INFORMATION SECURITY POLICY

Week 6-7

LEARNING OBJECTIVES

- Define Information security policy and understand its central role in a successful information security program
- Recognize the three major types of information security policy and know what goes into each type
- Develop, implement, and maintain various types of information security policies

INTRODUCTION

- The success of any information security program lies in policy development
- Policy is the essential foundation of an effective information security program
- The centrality of information security polices to virtually everything that happens in the information security field
- An elective information security training and awareness effort cannot be initiated without writing information security policies

NIST—Executive Guide to the Protection of Information Resources

- "The success of an information resources protection program depends on the policy generated, and on the attitude of management toward securing information on automated systems. You, the policy maker, set the tone and the emphasis on how important a role information security will have within your agency. Your primary responsibility is to set the information resource security policy for the organization within the objectives of reduced risk, compliance with laws and regulations and assurance of operational continuity, information integrity, and confidentiality."

BASIC RULES IN SHAPING A POLICY

- Policy should never conflict with law
- Policy must be able to stand up in court, if challenged
- Policy must be properly supported and administered
- Example: Enron's dubious business practices and misreporting the financial records - Policy of shredding working papers by accountants

WHY POLICY

- A quality information security program begins and ends with policy
- Although information security policies are the least expensive means of control to execute, they are often the most difficult to implement
- Policy controls cost only the time and effort that the management team spends to create, approve and communicate them, and that employees spend integrating the policies into their daily activities
- Cost of hiring a consultant is minimal compared to technical controls

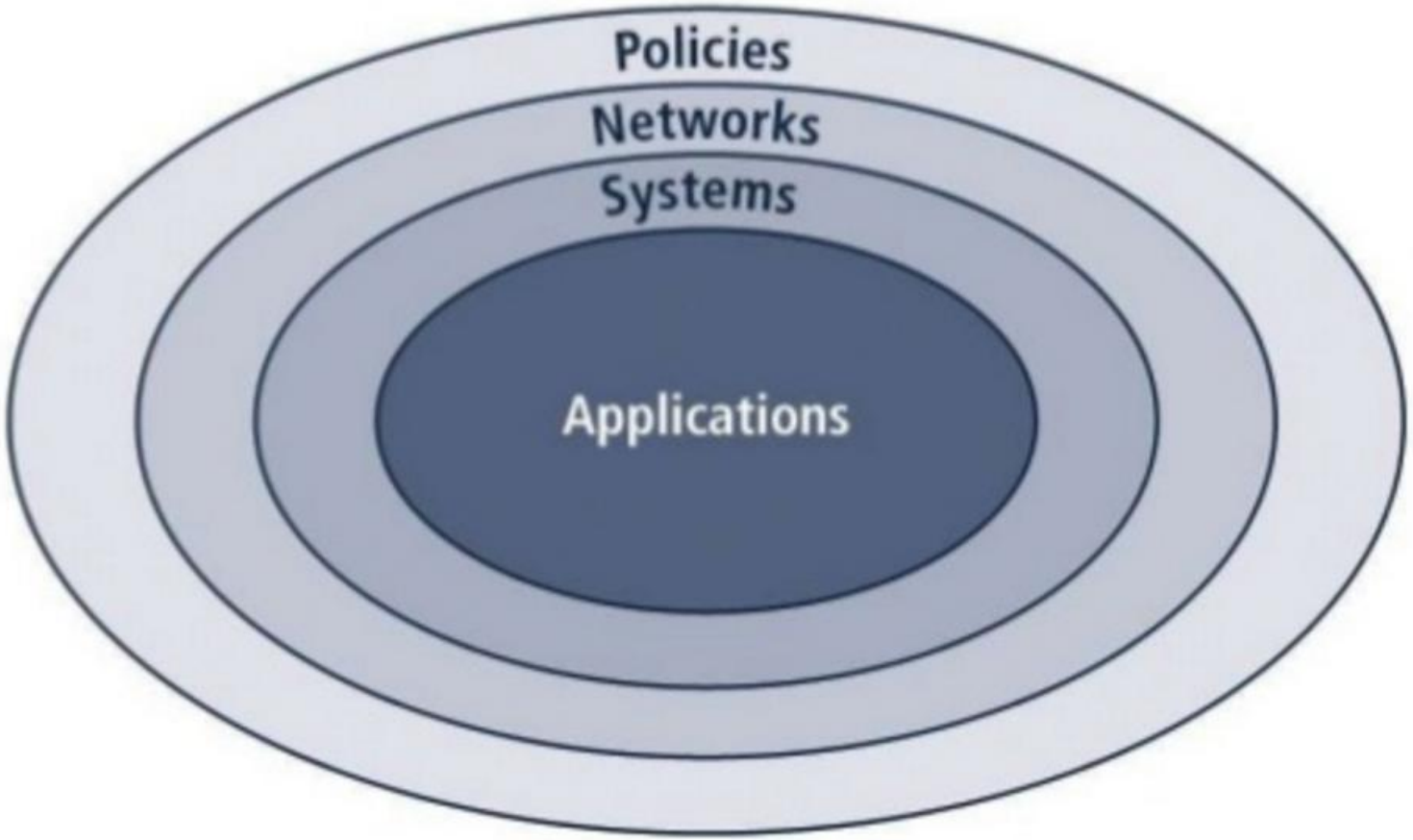
GUIDELINES FOR IT POLICY

- All policies must contribute to the success of the organization
- Management must ensure the adequate sharing of responsibility for proper use of information systems
- End users of information systems should be involved in the steps of policy formulation

BULL'S EYE MODEL

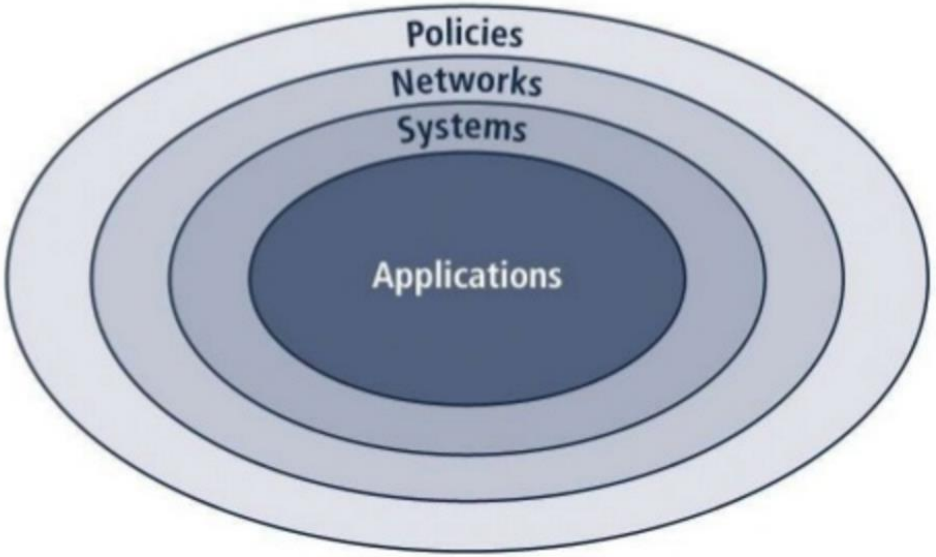
- Proven mechanism for prioritizing complex changes
- Issues are addressed by moving from general to specifics
- Focus of systemic solutions instead of individual problems

BULL'S EYE MODEL



BULL'S EYE MODEL LAYERS

- **Policies** —the outer layer in the bull's eye diagram
- **Networks** —the place where threats from public networks meet the organization's networking infrastructure; in the past, most information security eñorts have focused on networks, and until recently information security was often thought to be synonymous with network security
- **Systems** —computers used as servers, desktop computers, and systems used for process control and manufacturing systems
- **Application** —all applications systems, ranging from packed applications such as oñice automation and e-mail programs, to high-end ERP packages and custom application software developed by the organization



CHARLES CRESSON WOOD'S NEED FOR POLICY

---policies are important reference documents for internal audits and for the resolution of legal disputes about management's due diligence [and] policy documents can act as a clear statement of management's intent...

POLICY,STANDARDS, AND PRACTICES

- Policy represents the formal statement of the organization's managerial policy, in case of our focus, the organization's information security philosophy
- Tradition communities of interest use policy to express their views which then becomes the basis of planning, management and maintenance of the information security profile
- Policies—set of rules that dictate acceptable and unacceptable behavior within an organization
- Policies should not specify the proper operation of equipment or software

POLICY, STANDARDS, AND PRACTICES (CONTD)

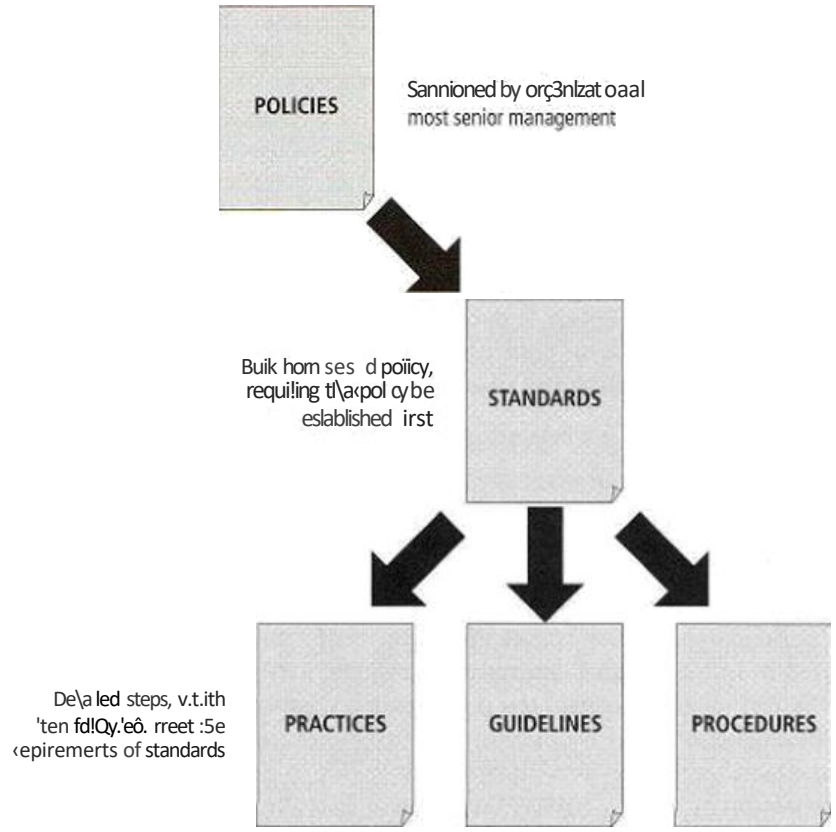


FIGURE 4•2 Polîcles, Standards, and Practices

POLICY, STANDARDS, AND PRACTICES (CONTD)

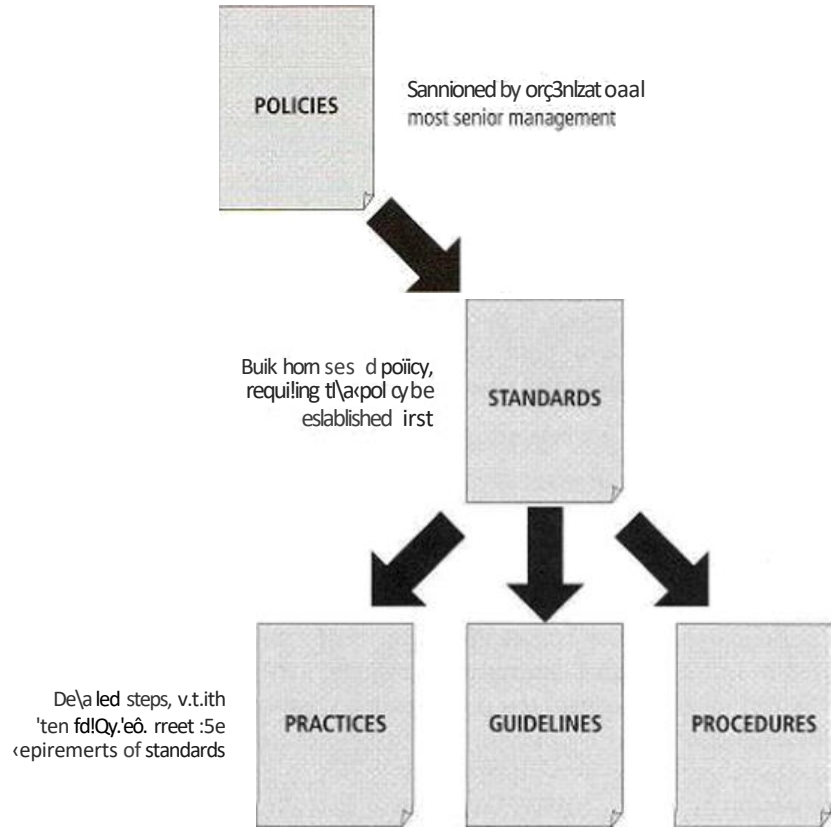


FIGURE 4•2 Polîcles, Standards, and Practices

TYPE OF INFOSEC POLICIES

- Based on NIST Special Publication 800-14, the three types of information security policies are
  - Enterprise information security program policy
  - Issue-specific security policies
  - System-specific security policies
- The usual procedure
  - First – creation of the enterprise information security policy – the highest level of policy
  - Next – general policies are met by developing issue- and system-specific policies

ENTERPRISE INFORMATION SECURITY POLICY (EISP)

- EISP sets the strategic direction, scope, and tone for all of an organization's security eXorts
- EISP assigns responsibilities for the various areas of information security including maintenance of information security policies and the practices and responsibilities of other users.
- EISP guides the development, implementation, and management requirements of the information security program
- EISP should directly support the mission and vision statements

INTEGRATING AN ORGANIZATION'S MISSION AND OBJECTIVES INTO THE EISP

- EISP plays a number of vital roles
- One of the important role is to state the importance of InfoSec to the organization's mission and objectives.
- InfoSec strategic planning derives from IT strategic planning which is itself derived from the organization's strategic planning
- Policy will become confusing if EISP does not directly reflect the above association

EISP ELEMENTS

- An overview of the corporate philosophy on security
- Information on the structure of the InfoSec organization and individuals who fulfill the InfoSec role
- Fully articulated responsibilities for security that are shared by all members of the organization
- Fully articulated responsibilities for security that are *unique to each role* within the organization

COMPONENTS OF A GOOD EISP

- Statement of Purpose
- Information Technology Security Elements
- Need for Information Technology Security
- Information Technology Security Responsibilities and Roles
- Reference to Other Information Technology Standards and Guidelines

ISSUE-SPECIFIC SECURITY POLICY

- Provides a common understanding of the purposes for which an employee can and cannot use a technology
  - —Should not be presented as a foundation for legal prosecution
- Protects both the employee and organization from ine0iciency and ambiguity

EFFECTIVE ISSP

- Articulates expectations for use of technology-basedsystem
- Identifies the processes and authorities that provide documented control
- Indemnifies the organization against liability for an employee's inappropriate or illegal use of the system

ISSP TOPICS

- Use of Internet, e-mail, phone, and office equipment
- Incident response
- Disaster/business continuity planning
- Minimum system configuration requirements
- Prohibitions against hacking/testing security controls
- Home use of company-owned systems
- Use of personal equipment on company networks

ISSP COMPONENTS

- Systems Management
  - Users relationship to systems management
  - Outline users' and administrators' responsibilities
- Violations of Policy
  - Penalties specified for each kind of violation
  - Procedures for (often anonymously) reporting
    - policy violation
- Policy Review/Modification
- Limitations of Liability

ISSP IMPLEMENTATION

- Three common approaches for creating/managing ISSP
  - —Create individual independent ISSP documents, tailored for specific issues
  - —Create a single ISSP document covering all issues
  - —Create a modular ISSP document unifying overall policy creation/management while addressing specific details with respect to individual issues

SYSTEM SPECIFIC SECURITY POLICY (SysSPs)

- SysSPs provide guidance and procedures for configuring specific systems, technologies, and applications
  - —Intrusion detection systems
  - —Firewall configuration
  - —Workstation configuration
- SysSPs are most often technical in nature, but can also be managerial
  - —Guiding technology application to enforce higher level policy (e.g. firewall to restrict Internet access)

GUIDEIINES FOR EFFECTIVE POIICY

- Developed using industry-accepted practices
- Distributed using all appropriate methods
- Reviewed or read by ali employees
- Understood by all employees
- Formally agreed to by act or assertion
- Uniformly applied and enforced

DEVELOPING INFORMATION SECURITY POLICY

- Investigation Phase
- Analysis Phase
- Design Phase
- Implementation Phase
- Maintenance Phase

INVESTIGATION PHASE

- Support from senior management
- Support and active involvement of IT management
- Clear articulation of goals
- Participation by the affected communities of interest
- Detailed outline of the scope of the policy development project

ANALYSIS PHASE

- The analysis phase should produce the following:
  - —A new or recent risk assessment or IT audit documenting the information security needs of the organization.
  - —Gathering of key reference materials — including any existing policies

DESIGN PHASE

- Users or organization members acknowledge they have received and read the policy
  - —Signature and date on a form
  - —Banner screen with a warning

Implementation Phase

- Policy development team writes policies
- Resources:
  - —The Web
  - —Government sites such as NIST
  - —Professional literature
  - —Peer networks
  - —Professional consultants

Maintenance Phase

- Policy development team responsible for monitoring, maintaining, and modifying the policy

POLICY DISTRIBUTION

- Hand policy to employees
- Post policy on a public bulletin board
- E-mail
- Intranet
- Document management system

POLICY READING

- Barriers to employees' reading policies
  - —Literacy: 14º4 of American adults scored "below basic" level in prose literacy
  - —Language: non-English speaking residents

POLICY COMPREHENSION

- Language
  - —At a reasonable reading level
  - —With minimal technical jargon and management terminology
- Understanding of issues
  - —Quizzes

POLICY COMPLIANCE

- Policies must be agreed to act or aFirmation
- Corporations incorporate policy confirmation statements into employment contracts, annual evaluations

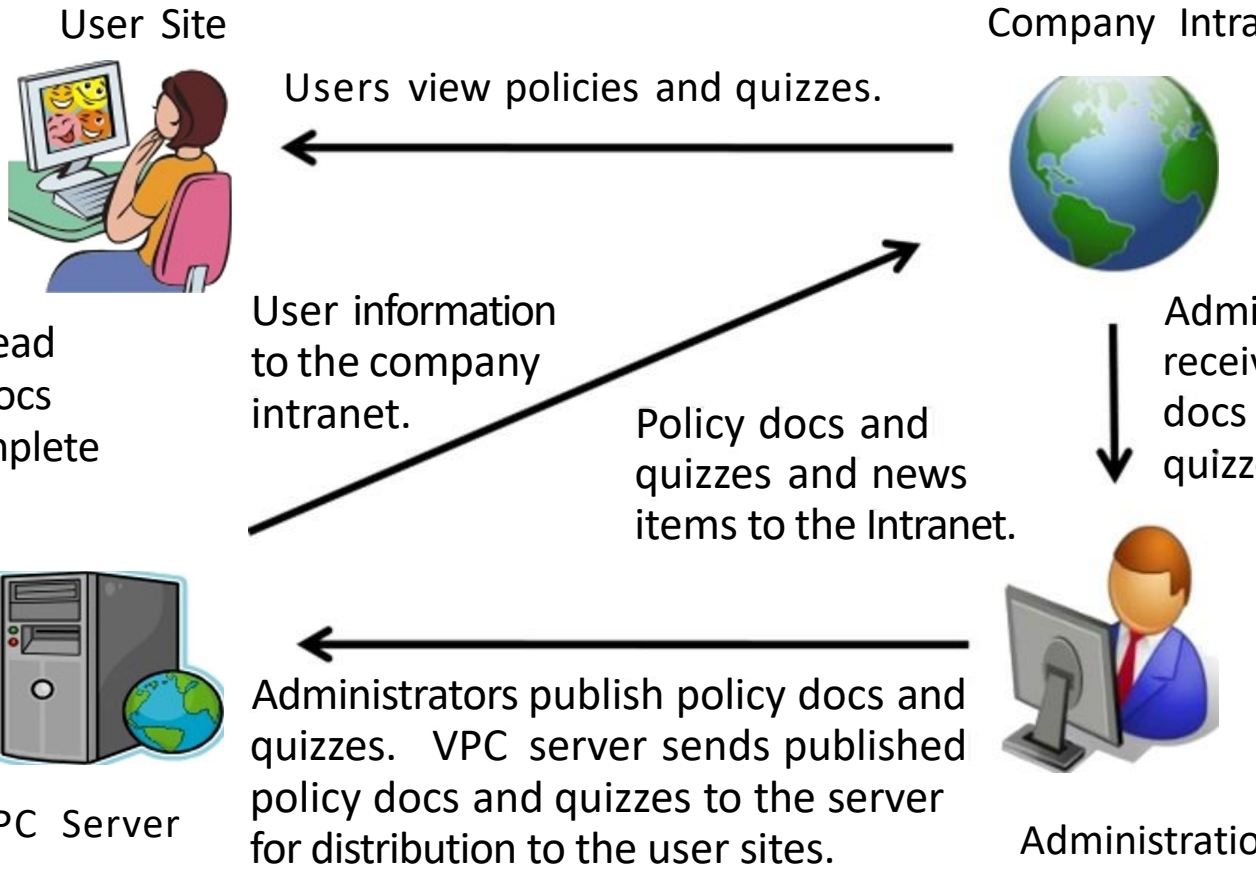
POLICY ENFORCEMENT

- Uniform and impartial enforcement — must be able to withstand external scrutiny
- High standards of due care with regard to policy management to defend against claims made by terminated employees

AUTOMATED TOOLS

- VigilEnt Policy Center —a centralized policy approval and implementation center
  - —Manage the approval process
  - —Reduces need to distribute paper copies
  - —Manage policy acknowledgement forms

VIGILENT POLICY CENTER ARCHITECTURE



POLICY MANAGEMENT

- Policy administrator
- Review schedule
- Review procedures and practices
- Poiicy and revision dates

POLICY ADMINISTRATOR

- Policy administrator
  - —Champion
  - —Mid-level staff member
  - —Solicits input from business and information security communities
  - —Makes sure policy document and subsequent revisions are distributed

REVIEW SCHEDULE

- Periodically reviewed for currency and accuracy, and modified to keep current
  - —Organized schedule of review
  - —Reviewed at least annually
  - —Solicit input from representatives of all a0ected parties, management, and staff

REVIEW PROCEDURES AND PRACTICES

- Easy submission of recommendations
- All comments examined
- Management approved changes implemented

POLICY AND REVISION DATE

- Often published without a date
  —Legal issue —are employees “complying with an out-of-date policy
- Should include date of origin, revision dates
  —don't use “today's date” in the document
- Sunset clause (expiration date)

FINAL NOTE

- Policies are a countermeasure to protect assets from threats
  - —Policies exist to inform employees of acceptable (unacceptable)behavior
  - —Are meant to improve employee productivity and prevent potentially embarrassing situations
  - —Communicate penalties for noncompliance