CYBER LAW AND POLICY

Lesson 6

Information security policies

Objectives

- Upon completion of this material you should be able to:
  - Define information security policy and understand its central role in a successful information security program
  - Describe the three major types of information security policy and explain what goes into each type
  - Develop, implement, and maintain various types of information security policies

Introduction

- Policy is the essential foundation of an effective information security program
  - “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”
- Policy maker sets the tone and emphasis on the importance of information security

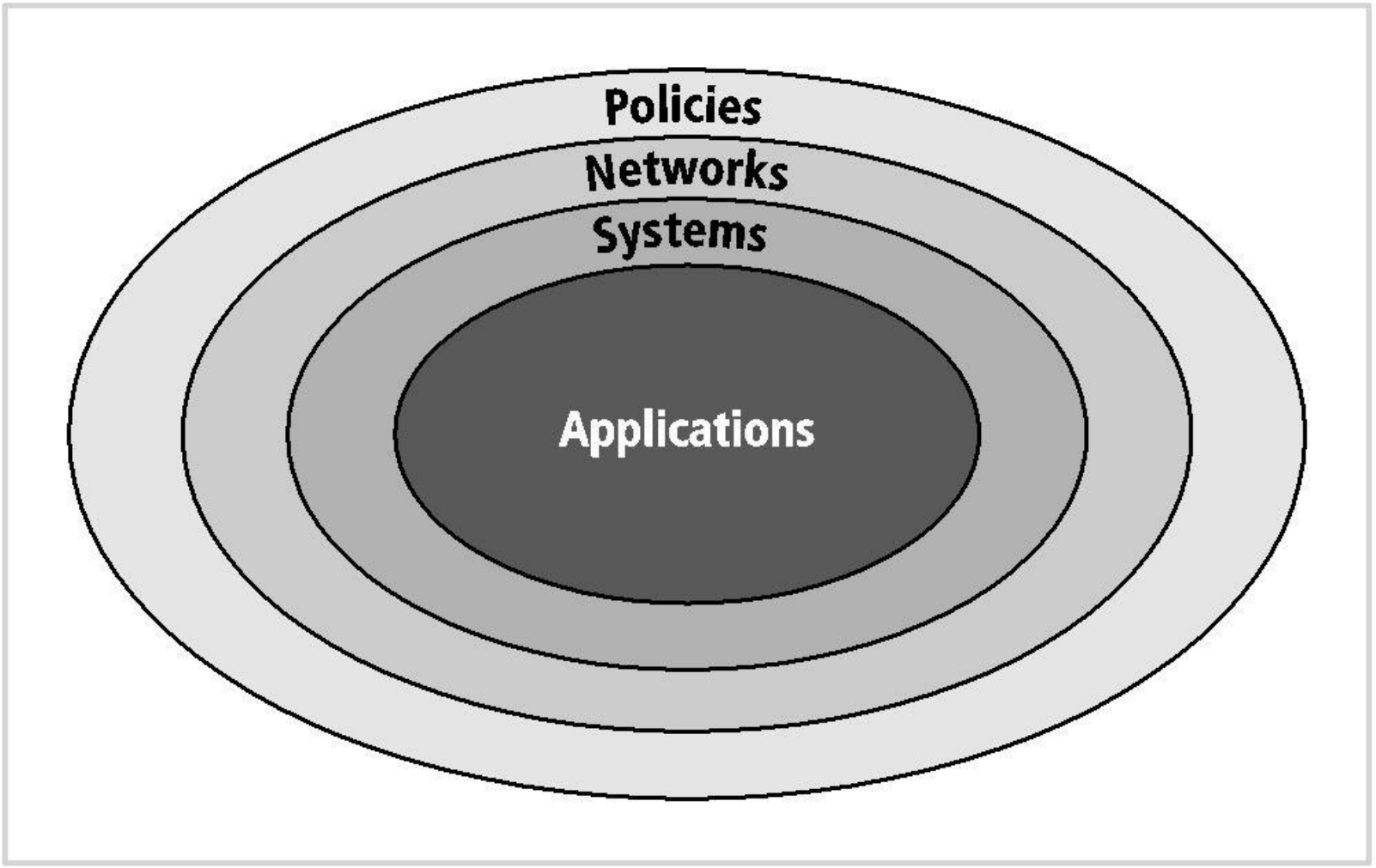
Introduction (cont'd.)

- Policy objectives
  - Reduced risk
  - Compliance with laws and regulations
  - Assurance of operational continuity, information integrity, and confidentiality

Why Policy?

- A quality information security program begins and ends with policy
- Policies are the least expensive means of control and often the most difficult to implement
- Basic rules for 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

Why Policy? (cont'd.)



Why Policy? (cont'd.)

- Bulls-eye model layers
  - Policies: first layer of defense
  - Networks: threats first meet the organization's network
  - Systems: computers and manufacturing systems
  - Applications: all applications systems

Why Policy? (cont'd.)

- Policies are important reference documents
  - For internal audits
  - For the resolution of legal disputes about management's due carefulness
  - Policy documents can act as a clear statement of management's intent

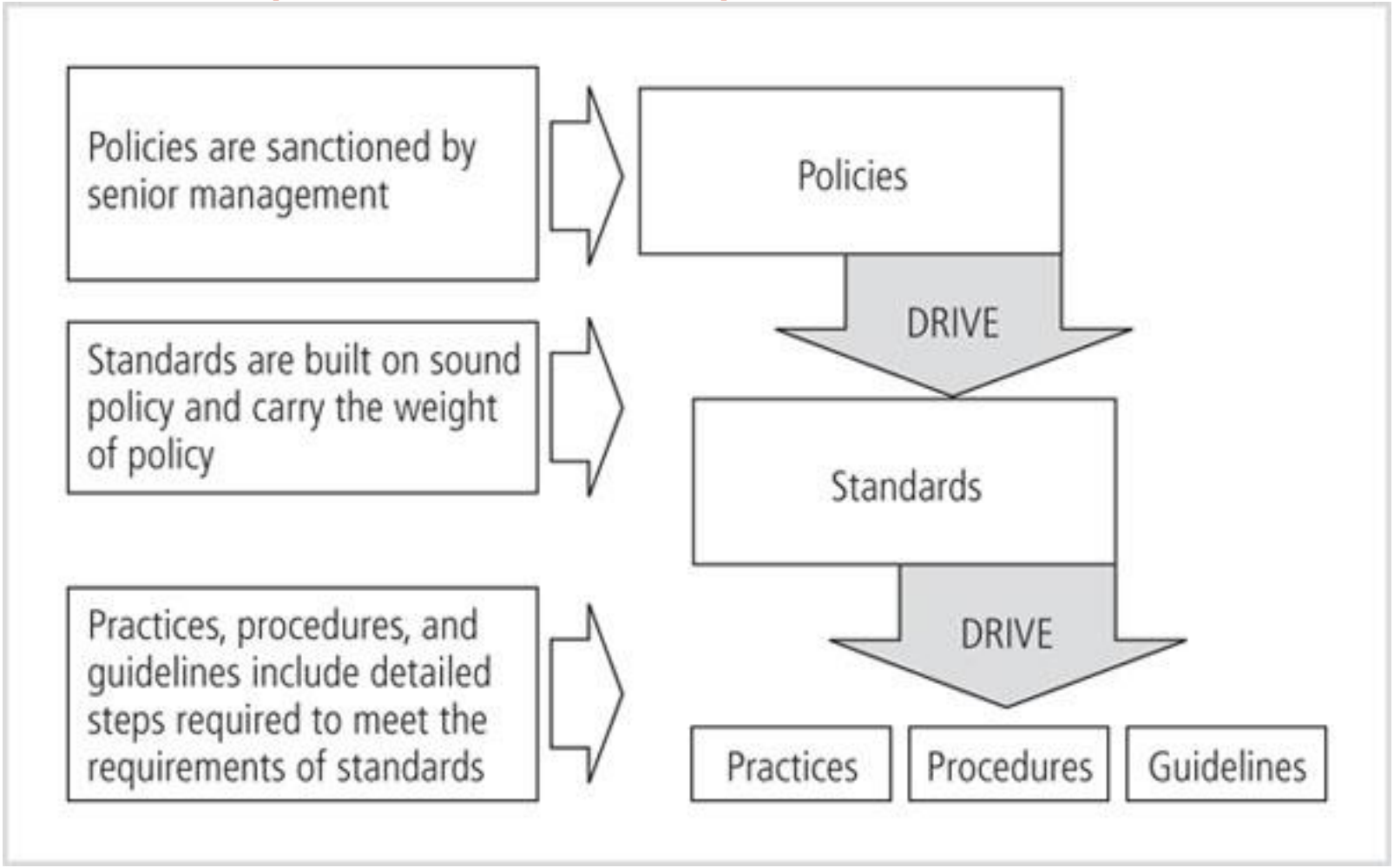
Policy, Standards, and Practices

- Policy
  - A plan or course of action that influences decisions
  - For policies to be effective they must be properly disseminated, read, understood, agreed-to, and uniformly enforced
  - Policies require constant modification and maintenance

Policy, Standards, and Practices (cont'd.)

- Types of information security policy
  - Enterprise information security program policy
  - Issue-specific information security policies
  - Systems-specific policies
- Standards
  - A more detailed statement of what must be done to comply with policy
- Practices
  - Procedures and guidelines explain how employees will comply with policy

Policies, Standards, & Practices



Enterprise Information Security Policy (EISP)

- Sets strategic direction, scope, and tone for organization's security efforts
- Assigns responsibilities for various areas of information security
- Guides development, implementation, and management requirements of information security program

Example EISP Components

- Statement of purpose
  - What the policy is for
- Information security elements
  - Defines information security
- Need for information security
  - Justifies importance of information security in the organization

Example EISP Components (cont'd.)

- Information security responsibilities and roles
  - Defines organizational structure
- Reference to other information security standards and guidelines

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)

- Provides detailed, targeted guidance
  - Instructs the organization in secure use of a technology systems
  - Begins with introduction to fundamental technological philosophy of the organization
- Protects organization from inefficiency and ambiguity
  - Documents how the technology-based system is controlled

Issue-Specific Security Policy (cont'd.)

- Protects organization from inefficiency and ambiguity (cont'd.)
  - Identifies the processes and authorities that provide this control
- Covers the organization against liability for an employee's inappropriate or illegal system use

Issue-Specific Security Policy (cont'd.)

- Every organization's ISSP should:
  - Address specific technology-based systems
  - Require frequent updates
  - Contain an issue statement on the organization's position on an issue

Issue-Specific Security Policy (cont'd.)

- ISSP topics
  - Email and internet use
  - Prohibitions against hacking
  - Home use of company-owned computer equipment
  - Use of personal equipment on company networks
  - Use of telecommunications technologies
  - Use of photocopy equipment

Components of the ISSP

1. Statement of Purpose
   - Scope and applicability
   - Definition of technology addressed
   - Responsibilities
2. Authorized Access and Usage of Equipment
   - User access
   - Fair and responsible use
   - Protection of privacy

Components of the ISSP (cont'd.)

3. Prohibited Usage of Equipment
   - Disruptive use or misuse
   - Criminal use
   - Offensive or harassing materials
   - Copyrighted, licensed or other intellectual property
   - Other restrictions

Components of the ISSP (cont'd.)

4. Systems management
   - Management of stored materials
   - Employer monitoring
   - Virus protection
   - Physical security
   - Encryption
5. Violations of policy
   - Procedures for reporting violations
   - Penalties for violations

Components of the ISSP (cont'd.)

6. Policy review and modification
   - Scheduled review of policy and procedures for modification
7. Limitations of liability
   - Statements of liability or disclaimers

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.

Implementing the ISSP

- Common approaches
  - Several independent ISSP documents
  - A single comprehensive ISSP document
  - A modular ISSP document that unifies policy creation and administration
- The recommended approach is the modular policy
  - Provides a balance between issue orientation and policy management

System-Specific Security Policy

- System-specific security policies (SysSPs) frequently do not look like other types of policy
  - They may function as standards or procedures to be used when configuring or maintaining systems
- SysSPs can be separated into
  - Management guidance
  - Technical specifications
  - Or combined in a single policy document

Managerial Guidance SysSPs

- Created by management to guide the implementation and configuration of technology
- Applies to any technology that affects the confidentiality, integrity or availability of information
- Informs technologists of management intent

Technical Specifications SysSPs

- System administrators' directions on implementing managerial policy
- Each type of equipment has its own type of policies
- General methods of implementing technical controls
  - Access control lists
  - Configuration rules

Technical Specifications SysSPs (cont'd.)

- Access control lists
  - Include the user access lists and capability tables that govern the rights and privileges
  - A similar method that specifies which subjects and objects users or groups can access is called a capability table
  - These specifications are frequently complex matrices, rather than simple lists or tables

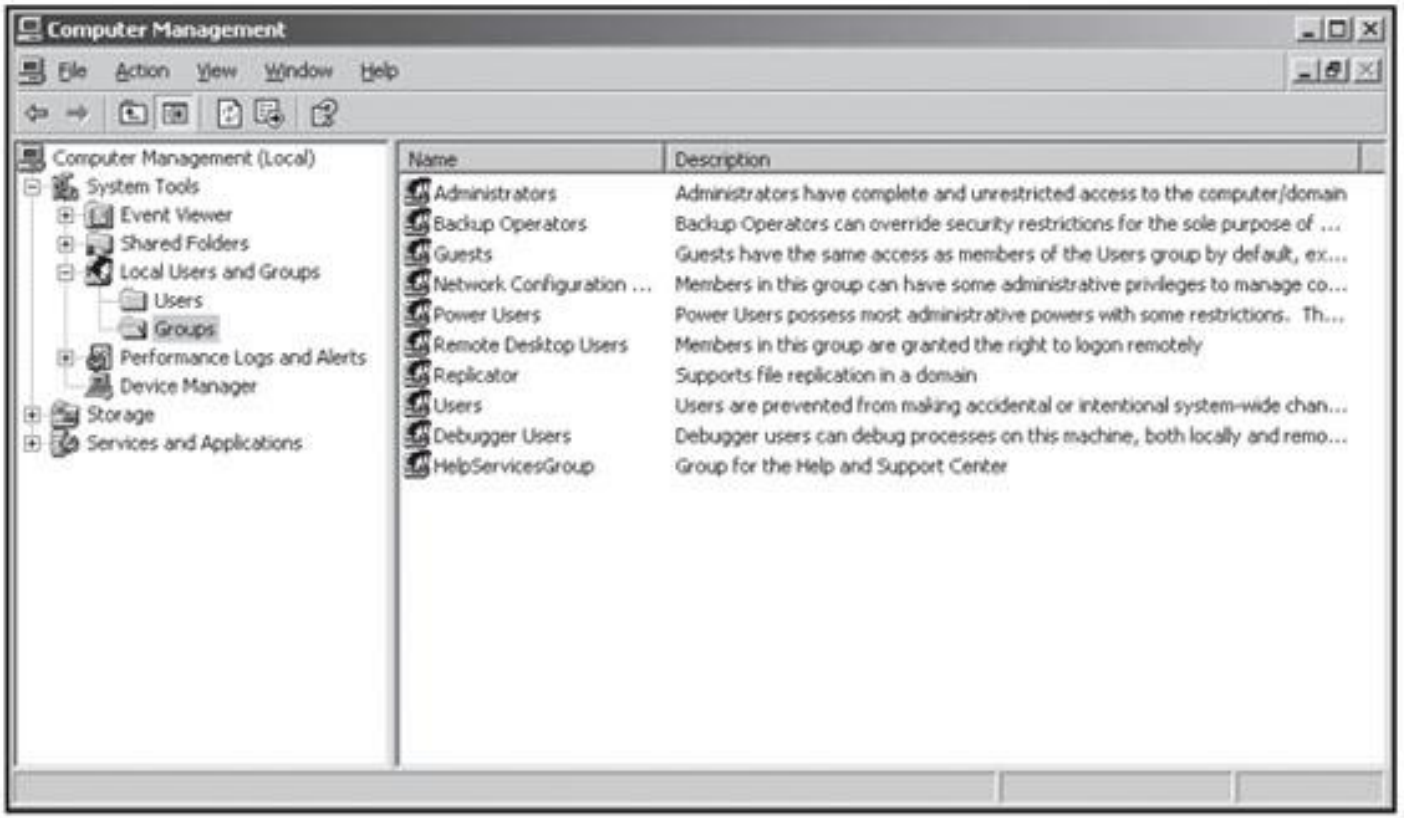
Technical Specifications SysSPs (cont'd.)

- Access control lists (cont'd.)
  - Enable administrations to restrict access according to user, computer, time, duration, or even a particular file
- Access control lists regulate
  - Who can use the system
  - What authorized users can access
  - When authorized users can access the system

Technical Specifications SysSPs (cont'd.)

- Access control lists regulate (cont'd.)
  - Where authorized users can access the system from
  - How authorized users can access the system
  - Restricting what users can access, e.g. printers, files, communications, and applications
- Administrators set user privileges
  - Read, write, create, modify, delete, compare, copy

Technical Specifications SysSPs (cont'd.)



The list of "built-in" groups specifies which rights individual users have to and within a particular system.

Technical Specifications SysSPs (cont'd.)

- Configuration rules
  - Specific instructions entered into a security system to regulate how it reacts to the data it receives
  - Rule policies are more specific to system operation than ACLs
  - May or may not deal with users directly

Technical Specifications SysSPs (cont'd.)

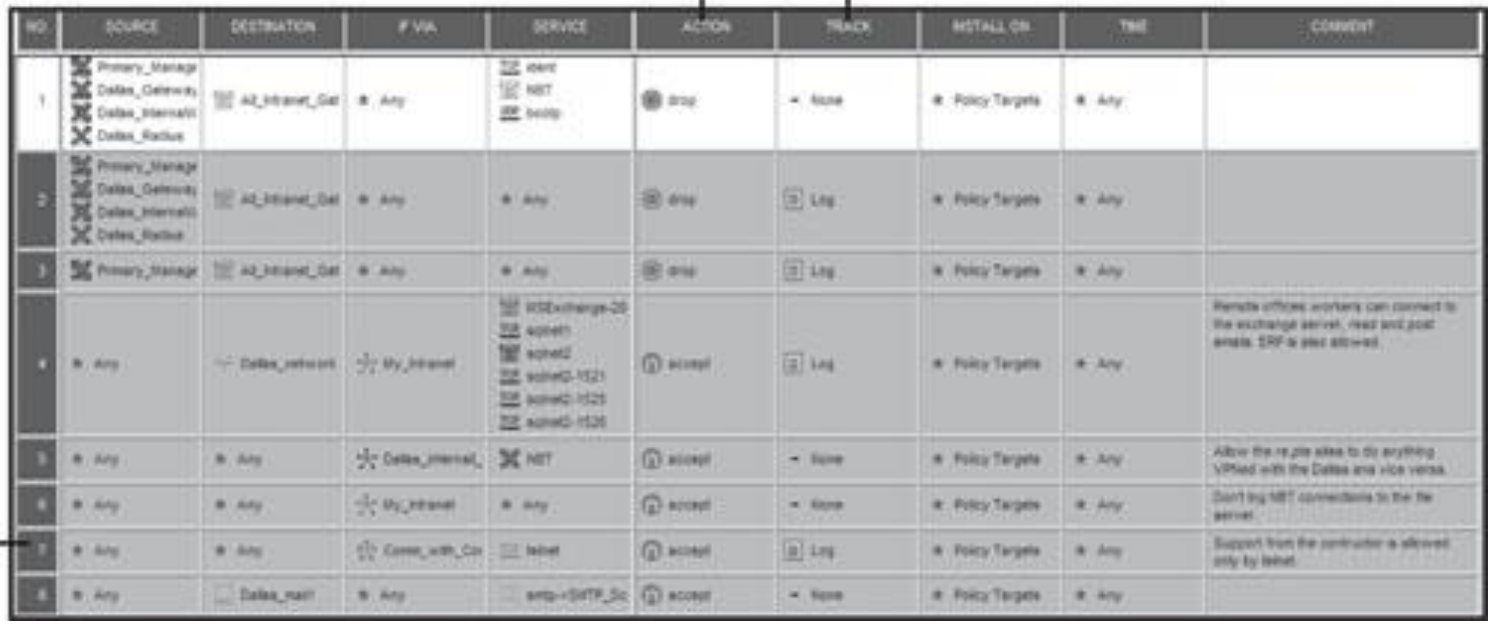
- Many security systems require specific configuration scripts telling the systems what actions to perform on each set of information they process

Technical Specifications SysSPs (cont'd.)

Rule 7 states that any traffic coming in on a specified link (Comm_with_ Contractor) requesting a Telnet session will be accepted, but logged. This rule also implies that non-Telnet traffic will be denied.

Action specifies whether the packet from Source: is accepted (allowed through) or dropped.

Track specifies whether the processing of the specified packet is written to the system logs.



Technical Specifications SysSPs (cont'd.)

- Often organizations create a single document combining elements of both management guidance and technical specifications SysSPs
  - This can be confusing, but practical
  - Care should be taken to articulate the required actions carefully as the procedures are presented


This section defines which security levels are to be used and who is to be notified if that level file is modified.
This section looks for unauthorized modifications to Internet Explorer Registry edits, most likely due to virus or hacker efforts.
This section defines the rules necessary to detect and react to the Nimda virus.
This Policy was created by the Tripwire Policy Resource Center
Created on: Mon Mar 25 21:54:27 GMT 2002
Copyright (C) 2001, Tripwire Inc. Reprinted with permission
@@section global
SYSTEMDRIVE="C:" ;
BOOTDRIVE="C:" ;
SYSTEMROOT="C:\\Winnt" ;
PROGRAMFILES="C:\\Program Files" ;
IES="C:\\Program Files\\Plus!\\Microsoft Internet" ;
# Email Recipients # #
SIG_HIGHEST_MAILRECIPIENTS = "Administrator" ;
SIG_HIGH_MAILRECIPIENTS = "Administrator" ;
SIG_MED_MAILRECIPIENTS = "Administrator" ;
SIG_LOW_MAILRECIPIENTS = "Administrator" ;
# Security Levels # #
SIG_LOW = 33 ; # Non-critical files that are of minimal security impact
SIG_MED = 66 ; # Non-critical files that are of significant security impact
SIG_HIGH = 100 ; # Critical files that are significant points of vulnerability
SIG_HIGHEST = 1000 ; # Super-critical files. Mostly used for the TCB section.
@@section NTFS
(
rulename = "IE 5.01 Registry keys",
severity = $ (SIG_HIGHEST),
emailto = $ (SIG_HIGHEST_MAILRECIPIENTS),
recurse = true
)
{
$ (HKLM_CCS_SM_CBadApps) -> $ (REG_SEC_HIGHEST) ;
$ (HKLM_CRYPT) -> $ (REG_SEC_HIGHEST) ;
$ (HKLM_CRYPTINIT) -> $ (REG_SEC_HIGHEST) ;
$ (HKLM_CRYPTMSG) -> $ (REG_SEC_HIGHEST) ;
$ (HKLM_CRYPTSIGN) -> $ (REG_SEC_HIGHEST) ;
$ (HKLM_EventSystem) -> $ (REG_SEC_HIGHEST) ;
$ (HKLM_SW_IE_Setup) -> $ (REG_SEC_HIGHEST) ;
$ (HKLM_WHM) -> $ (REG_SEC_HIGHEST) ;
$ (HKLM_WIE) -> $ (REG_SEC_HIGHEST) ;
$ (HKLM_WIE_INF_Setup) -> $ (REG_SEC_HIGHEST) ;
$ (HKLM_WMM) -> $ (REG_SEC_HIGHEST) ;
}
# Snippet Name: A Nimda Virus Rule # #
# Snippet Author: support@tripwire.com # #
# Snippet Version: 1.0.0 # #
# Nimda# # #
@@section NTFS
(
rulename = "Nimda File Scan",
Severity = 100
)
{
$ (SYSTEMROOT)\ZaCker.vbs -> $ (IgnoreNone);
$ (SYSTEMROOT)\MixDaLaL.vbs -> $ (IgnoreNone);
$ (SYSTEMDIR)\ZaCker.vbs -> $ (IgnoreNone);
$ (SYSTEMDIR)\MixDaLaL.vbs -> $ (IgnoreNone);
}

Guidelines for Effective Policy

- For policies to be effective, they must be properly:
  - Developed using industry-accepted practices
  - Distributed or disseminated using all appropriate methods
  - Reviewed or read by all employees
  - Understood by all employees
  - Formally agreed to by act or assertion
  - Uniformly applied and enforced

Developing Information Security Policy

- It is often useful to view policy development as a two-part project
  - First, design and develop the policy (or redesign and rewrite an outdated policy)
  - Second, establish management processes to continue the policy within the organization
- The former is an exercise in project management, while the latter requires adherence to good business practices

Developing Information Security Policy (cont'd.)

- Policy development projects should be
  - Well planned
  - Properly funded
  - Aggressively managed to ensure that it is completed on time and within budget
- The policy development project can be guided by the SecSDLC process

Developing Information Security Policy (cont'd.)

- Investigation phase
  - Obtain support from senior management, and active involvement of IT management, specifically the CIO
  - Clearly articulate the goals of the policy project
  - Gain participation of correct individuals affected by the recommended policies

Developing Information Security Policy (cont'd.)

- Investigation phase (cont'd.)
  - Involve legal, human resources and end-users
  - Assign a project champion with sufficient stature and prestige
  - Acquire a capable project manager
  - Develop a detailed outline of and sound estimates for project cost and scheduling

Developing Information Security Policy (cont'd.)

- Analysis phase should produce
  - New or recent risk assessment or IT audit documenting the current information security needs of the organization
  - Key reference materials
    - Including any existing policies

Developing Information Security Policy (cont'd.)

Figure 4-8 End user license agreement for Microsoft Windows XP

Source: Course Technology/Cengage Learning

Developing Information Security Policy (cont'd.)

- Design phase includes
  - How the policies will be distributed
  - How verification of the distribution will be accomplished
  - Specifications for any automated tools
  - Revisions to feasibility analysis reports based on improved costs and benefits as the design is clarified

Developing Information Security Policy (cont'd.)

- Implementation phase includes
  - Writing the policies
    - Making certain the policies are enforceable as written
    - Policy distribution is not always straightforward
    - Effective policy is written at a reasonable reading level, and attempts to minimize technical jargon and management terminology

Developing Information Security Policy (cont'd.)

- Maintenance Phase
  - Maintain and modify the policy as needed to ensure that it remains effective as a tool to meet changing threats
  - The policy should have a built-in mechanism via which users can report problems with the policy, preferably anonymously
  - Periodic review should be built in to the process

Policy Comprehension

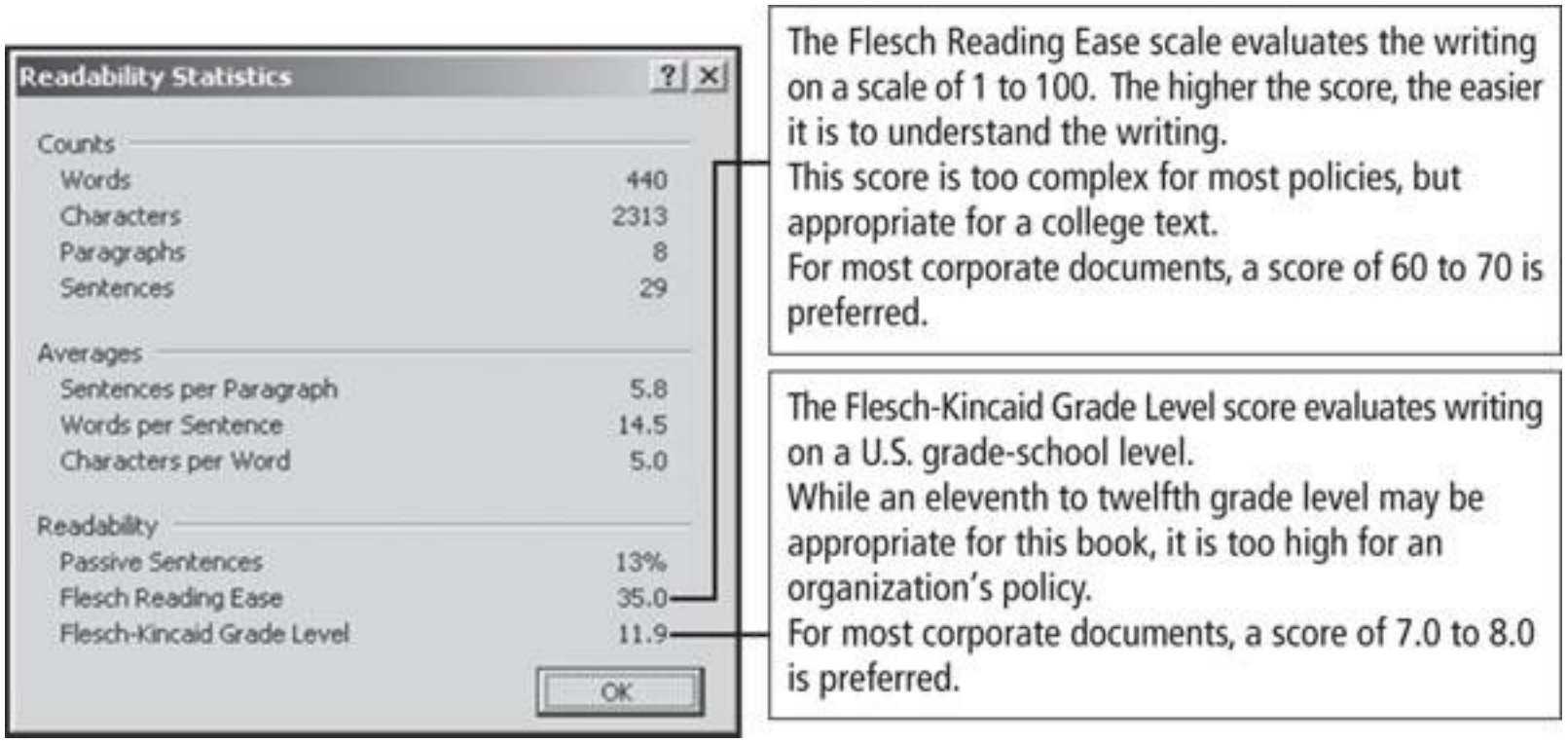


Figure 4-9 Readability statistics

A Final Note on Policy

- Lest you believe that the only reason to have policies is to avoid litigation, it is important to emphasize the preventative nature of policy
  - Policies exist, first and foremost, to inform employees of what is and is not acceptable behavior in the organization
  - Policy seeks to improve employee productivity, and prevent potentially embarrassing situations

Summary

- Introduction
- Why Policy?
- Enterprise Information Security Policy
- Issue-Specific Security Policy
- System-Specific Policy
- Guidelines for Policy Development