UNIT IV LOGICAL DESIGN

Blueprint for Security, Information Security policy, Standards and Practices, ISO 17799/BS 7799, NIST Models, VISA International Security Model, Design of Security Architecture, Planning for Continuity.

Planning for Security -

- Creation of information security program begins with creation and/or review of organization's information security policies, standards, and practices
- Then, selection or creation of information security architecture and the development and use of a detailed information security blueprint creates plan for future success
- Security education and training to successfully implement policies and ensure secure environment

Why Policy?

- A quality information security program begins and ends with policy
- Policies are least expensive means of control and often the most difficult to implement
- Some basic rules must be followed when shaping a policy:
    - Never conflict with law
    - Stand up in court
    - Properly supported and administered
    - Contribute to the success of the organization
    - Involve end users of information systems

Definitions

- **Policy**: course of action used by an organization to convey instructions from management to those who perform duties
    - Organizational rules for acceptable/unacceptable behavior
    - Penalties for violations
    - Appeals process
- **Standards**: more detailed statements of what must be done to comply with policy
- **Practices, procedures and guidelines** effectively explain how to comply with policy
- For a policy to be effective it must be
    - Properly disseminated
    - Read
    - Understood
    - Agreed to by all members of organization

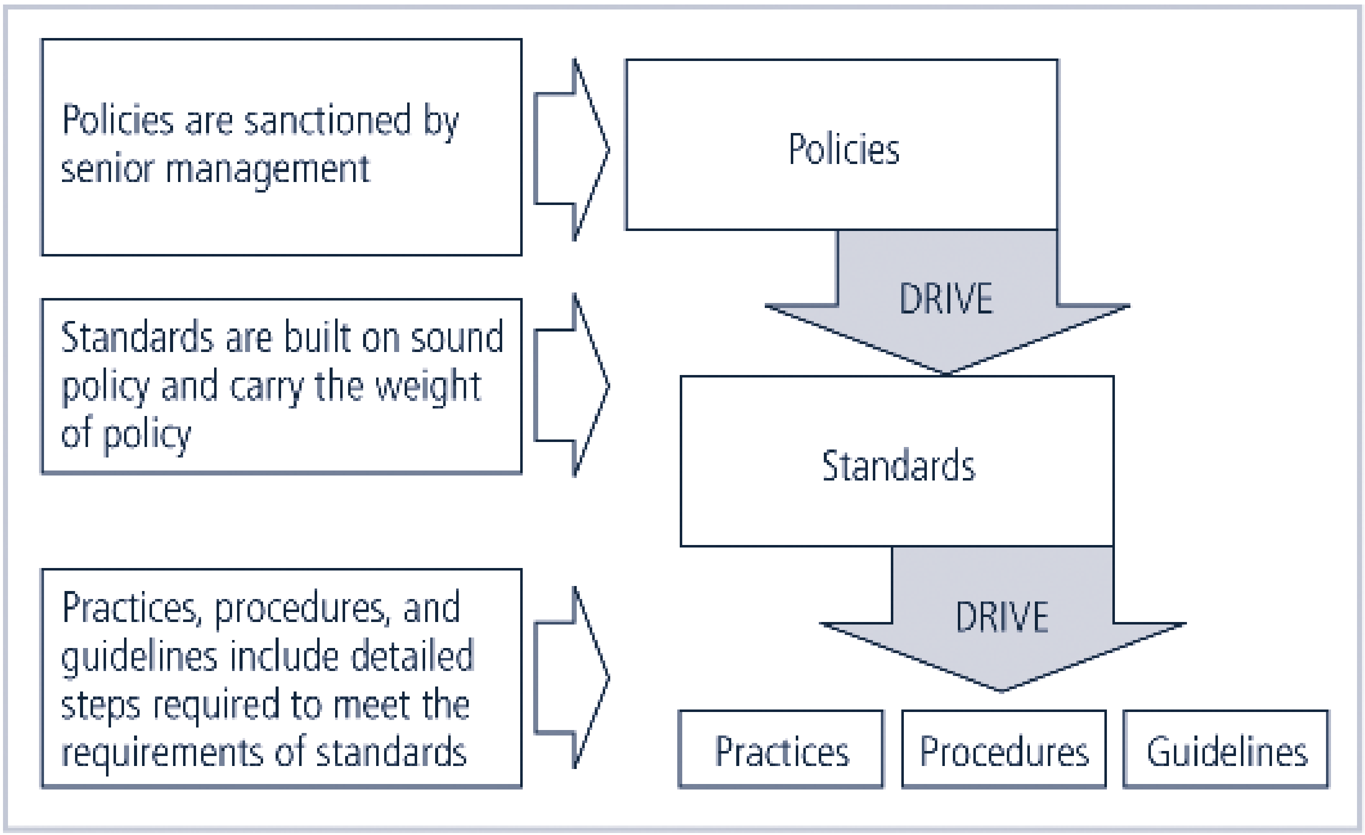

Policies are sanctioned by senior management
Standards are built on sound policy and carry the weight of policy
Practices, procedures, and guidelines include detailed steps required to meet the requirements of standards
Policies
DRIVE
Standards
DRIVE
Practices
Procedures
Guidelines

FIGURE 5-1 Policies, Standards, and Practices

<u>Types of Policies</u>

- Enterprise information Security program Policy(EISP)
- Issue-specific information Security Policy (ISSP)
- Systems-specific information Security Policy (SysSP)

Enterprise Information Security Policy (EISP)

- Also Known as a general Security policy, IT security policy, or information security policy.
- Sets strategic direction, scope, and tone for all security efforts within the organization
- Assigns responsibilities to various areas of information security
- Guides development, implementation, and management of information security program

Issue-Specific Security Policy (ISSP)

- The ISSP:
  - Addresses specific areas of technology
  - Requires frequent updates
  - Contains statement on position on specific issue
- Approaches to creating and managing ISSPs:
  - Create number of independent ISSP documents

    - Create a single comprehensive ISSP document
    - Create a modular ISSP document
- ISSP topics could include:
    - E-mail, use of Web, configurations of computers to defend against worms and viruses, prohibitions against hacking or testing organisation security controls, home use of company-owned computer equipment, use of personal equipment on company networks, use of telecommunications technologies(FAX and phone), use of photocopiers

Components of the ISSP

- Statement of Policy
    - Scope and Applicability
    - Definition of Technology Addressed
    - Responsibilities
- Authorized Access and Usage of Equipment
    - User Access
    - Fair and Responsible Use
    - Protection of Privacy
- Prohibited Usage of Equipment
    - Disruptive Use or Misuse
    - Criminal Use
    - Offensive or Harassing Materials
    - Copyrighted, Licensed or other Intellectual Property
    - Other Restrictions
- Systems Management
    - Management of Stored Materials
    - Employer Monitoring
    - Virus Protection
    - Physical Security
    - Encryption
- Violations of Policy
    - Procedures for Reporting Violations
    - Penalties for Violations
- Policy Review and Modification
    - Scheduled Review of Policy and Procedures for Modification
- Limitations of Liability
    - Statements of Liability or Disclaimers

Systems-Specific Policy (SysSP)

- SysSPs are frequently codified as standards and procedures to be used when configuring or maintaining systems
- Systems-specific policies fall into two groups:
- **Access control lists (ACLs)** consist of the access control lists, matrices, and capability tables governing the rights and privileges of a particular user to a particular system
- **Configuration rules** comprise the specific configuration codes entered into security systems to guide the execution of the system

ACL Policies

- Both Microsoft Windows NT/2000 and Novell Netware 5.x/6.x families of systems translate ACLs into sets of configurations that administrators use to control access to their respective systems
- ACLs allow a configuration to restrict access from anyone and anywhere
- ACLs regulate:
  - Who can use the system
  - What authorized users can access
  - When authorized users can access the system
  - Where authorized users can access the system from
  - How authorized users can access the system

The Information Security Blueprint

- It is the basis for the design, selection, and implementation of all security policies, education and training programs, and technological controls.
- More detailed version of **security framework**, which is an outline of overall information security strategy for organization and a road map for planned changes to the information security environment of the organization.
- Should specify tasks to be accomplished and the order in which they are to be realized.
- Should also serve as a scalable, upgradeable, and comprehensive plan for the information security needs for coming years.

Security Models

ISO 17799/BS 7799

- One of the most widely referenced and often discussed security models is the Information Technology – Code of Practice for Information Security Management, which was originally published as British Standard BS 7799
- In 2000, this Code of Practice was adopted as an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799.

Drawbacks of ISO 17799/BS 7799

- Several countries have not adopted 17799 claiming there are fundamental problems:
  - The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799
  - 17799 lacks “the necessary measurement precision of a technical standard”
  - There is no reason to believe that 17799 is more useful than any other approach currently available

- 17799 is not as complete as other frameworks available
- 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security controls

Objectives of ISO 17799

Organizational Security Policy is needed to provide management direction and support.

Ten Sections of ISO/IEC 17799

a. Organizational Security Policy
b. Organizational Security Infrastructure
c. Asset Classification and Control
d. Personnel Security
e. Physical and Environmental Security
f. Communications and Operations Management
g. System Access Control
h. System Development and Maintenance
i. Business Continuity Planning
j. Compliance

Alternate Security Models available other than ISO 17799/BS 7799

NIST Security Models

- This refers to "The National Security Telecommunications and Information systems Security Committee" document. This document presents a comprehensive model for information security. The model consists of three dimensions.
- Another possible approach available is described in the many documents available from the Computer Security Resource Center of the National Institute for Standards and Technology (csrc.nist.gov).

The following NIST documents can assist in the design of a security framework:

- **NIST SP 800-12 :** *An Introduction to Computer Security*: The NIST Handbook
- ***NIST SP 800-14 :*** *Generally Accepted Security Principles and Practices fo Securing IT Systems*
- **NIST SP 800-18** : *The Guide for Developing Security Plans for IT Systems*
- **NIST SP 800-26**: *Security Self-Assessment Guide for IT systems.*
- **NIST SP 800-30**: *Risk Management for IT systems.*

NIST Special Publication SP 800-12

- **SP 800-12** is an excellent reference and guide for the security manager or administrator in the routine management of information security.

- It provides little guidance, however, on design and implementation of new security systems, and therefore should be used only as a valuable precursor to understanding an information security blueprint.

NIST Special Publication SP 800-14

- Generally accepted Principles and practices for Security Information Technology Systems.
- Provides best practices and security principles that can direct the security team in the development of **Security Blue Print**.
- The scope of NIST SP 800-14 is broad. It is important to consider each of the security principles it presents, and therefore the following sections examine some of the more significant points in more detail:
  - Security Supports the Mission of the Organization
  - Security is an Integral Element of Sound Management
  - Security Should Be Cost-Effective
  - Systems Owners Have Security Responsibilities Outside Their Own Organizations
  - Security Responsibilities and Accountability Should Be Made Explicit
  - Security Requires a Comprehensive and Integrated Approach
  - Security Should Be Periodically Reassessed
  - Security is Constrained by Societal Factors
  - 33 Principles enumerated

NIST SP 800-18

- The Guide for Developing Security plans for Information Technology Systems can be used as the foundation for a comprehensive security blueprint and framework.
- It provides detailed methods for assessing, and implementing controls and plans for applications of varying size.
- It can serve as a useful guide to the activities and as an aid in the planning process.
- It also includes templates for major application security plans.
- The table of contents for Publication 800-18 is presented in the following.

  System Analysis
    - System Boundaries
    - Multiple similar systems
    - System Categories

  Plan Development- All Systems
    - Plan control
    - System identification
    - System Operational status
    - System Interconnection/ Information Sharing
    - Sensitivity of information handled
    - Laws, regulations and policies affecting the system

  Management Controls
    - Risk Assessment and Management

- Review of Security Controls
- Rules of behavior
- Planning for security in the life cycle
- Authorization of Processing (Certification and Accreditation)
- System Security Plan

Operational Controls

1. Personnel Security
2. Physical Security
3. Production, Input/Output Controls
4. Contingency Planning
5. Hardware and Systems Software
6. Data Integrity
7. Documentation
8. Security Awareness, Training, and Education
9. Incident Response Capability

Technical Controls

- Identification and Authentication
- Logical Access Controls
- Audit Trails

NIST SP 800-26: *Security Self-Assessment Guide for IT systems*

NIST SP 800-26 Table of contents

Management Controls

Operational Controls

Technical Controls

Management controls address the design and implementation of the security planning process and security program management. They also address risk management and security control reviews. They further describe the necessity and scope of legal compliance and the maintenance of the entire security life cycle.

Operational controls deal with the operational functionality of security in the organization. They include management functions and lower level planning, such as disaster recovery and incident response planning. They also address personnel security, physical security, and the protection of production inputs and outputs. They guide the development of education, training and awareness programs for users, administrators, and management. Finally, they address hardware and software systems maintenance and the integrity of data.

Technical controls address the tactical and technical issues related to designing and implementing security in the organization, as well as issues related to examining and selecting the technologies appropriate to protecting information. They address the specifics of technology selection and the acquisition of certain technical components. They also include logical access controls, such as identification, authentication, authorization, and accountability. They cover cryptography to protect information in storage and transit. Finally, they include the classification of assets and users, to facilitate the authorization levels needed.

Using the three sets of controls, the organization should be able to specify controls to cover the entire spectrum of safeguards, from strategic to tactical, and from managerial to technical.

VISA International Security Model

- It promotes strong security measures in its business associates and has established guidelines for the security of its information systems.
- It has developed two important documents
  1. Security Assessment Process
  2. Agreed Upon Procedures.

- Both documents provide specific instructions on the use of the VISA Cardholder Information Security Program.
- The Security Assessment Process document is a series of recommendations for the detailed examination of an organization’s systems with the eventual goal of integration into the VISA systems.
- The Agreed upon Procedures document outlines the policies and technologies required for security systems that carry the sensitive card holder information to and from VISA systems.
- Using the two documents, a security team can develop a sound strategy for the design of good security architecture.
- The only downside to this approach is the specific focus on systems that can or do integrate with VISA’s systems with the explicit purpose of carrying the aforementioned cardholder information.

Baselining & Best Business Practices

- Baselining and best practices are solid methods for collecting security practices, but provide less detail than a complete methodology
- Possible to gain information by baselining and using best practices and thus work backwards to an effective design

- The Federal Agency Security Practices (FASP) site (fasp.nist.gov) designed to provide best practices for public agencies and adapted easily to private institutions.
- The documents found in this site include specific examples of key policies and planning documents, implementation strategies for key technologies, and position descriptions for key security personnel.
- Of particular value is the section on program management, which includes the following:
    - A summary guide: public law, executive orders, and policy documents
    - Position description for computer system security officer.
    - Position description for information security officer
    - Position description for computer specialist.
    - Sample of an information technology(IT) security staffing plan for a large service application(LSA)
    - Sample of an information technology(IT) security program policy
    - Security handbook and standard operating procedures.
    - Telecommuting and mobile computer security policy.

Hybrid Framework for a Blueprint of an Information Security System

-The framework of security includes philosophical components of the Human Firewall Project, which maintain that people, not technology, are the primary defenders of information assets in an information security program, and are uniquely responsible for their protection.

- The spheres of security are the foundation of the security framework.

- The sphere of use, at the left in fig, explains the ways in which people access information; for example, people read hard copies of documents and can also access information through systems.

- The sphere of protection at the right illustrates that between each layer of the sphere of use there must exist a layer of protection to prevent access to the inner layer from the outer layer.

- Each shaded band is a layer of protection and control.

Sphere of Protection

- The "sphere of protection" overlays each of the levels of the "sphere of use" with a layer of security, protecting that layer from direct or indirect use through the next layer
- The people must become a layer of security, a **human firewall** that protects the information from unauthorized access and use
- Information security is therefore designed and implemented in three layers
    - policies
    - people (education, training, and awareness programs)
    - technology

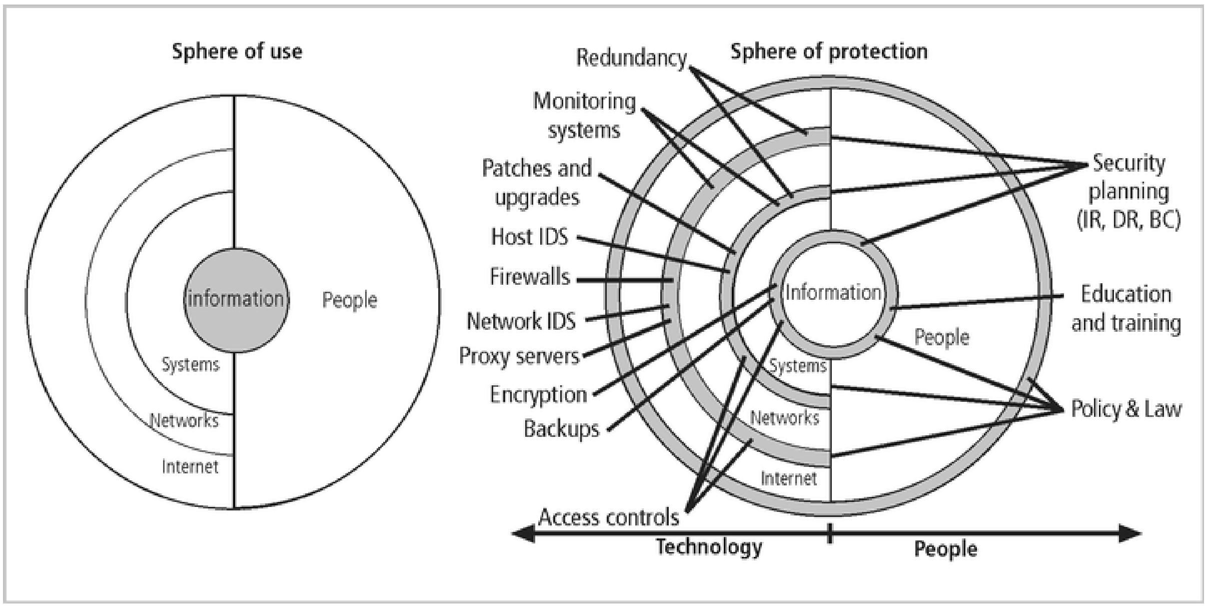


FIGURE 6-16 Spheres of Security

- As illustrated in the sphere of protection, a variety of controls can be used to protect the information.
- The items of control shown in the figure are not intended to be comprehensive but rather illustrate individual safeguards that can protect the various systems that are located closer to the center of the sphere.
- However, because people can directly access each ring as well as the information at the core of the model, the side of the sphere of protection that attempt to control access by relying on people requires a different approach to security than the side that uses technology.

Design of Security Architecture

Defense in Depth

- One of the basic foundations of security architectures is the implementation of security in layers. This layered approach is called **defense in depth**.

- Defense in depth requires that the organization establish sufficient security controls and safeguards, so that an intruder faces multiple layers of controls.

-These layers of control can be organized into policy, training and education and technology as per the NSTISSC model.

- While policy itself may not prevent attacks, they coupled with other layers and deter attacks.

- Training and Education are similar.
- Technology is also implemented in layers, with detection equipment, all operating behind access control mechanisms.
- Implementing multiple types of technology and thereby preventing the failure of one system from compromising the security of the information is referred to as **redundancy**.
- Redundancy can be implemented at a number of points throughout the security architecture, such as firewalls, proxy servers, and access controls.
- The figure shows the use of firewalls and intrusion detection systems(IDS) that use both packet-level rules and data content analysis.

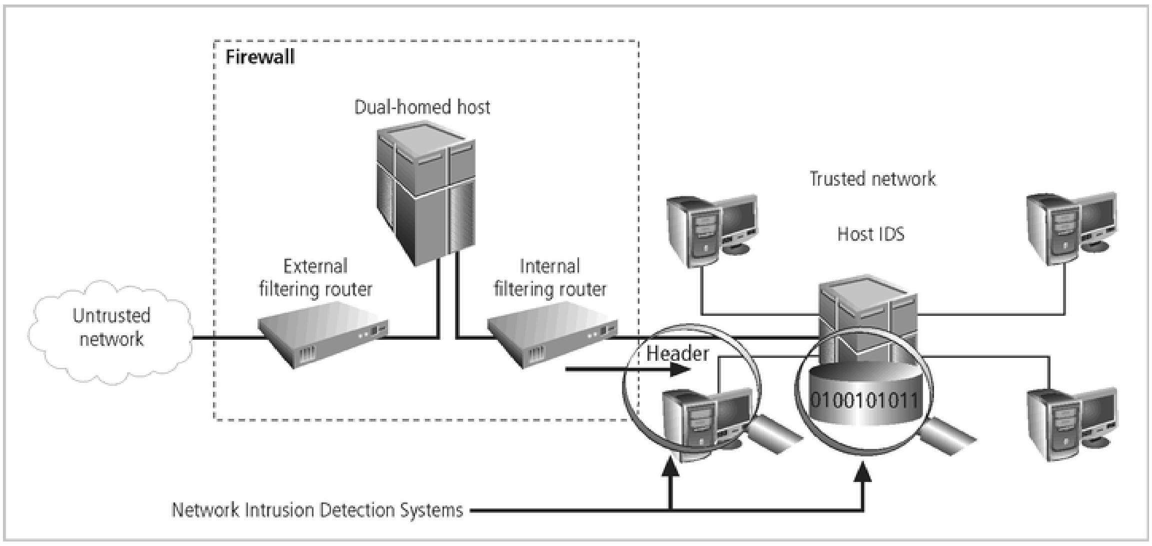

Firewall
Dual-homed host
Trusted network
Host IDS
External filtering router
Internal filtering router
Untrusted network
Header
0100101011
Network Intrusion Detection Systems

FIGURE 6-18 Defense in Depth

Security Perimeter

- A Security Perimeter is the first level of security that protects all internal systems from outside threats.
- Unfortunately, the perimeter does not protect against internal attacks from employee threats, or on-site physical threats.
- Security perimeters can effectively be implemented as multiple technologies that segregate the protected information from those who would attack it.
- Within security perimeters the organization can establish security domains, or areas of trust within which users can freely communicate.
- The presence and nature of the security perimeter is an essential element of the overall security framework, and the details of implementing the perimeter make up a great deal of the particulars of the completed security blueprint.

- The key components used for planning the perimeter are presented in the following sections on firewalls, DMZs, proxy servers, and intrusion detection systems.

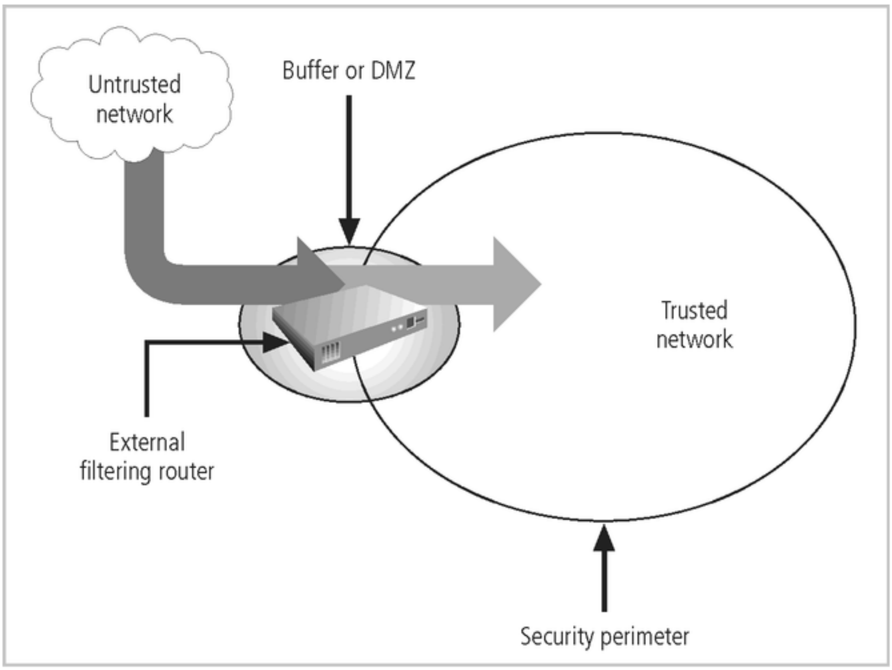


FIGURE 6-19 Security Perimeters and Domains

Key Technology Components

- Other key technology components
  - A **firewall** is a device that selectively discriminates against information flowing into or out of the organization.
  - Firewalls are usually placed on the security perimeter, just behind or as part of a **gateway router**.
  - Firewalls can be packet filtering, stateful packet filtering, proxy, or application level.
  - A Firewall can be a single device or a **firewall subnet**, which consists of multiple firewalls creating a buffer between the outside and inside networks.
  - The **DMZ** (demilitarized zone) is a no-man's land, between the inside and outside networks, where some organizations place Web servers
  - These servers provide access to organizational web pages, without allowing Web requests to enter the interior networks.
  - **Proxy server-** An alternative approach to the strategies of using a firewall subnet or a DMZ is to use a **proxy server**, or **proxy firewall**.
  - When an outside client requests a particular Web page, the proxy server receives the request as if it were the subject of the request, then asks for the same information from the true Web server(acting as a proxy for the requestor), and then responds to the request as a proxy for the true Web server.

- For more frequently accessed Web pages, proxy servers can cache or temporarily store the page, and thus are sometimes called **cache servers.**

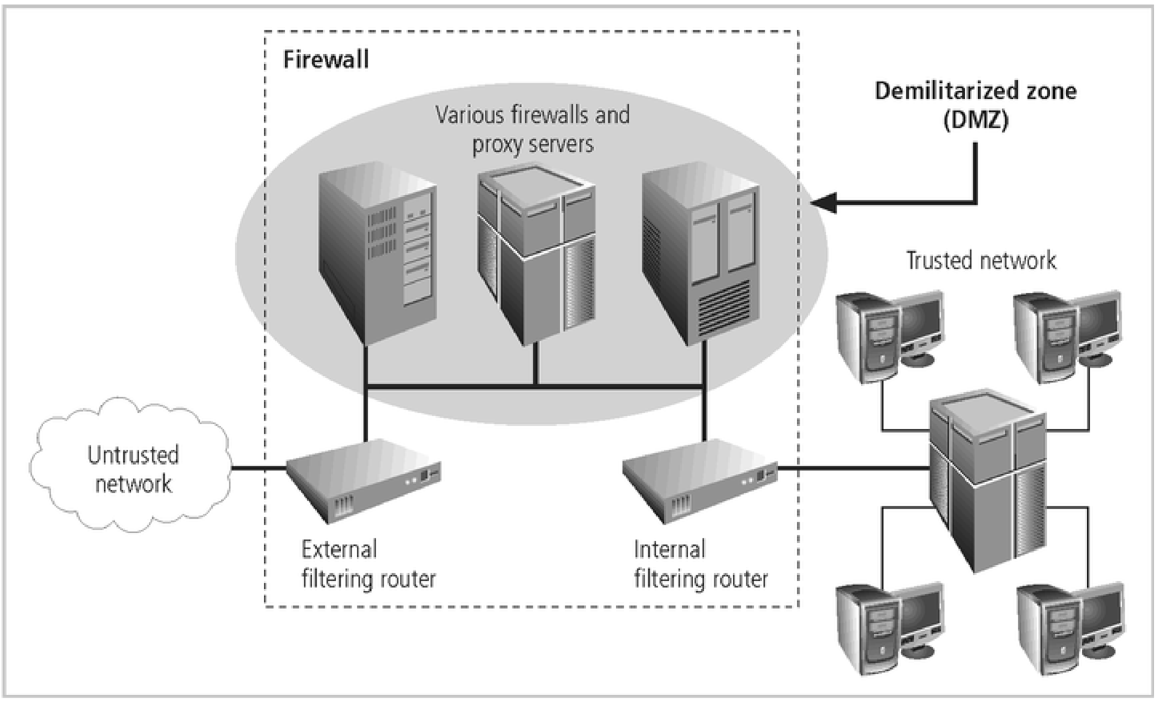

Firewall
Various firewalls and proxy servers
Demilitarized zone (DMZ)
Trusted network
Untrusted network
External filtering router
Internal filtering router

FIGURE 6-20 Firewalls, Proxy Servers, and DMZs

- **Intrusion Detection Systems (IDSs).** In an effort to detect unauthorized activity within the inner network, or on individual machines, an organization may wish to implement **Intrusion Detection Systems or IDS**.
- **IDs** come in two versions. Host-based & Network-based IDSs.
- **Host-based IDSs** are usually installed on the machines they protect to monitor the status of various files stored on those machines.
- **Network-based IDSs** look at patterns of network traffic and attempt to detect unusual activity based on previous baselines.
- This could include packets coming into the organization's networks with addresses from machines already within the organization (IP spoofing).
- It could also include high volumes of traffic going to outside addresses (as in cases of data theft) or coming into the network (as in a denial of service attack).
- Both host-and network based IDSs require a database of previous activity.

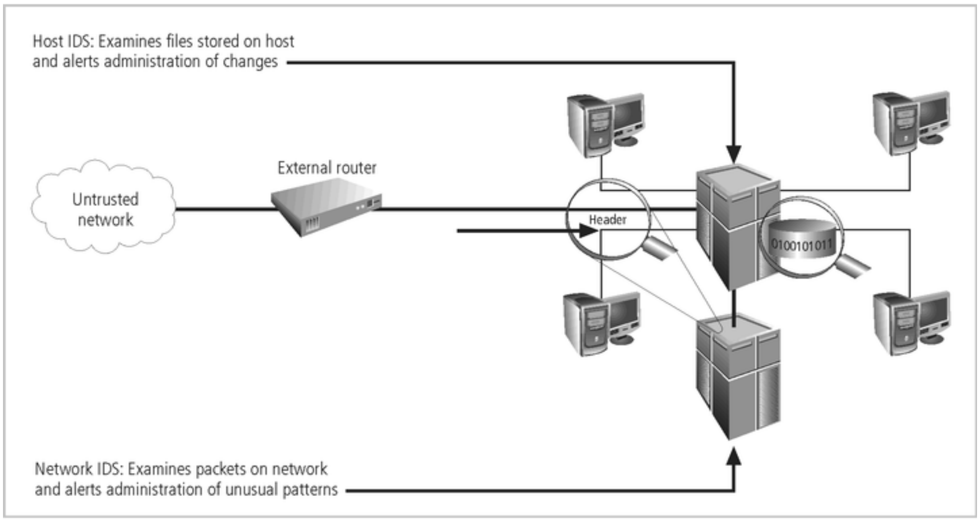

Host IDS: Examines files stored on host and alerts administration of changes
External router
Untrusted network
Header
0100101011
Network IDS: Examines packets on network and alerts administration of unusual patterns

FIGURE 6-21 Intrusion Detection Systems

Security Education, Training, and Awareness Program

- As soon as general security policy exists, policies to implement **security education, training and awareness (SETA)** program should follow.
- SETA is a control measure designed to reduce accidental security breaches by employees.
- Security education and training builds on the general knowledge the employees must possess to do their jobs, familiarizing them with the way to do their jobs securely
- The SETA program consists of three elements: security education; security training; and security awareness
- The 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 Education

- Everyone in an organization needs to be trained and aware of information security, but not every member of the organization needs a formal degree or certificate in information security.
- A number of universities have formal coursework in information security.
- For those interested in researching formal information security programs, there are resources available, such as the NSA-identified Centers of Excellence in Information Assurance Education.

Security Training

- It involves providing members of the organization with detailed information and hands-on instruction to prepare them to perform their duties securely.
- Management of information security can develop customized in-house training or outsource the training program.

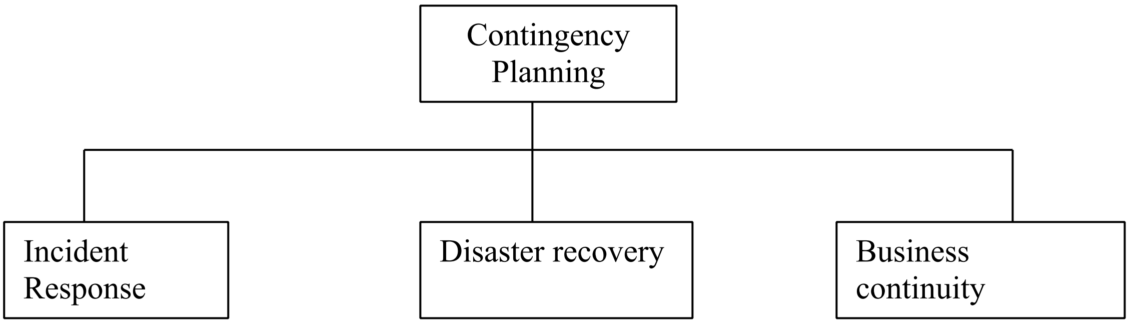
Security Awareness

- One of the least frequently implemented, but most beneficial programs is the security awareness program
- Designed to keep information security at the forefront of users' minds
- Need not be complicated or expensive
- If the program is not actively implemented, employees may begin to "tune out" and risk of employee accidents and failures increases

Contingency Planning (CP)

- Contingency Planning (CP) comprises a set of plans designed to ensure the effective reaction and recovery from an attack and the subsequent restoration to normal modes of business operations.
- Organizations need to develop disaster recovery plans, incident response plans, and business continuity plans as subsets of an overall CP.
- An **incident response plan (IRP)** deals with the identification, classification, response, and recovery from an incident, but if the attack is disastrous(e.g., fire, flood, earthquake) the process moves on to disaster recovery and BCP
- A **disaster recovery plan (DRP)** deals with the preparation for and recovery from a disaster, whether natural or man-made and it is closely associated with BCP.
- A **Business continuity plan (BCP)** ensures that critical business functions continue, if a catastrophic incident or disaster occurs. BCP occurs concurrently with DRP when the damage is major or long term, requiring more than simple restoration of information and information resources.

Components of Contingency Planning



There are six steps to contingency planning. They are

1. Identifying the mission-or business-critical functions,
2. Identifying the resources that support the critical functions,
3. Anticipating potential contingencies or disasters,
4. Selecting contingency planning strategies,
5. Implementing the contingencies strategies,
6. and Testing and revising the strategy.

Incident response plan (IRP)

- It is the set of activities taken to plan for, detect, and correct the impact of an incident on information assets.
- IRP consists of the following 4 phases:
  1. Incident Planning
  2. Incident Detection
  3. Incident Reaction
  4. Incident Recovery

Incident Planning

-Planning for an incident is the first step in the overall process of incident response planning.
- The planners should develop a set of documents that guide the actions of each involved individual who reacts to and recovers from the incident.
- These plans must be properly organized and stored to be available when and where needed, and in a useful format.

Incident Detection

-Incident Detection relies on either a human or automated system, which is often the help desk staff, to identify an unusual occurrence and to classify it properly as an incident.
- The mechanisms that could potentially detect an incident include intrusion detection systems (both host-based and network based), virus detection software, systems administrators, and even end users.
- Once an attack is properly identified, the organization can effectively execute the corresponding procedures from the IR plan. Thus, **incident classification** is the process of examining a potential incident, or **incident candidate**, and determining whether or not the candidate constitutes an actual incident.
- **Incident Indicators**- There is a number of occurrences that could signal the presence of an incident candidate.
- **Donald Pipkin**, an IT security expert, identifies three categories of incident indicators: **Possible, Probable, and Definite Indicators**.
-**Possible Indicators**- There are 4 types of possible indicators of events ,they are,

1. Presence of unfamiliar files.
2. Presence or execution of unknown programs or processes.
3. Unusual consumption of computing resources
4. Unusual system crashes

- **Probable Indicators**- The four types of probable indicators of incidents are

1. Activities at unexpected times.
2. Presence of new accounts
3. Reported attacks
4. Notification from IDS

Definite Indicators- The five types of definite indicators of incidents are

1. Use of Dormant accounts
2. Changes to logs
3. Presence of hacker tools
4. Notifications by partner or peer
5. Notification by hacker

Incident Reaction

- It consists of actions outlined in the IRP that guide the organization in attempting to stop the incident, mitigate the impact of the incident, and provide information for recovery from the incident.
- These actions take place as soon as the incident itself is over.
- In reacting to the incident there are a number of actions that must occur quickly, including notification of key personnel and documentation of the incident.
- These must have been prioritized and documented in the IRP for quick use in the heat of the moment.

Incident Recovery

- The recovery process involves much more than the simple restoration of stolen, damaged, or destroyed data files. It involves the following steps.
  1. Identify the Vulnerabilities
  2. Address the safeguards.
  3. Evaluate monitoring capabilities
  4. Restore the data from backups.
  5. Restore the services and processes in use.
  6. Continuously monitor the system
  7. Restore the confidence of the members of the organization's communities of interest.

Disaster Recovery Plan (DRP)

- DRP provides detailed guidance in the event of a disaster and also provides details on the roles and responsibilities of the various individuals involved in the disaster recovery effort, and identifies the personnel and agencies that must be notified.
- At a minimum, the DRP must be reviewed during a walk-through or talk-through on a periodic basis.

Many of the same precepts of incident response apply to disaster recovery:

1. There must be a clear establishment of priorities
2. There must be a clear delegation of roles and responsibilities
3. Someone must initiate the alert roster and notify key personnel.
4. Someone must be tasked with the documentation of the disaster.
5. If and only if it is possible, attempts must be made to mitigate the impact of the disaster on the operations of the organization.

Business Continuity Plan (BCP)

- It prepares an organization to reestablish critical business operations during a disaster that affects operations at the primary site.
- If a disaster has rendered the current location unusable for continued operations, there must be a plan to allow the business to continue to function.

Developing Continuity Programs

- Once the incident response plans and disaster recovery plans are in place, the organization needs to consider finding temporary facilities to support the continued viability of the business in the event of a disaster.
- The development of the BCP is simpler than that of the IRP and DRP ,in that it consists of selecting a continuity strategy and integrating the off-site data storage and recovery functions into this strategy.

Continuity Strategies

- There are a number of strategies from which an organization can choose when planning for business continuity.
- The determining factor in selection between these options is usually cost.
- In general there are three exclusive options: Hot sites, Warm Sites, and Cold sites; and three shared functions: Time-share, Service bureaus, and Mutual Agreements.

Hot sites: A hot site is a fully configured facility, with all services, communications links, and physical plant operations including heating and air conditioning. It is the pinnacle of contingency planning, a duplicate facility that needs only the latest data backups and the personnel to function as a fully operational twin of the original. Disadvantages include the need to provide maintenance for all the systems and equipment in the hot site, as well as physical and information security.

Warm sites: A warm site includes computing equipment and peripherals with servers but not client work stations. It has many of the advantages of a hot site, but at a lower cost.

Cold Sites: A cold site provides only rudimentary services and facilities, No computer hardware or peripherals are provided. Basically a cold site is an empty room with heating, air conditioning, and electricity. The main advantage of cold site is in the area of cost.

Time-shares: It allows the organization to maintain a disaster recovery and business continuity option, but at a reduced overall cost. The advantages are identical to the type of site selected(hot, warm, or cold). The disadvantages are the possibility that more than one organization involved in the time share may need the facility simultaneously and the need to stock the facility with the equipment and data from all organizations involved, the negotiations for arranging the time-share, and associated arrangements, should one or more parties decide to cancel the agreement or to sublease its options.

Service bureaus: A service bureau is an agency that provides a service for a fee. In the case of disaster recovery and continuity planning, the service is the agreement to provide physical facilities in the event of a disaster. These types of agencies also provide off-site data storage for a fee. The disadvantage is that it is a service, and must be renegotiated periodically. Also, using a service bureau can be quite expensive.

Mutual Agreements: A mutual agreement is a contract between two or more organizations that specifies how each will assist the other in the event of a disaster.

Review Questions

1. What is a policy?
2. Explain how information security policy is implemented as procedure?
3. What are the three types of security policies? Explain.
4. What are ACL Policies?
5. What is Information Security Blueprint?
6. Define ISO 17799/BS 7799 Standards and their drawbacks
7. What are the objectives of ISO 17799?
8. What is the alternate Security Models available other than ISO 17799/BS 7799?
9. Compare the Issues-Specific Security Policy(ISSP) and System Specific Policies (SysSP).
10. What is meant by International Security Model?
11. State the pros of VISA international security model.
12. Describe NIST security models.
13. Explain NIST SP 800-14
14. Explain NIST SP 800-26
15. What is Sphere of protection?
16. What is Defense in Depth?
17. What is Security perimeter?
18. What are the key technological components used for security implementation?
19. How can a security framework assist in the design and implementation of a security infrastructure?
20. Briefly describe management, operational, and technical controls, and explain when each would be applied as part of a security framework?
21. What is contingency planning? What are the components of contingency planning?
22. When is IRP used?
23. When is DRP used?
24. When is BCP used? How do you determine when to use IRP, DRP, or BCP plans?
25. What are Pipkin's three categories of incident indicators?
26. List and describe the six continuity strategies.
27. Explain clearly about spheres of security for a blue print of an Information Security System.
28. List the styles of architecture security models. Discuss them in detail.