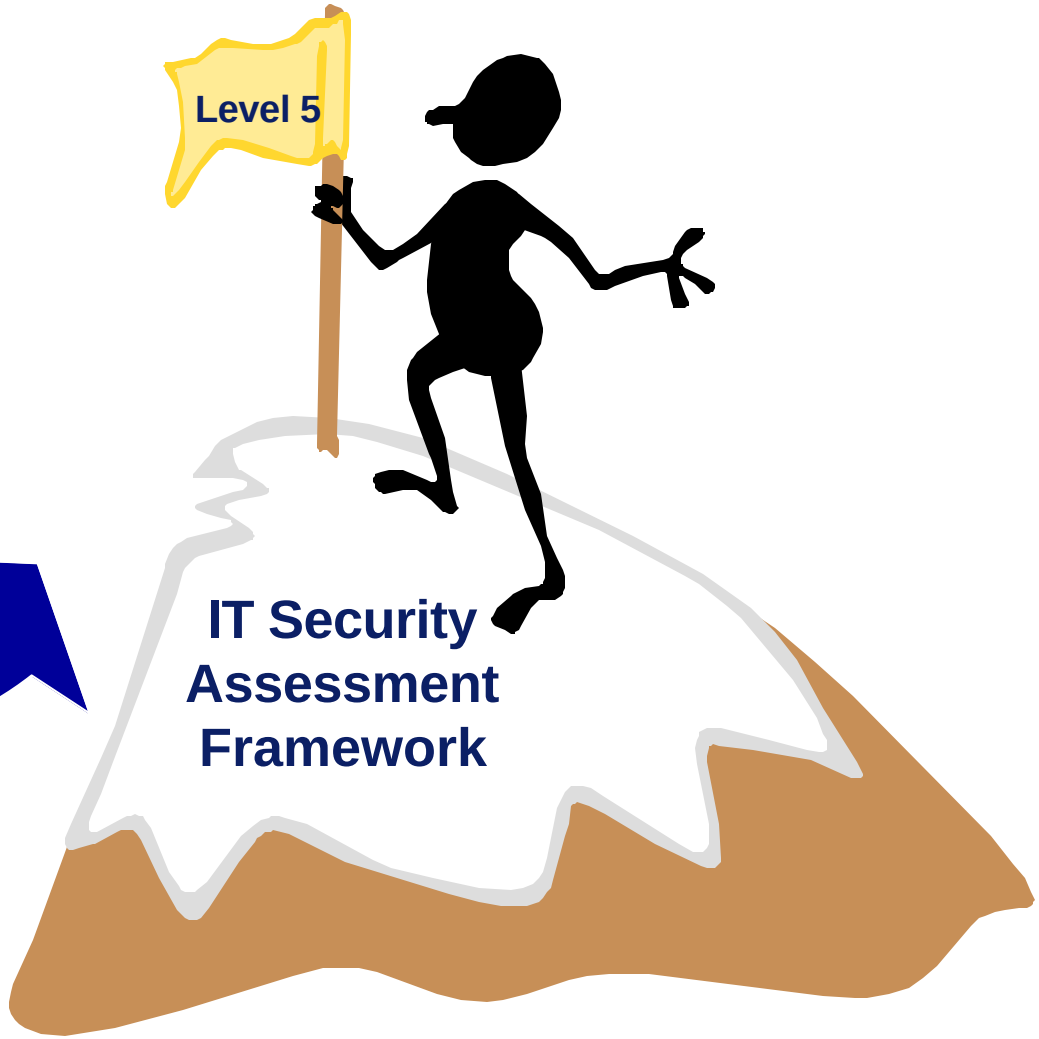
- Develop the business case to support your security awareness and training program
- Deliver the message to senior officials and managers—successful security awareness and training programs are an effective countermeasure for reducing risk
- Link development of security awareness and training program to management's Government Performance and Results Act (GPRA) goals
- Develop training to address the "when, what, where, why, and how" of security
- Build effective programs to improve competencies and security performance



Cause and Effect

Effective Security Awareness and Training Program

LEADS TO



Security Awareness and Training—The Neglected Countermeasure

Federal Information System Security Educators Association

16th Annual Conference

March 5, 2003

Thanks for attending this session!

Prepared by:
Marge Spanninger
Booz Allen Hamilton
(703) 289-5471
spanninger_margaret@bah.com

Booz | Allen | Hamilton