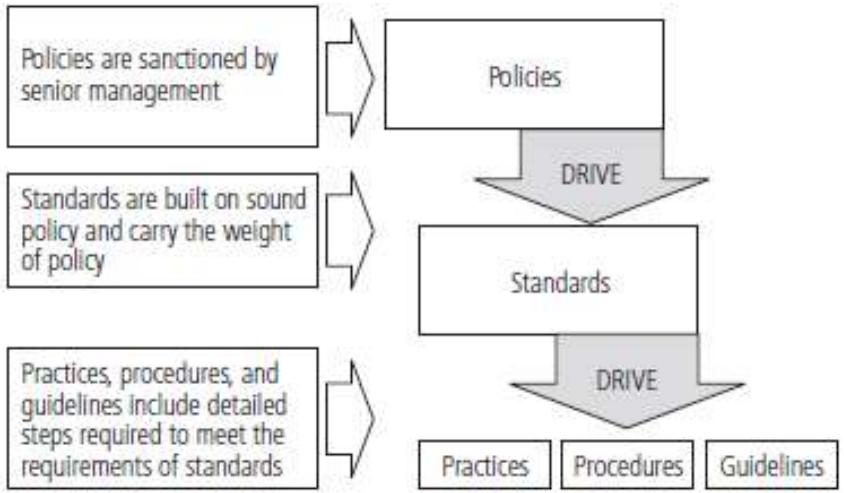
Security Policies and Standards

Introduction

- Organization
  - Collection of people working together toward a common goal
- Must have clear understanding of the rules of acceptable behavior
- Policy
  - Conveys management's intentions to its employees
- Effective security program
  - Use of a formal plan to implement and manage security in the organization

Policies, Standards, and Procedures

- Policy
  - Set of guidelines or instructions
  - Organization's senior management implements
  - Idea
- Standards
  - More detailed descriptions of what must be done to comply with policy
  - Specifics and outline
- Procedures
  - How to accomplish the policies and standards



Effective Policies

- For a policy to be considered effective and legally enforceable:
  - Dissemination
    - Distribution of the information
    - Is it in a readily available place?
  - Review
    - Has it been read?
    - Who is reading it?
  - Comprehension
    - Is it understandable?
    - Too confusing?
  - Compliance
    - Acknowledge vs. Agree
  - Uniform enforcement
    - How are violations being handled?

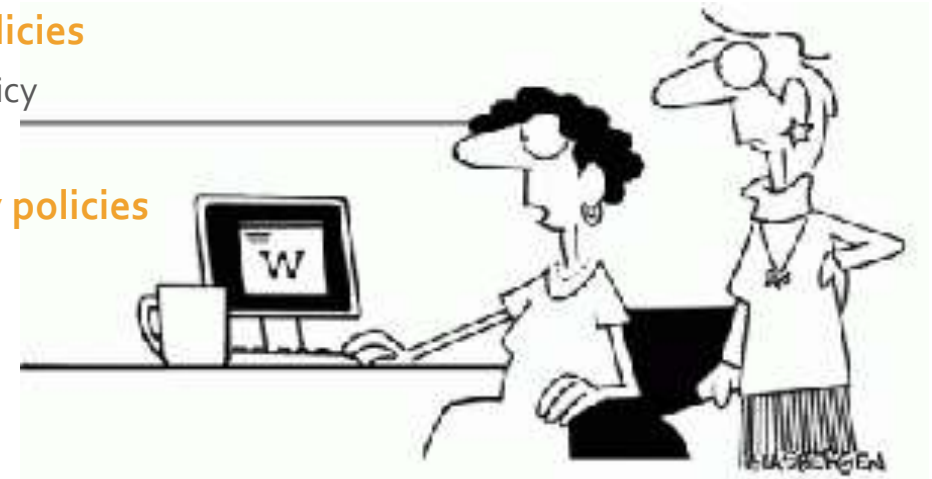
What Drives Policy Development?

- Mission of an organization
  - Written statement of purpose of organization
  - Usually Not Modified
- Vision of an organization
  - Witten statement of the organization's long-term goals
  - Occasionally Modified
- Strategic planning
  - Process of moving the organization toward its vision.
  - Constantly Reworked to promote progress
- Security policy
  - Set of rules that protects an organization's assets

- **Question:** What are some security policies you are aware of?

Types of Information Security Policies

- Information security policy
  - Set of rules for the protection of an organization's information assets
    - **Enterprise information security policies**
      - General security policy
    - **Issue-specific security policies**
      - Specific technology policy
    - **Systems-specific security policies**
      - Configurations



Enterprise Information Security Policy (EISP)

- Supports the mission, vision, and direction of the organization
- Sets the strategic direction, scope, and tone for all security efforts
- Executive-level document
- Drafted by organization's chief information officer
- Expresses the security philosophy within the IT environment
- Guides the development, implementation, and management of the security program
- Address an organization's need to comply with laws and regulations in two ways:
  - General compliance
  - Identification of specific penalties and disciplinary actions

Components of EISP

Component	Description
Statement of Purpose	Answers the question, "What is this policy for?" Provides a framework that helps the reader understand the intent of the document. Here's a sample Statement of Purpose: "This document will: identify the elements of a good security policy explain the need for information security specify the various categories of information security identify the information security responsibilities and roles identify appropriate levels of security through standards and guidelines This document establishes an overarching security policy and direction for our company. Individual departments are expected to establish standards, guidelines, and operating procedures that adhere to and reference this policy while addressing their specific and individual needs."[5]
Information Technology Security Elements	Defines information security. For example: "Protecting the confidentiality, integrity, and availability of information while in processing, transmission, and storage through the use of policy, education and training, and technology...." This section can also lay out security definitions or philosophies to clarify the policy.
Need for Information Technology Security	Provides information on the importance of information security in the organization and the obligation (legal and ethical) to protect critical information about customers, employees, and markets.
Information Technology Security Responsibilities and Roles	Defines the organizational structure designed to support information security. Identifies categories of individuals with responsibility for information security (IT department, management, users) and their information security responsibilities, including maintenance of this document.
Reference to Other Information Technology Standards and Guidelines	Lists other standards that influence and are influenced by this policy document, perhaps including relevant laws (federal and state) and other policies.

Issue-Specific Security Policy (ISSP)

- Addresses specific areas of technology
- Requires frequent updates
- Contains a statement on the organization's position on a specific issue
- May cover:
  - Use of company-owned networks and the Internet
  - Use of telecommunications technologies (fax and phone)
  - Use of electronic mail
  - Specific minimum configurations of computers to defend against worms and viruses
  - Prohibitions against hacking or testing organization security controls
  - Home use of company-owned computer equipment
  - Use of personal equipment on company networks
  - Use of photocopy equipment

Components of ISSP

Component	Description
1. Statement of policy a. Scope and applicability b. Definition of technology addressed c. Responsibilities	The policy should begin with a clear statement of purpose.
2. Authorized access and usage a. User access b. Fair and responsible use c. Protection of privacy	This section addresses *who* can use the technology governed by the policy and *what* it can be used for. An organization's information systems are the exclusive property of the organization, and users have no general rights of use. Each technology and process is provided for business operations. Use for any other purpose constitutes misuse.
3. Prohibited usage a. Disruptive use or misuse b. Criminal use c. Offensive or harassing materials d. Copyrighted, licensed, or other intellectual property e. Other restrictions	Unless a particular use is clearly prohibited, the organization cannot penalize its employees for using it in that fashion.
4. Systems management a. Management of stored materials b. Employer monitoring c. Virus protection d. Physical security e. Encryption	This section focuses on users' relationships to systems management. It is important that all such responsibilities be designated to either the systems administrators or the users; otherwise, both parties may infer that the responsibility belongs to the other party.
5. Violations of policy a. Procedures for reporting violations b. Penalties for violations	This section specifies the penalties for each category of violation as well as instructions on how individuals in the organization can report observed or suspected violations. Allowing anonymous submissions is often the only way to convince users to report the unauthorized activities of other, more influential employees.
6. Policy review and modification a. Scheduled review of policy and procedures for modification	Because a document is only useful if it is up to date, each policy should contain procedures and a timetable for periodic review. This section should specify a methodology for the review and modification of the policy, to ensure that users do not begin circumventing it as it grows obsolete.
7. Limitations of liability a. Statements of liability or disclaimers	If an employee is caught conducting illegal activities with organizational equipment or assets, management does not want the organization held liable. The policy should state that the organization will not protect employees who violate a company policy or any law using company technologies, and that the company is not liable for such actions.

Systems-Specific Policy (SysSP)

- Appear with the managerial guidance expected in a policy
- Include detailed technical specifications not usually found in other types of policy documents
- Managerial Guidance SysSPs
  - Guide the implementation and configuration of a specific technology
- Technical Specifications SysSPs
  - General methods for implementing technical controls
- Access control lists
  - Set of specifications that identifies a piece of technology's authorized users and includes details on the rights and privileges those users have on that technology
- Access control matrix
  - Combines capability tables and ACLs
- Configuration rules
  - Specific instructions entered into a security system to regulate how it reacts to the data it receives
- Rule-based policies
  - More specific to a system's operation than ACLs
  - May or may not deal with users directly

Frameworks and Industry Standards

- Security blueprint
  - Basis for the design, selection, and implementation of all security program elements
- Security framework
  - Outline of the overall information security strategy
  - Roadmap for planned changes to the organization's information security environment
    - The ISO 27000 Series
    - NIST Model

NIST Security Models

- Computer Security Resource Center (CSRC) publications
  - SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
    - Lists the principles and practices to be used in the development of a security blueprint
  - SP 800-41 Rev. 1: Guidelines on Firewalls and Firewall Policy
    - Provides an overview of the capabilities and technologies of firewalls and firewall policies
  - SP 800-53 Rev. 3: Recommended Security Controls for Federal Information Systems and Organizations
    - Describes the selection and implementation of security controls for information security to lower the possibility of successful attack from threats
  - SP 800-53 A, Jul 2008: Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans
    - Provides a systems developmental lifecycle approach to security assessment of information systems

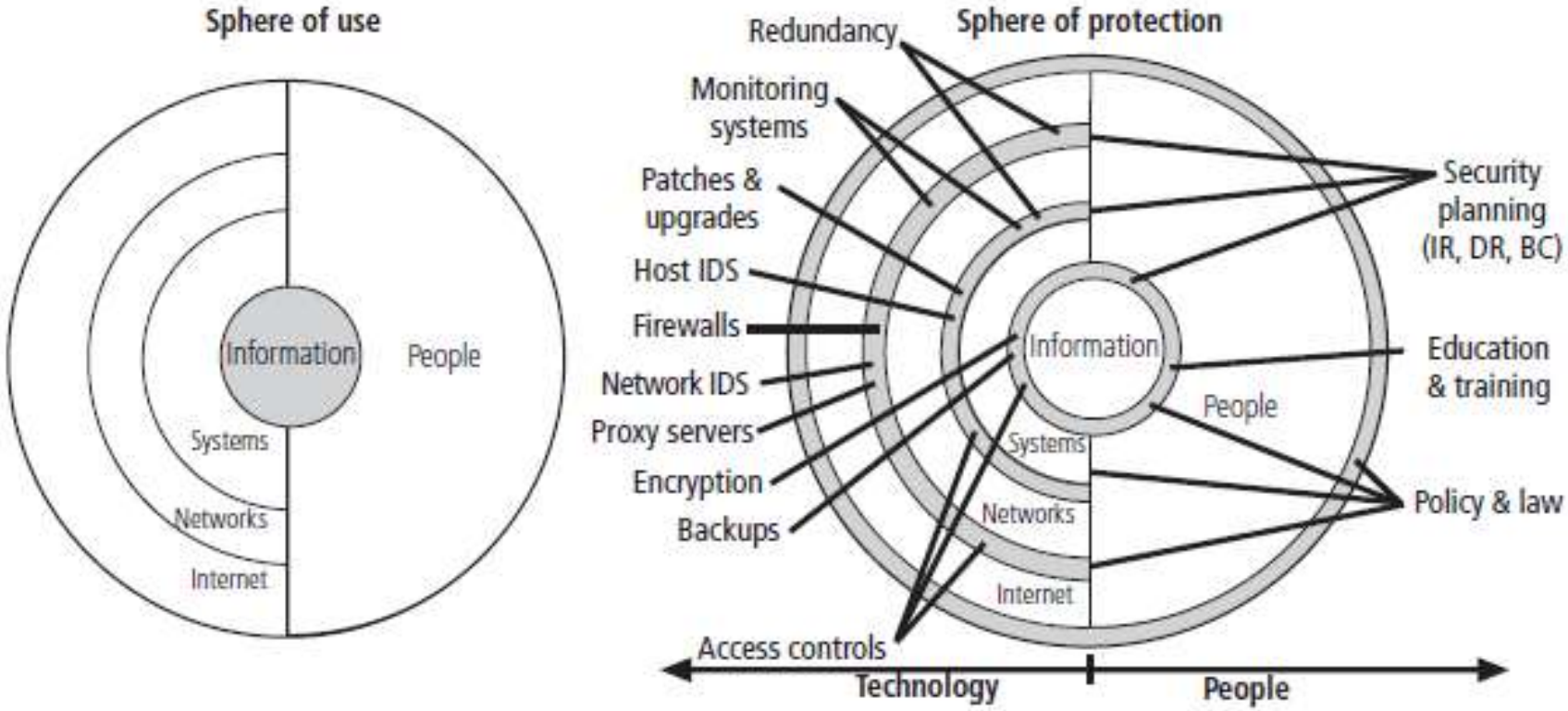
Other NIST Perimeter Defense Publications

Other NIST Special Publications of Interest for Perimeter Defense
SP 800-36: Guide to Selecting Information Technology Security Products
SP 800-40 Version 2.0: Creating a Patch and Vulnerability Management Program
SP 800-46 Rev. 1: Guide to Enterprise Telework and Remote Access Security
SP 800-47: Security Guide for Interconnecting Information Technology Systems
SP 800-48 Rev. 1: Guide to Securing Legacy IEEE 802.11 Wireless Networks
SP 800-51: Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
SP 800-61 Rev. 1: Computer Security Incident Handling Guide
SP 800-77: Guide to IPsec VPNs
SP 800-83: Guide to Malware Incident Prevention and Handling
SP 800-92: Guide to Computer Security Log Management
SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)
SP 800-113: Guide to SSL VPNs
SP 800-114: User's Guide to Securing External Devices for Telework and Remote Access

Benchmarking and Best Practices

- Best practices
  - Procedures that are accepted or prescribed as being correct or most effective
- Benchmarking
  - Evaluation against a standard
    - Spheres of security - Generalized foundation of a good security framework
    - Controls -Implemented between systems and the information, between networks and the computer systems, and between the Internet and internal networks
    - Information security - Designed and implemented in three layers: policies, people (education, training, and awareness programs), and technology

Spheres of Security



Security Education, Training, and Awareness Program

- Education, training, and awareness (SETA) program
- Responsibility of the CISO
- Control measure designed to reduce the incidences of accidental security breaches by employees
- Designed to supplement the general education and training programs

Purpose of SETA

- The Program Elements:
  - Security education
    - Provide Opportunity , Inform
    - The Why
  - Security training
    - Hands-on Education and Experience
    - The How
  - Security awareness
    - Reinforce
    - The What
- Purpose of SETA is to enhance security by:
  - Improving awareness of the need to protect system resources
  - Developing skills and knowledge so computer users can perform their jobs more securely
  - Building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems

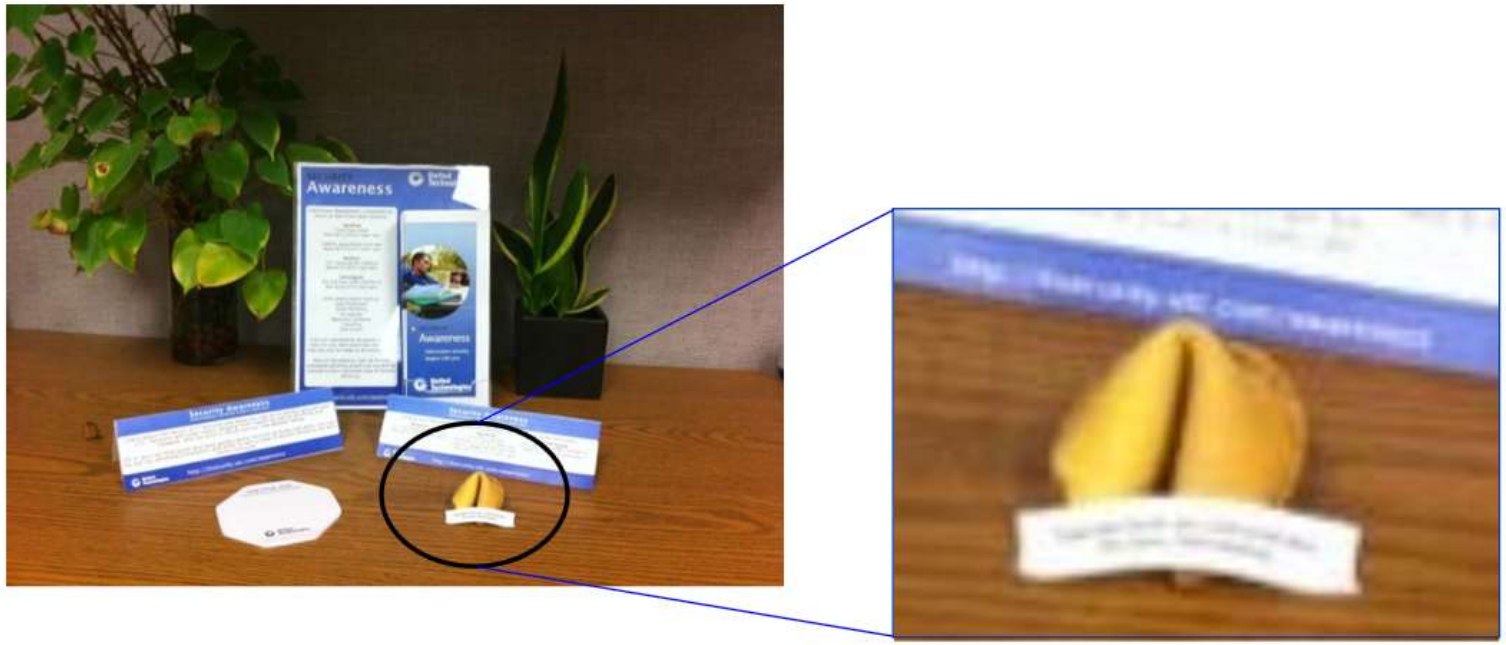
Security Awareness Example

Security Awareness Example

Security Awareness Example

Security Awareness Example

UTC AWARENESS COOKIE



"Sharing personal information on social networking sites can make you vulnerable to identify theft, targeted phishing attacks, and robbery" *

Summary

- Policy
  - Basis for all information security planning, design, and deployment
- Security team develops a design blueprint used to implement the security program
- Implement a security education, training, and awareness (SETA) program
  - Supplement the general education and training programs