

Operational and Organizational Security



Chapter 3

Background

- Prevention technologies
 - Prevent unauthorized individuals from gaining access to systems or data.
 - Static.
 - They are put in place and generally left alone.
 - In an operational environment, prevention is difficult.

Relying on prevention technologies alone is not sufficient.
- Detection and response technologies
 - Dynamic.
 - Acknowledge that security is an ongoing process.



Security Operations

- **Policies**

- High-level, broad statements of what the organization wants to accomplish.
- Made by the management when laying out the organization's position on some issues.
- Focus: long-term and strategic

- **Policies support five common aims:**

1. **Prevention** – security from internal and external penetration, and prevention of undesirable occurrence
2. **Detection** – reaction to the nature, existence, presence, or fact of a penetration
3. **Containment** – protection of sensitive data
4. **Deterrence** – policies, procedures, and actions designed to discourage penetration
5. **Recovery** – restoration after a failure or penetration



Role of Policy in Creating an Infrastructure

- Policies state the approach that will be followed to enforce the pillars of security (Confidentiality, Integrity,)
 - Should be both comprehensive and coherent
 - Constitute the framework that dictates the scope and application of the information assurance process
 - Must have the right set of procedures to enact it

Procedures are progressively refined, until the desired level of control is established



Security Operations

- Procedures
 - Step-by-step instructions on how to implement policies in an organization.
 - Describe exactly how employees are expected to act in a given situation or to accomplish a specific task.
 - Focus: short-term and day-to-day
- Standards
 - Mandatory elements regarding the implementation of a policy.
 - Accepted specifications of specific details on how a policy is to be implemented or enforced.
- Guidelines
 - Recommendations relating to a policy.
 - Not mandatory.



Policy Changes

- **Policy Life Cycle:**
 - As the network constantly changes, the policies, procedures, and guidelines should be periodically evaluated and changed if necessary.
 - The constant monitoring of the network and the periodic review of the relevant documents are part of the operational model.
 - When applied to policies, this process results in the policy life cycle.

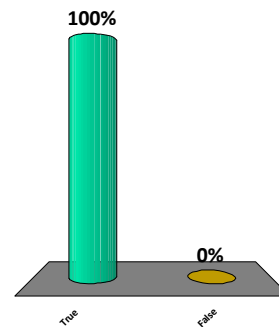
Policy Life Cycle

The four steps :

- Plan (Adjust)
 - Develop the policies, procedures, and guidelines that will be implemented and design the security components
 - Design the security components to protect the network.
- Implement
 - Deliver instructional period on the current plan
 - Includes user training
- Monitor
 - Ensures that hardware and software, policies, procedures, and guidelines are effective in securing the systems.
- Evaluate:
 - Assesses the effectiveness of security
 - Includes vulnerability assessment and penetration test of the system to ensure that security meets expectations.
 - A continuous process.

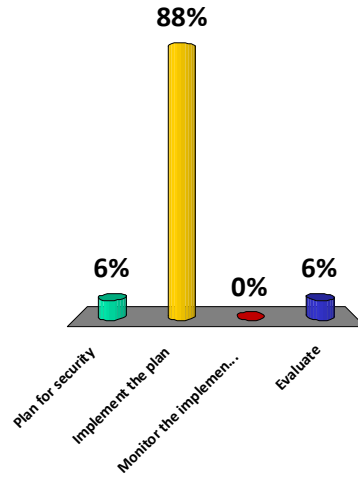
Procedures can be described as the step-by-step instructions on how to implement the policies

1. True
2. False



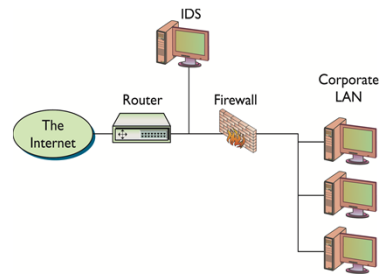
During which step of the policy lifecycle does training of users take place?

1. Plan for security
2. Implement the plan
3. Monitor the implementation
4. Evaluate



Is This the Security Perimeter?

Security Perimeter - Specific technology used to enforce operational or organizational security

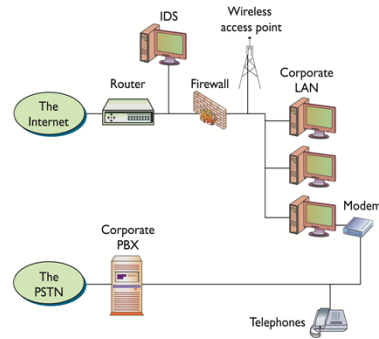


1. The router acts as first line of defense from external threats and will often do packet filtering at this layer of the defense.
2. An IDS may sit between the router and firewall to detect suspicious traffic before it get any further.
3. The firewall is another layer of protection with tighter controls on the kinds of traffic that can pass.

**Is this really the perimeter of the network that needs securing?
What is missing from this diagram?**

A More Complete Diagram

1. The telephone network must be included as a possible source of access for the network.
 - a) Voice over IP (VoIP) eliminates the traditional land lines in an organization and replaces them with special telephones that connect to the IP data network.
2. Wireless access point- Another area where perimeter may be open to attack



The biggest danger to any organization comes from the insider—a disgruntled employee or somebody else who has physical access to the facility.

Defense in Depth

Defense in depth:

Security is enhanced when there are multiple layers of security (the depth) through which an attacker would have to penetrate to reach the desired goal

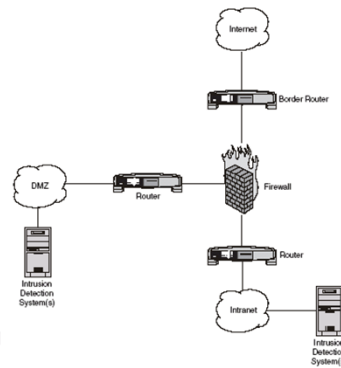


Figure 3.1
Example of defense in depth



Physical Security


- Physical access to computer systems and networks is restricted to authorized users.
 - Similar to computer and network access controls where access is restricted to the authorized users.
- Physical security safeguards assets from non-digital threats
 - Protects information processing facilities and equipment from deliberate or accidental harm
 - More involved and complex
- Uncontrolled physical space makes it easy for an attacker to subvert most security measures
 - Proximity to the equipment allows attackers to mount attacks more easily
- No matter how good is computer and network security , if a person has physical access, then can compromise the CIA of information in some way.

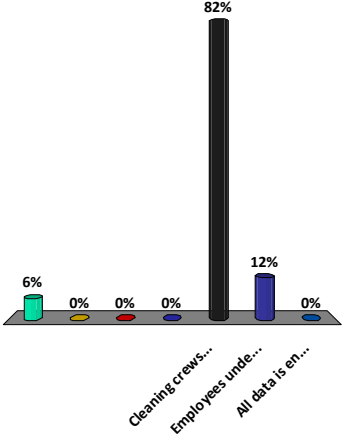


Physical Security

- Access from all six sides is important.
 - Floor, ceiling and the 4 walls
 - The security of obvious points of entry such as doors and windows should be examined.
 - Even floors and ceiling should be scrutinized for possible access points.
- The principle of identity is composed of two functions:
 - Identification function establishes the identity of every person or process that seeks access
 - Authentication function confirms that it is valid

Which of the following is a physical security threat?

- 1.
- 2.
- 3.
- 4.
5.  Cleaning crews are allowed unsupervised access because they have a contract.
6. Employees undergo background criminal checks before being hired.
7. All data is encrypted before being backed up.



Option	Percentage
Cleaning crews...	82%
Employees unde...	12%
All data is en...	0%
Other 1	6%
Other 2	0%
Other 3	0%

Access Controls

- Authentication via
 - Something you have – key or card
 - Something you know – combination locks
 - Something you are – biometrics
- Biometrics
 - More sophisticated and expensive
 - Not yet 100 percent foolproof
- Two factor authentication
 - Using two of the methods for authentication
- Other controls
 - Video surveillance, sign-in logs, security guards



Locks

- Lock
 - The most common physical access control device.
- Locks with keys depend on something the individual has (the key).
 - Key locks are simple and easy to use, but the key may be lost.
 - If the key is lost, a duplicate key has to be made or the lock has to be re-keyed.
 - Keys may also be copied and can be hard to control
- Combination locks
 - Represent an access control device that depends upon something the individual knows (the combination).
 - Combinations do not require any extra hardware, but they must be remembered
 - Individuals may write them, which is a security vulnerability in itself, and are hard to control.



Modern Locks

- Newer locks
 - Replace the traditional key with a card
 - Must be passed through a reader or placed against it.
 - The individual may also have to provide a personal access code, thus making this form of access both a something-you-know and something-you-have method.

In addition to locks on doors, other common physical security devices include video surveillance and even simpler access control logs (sign-in logs).



Access Control Logs

- Sign-in logs do not provide an actual barrier.
 - They provide a record of access.
 - Often used in conjunction with a guard who verifies an individual's identity.

- Human security guard.
 - Provide an extra level of examination of individuals who want to gain access.
 - Counter piggybacking.



Biometrics

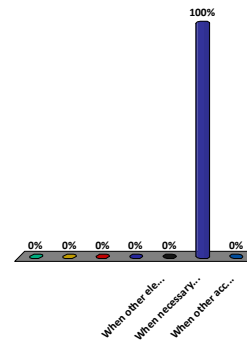
- Biometrics:
 - Uses something unique about the individual.
 - Does not rely on an individual to remember something or to have something.
 - Sophisticated access control approach and is also more expensive.
 - Can control access to computer systems, networks, and physical access control devices.
 - Biometrics provides an additional layer of security.
 - Biometrics is normally used in conjunction with another method.
 - Biometric devices are not 100 percent accurate and may allow access to unauthorized individuals.

Biometrics: Something You Are

- Problem with biometric technology:
 - Still in its infancy
 - Can fail due to its dependency on advanced processing capabilities
 - When it comes to the identity process, possible failures include:
 - False positives allow unauthorized individuals to access system resources
 - False negatives deny authorized people access

When should a human security guard be used for physical access control?

- 1.
- 2.
- 3.
- 4.
5. When other electronic access control mechanisms will not be accepted by employees
6. When necessary to avoid issues such as piggybacking, which can occur with electronic access controls
7. When other access controls are too expensive to implement





Physical Barriers

- Physical barriers
 - Another common security feature
 - Help implement the physical-world equivalent of layered security.
 - The outermost layer of physical security contains the public activities.
 - As individual progresses through the layers, the barriers and security mechanisms should become less public

- Some Physical barriers
 - Signs- Announce public/private areas to the public
 - Open space as a barrier.
 - An intruder must cross this open space which takes time.
 - During this time their presence may be discovered and hence they are vulnerable.
 - Man trap, Fences, Guard at the gate, Walls



Environmental Issues

- Can influence the availability of a computer system

- Heating, ventilation and air conditioning (HVAC)
 - Used to maintain the comfort of an office environment
 - Also maintained environment for computers
 - Heat and humidity sensitive devices and network components

- Electrical Power- Uninterruptable Power Supply (UPS)
 - Used for critical systems so that a loss of power will not halt processing
 - The larger the battery, the longer the equipment can operate during a loss of power



Fire Suppression

- Fire is a common disaster.
- Fire detectors
 - Smoke detection
 - Heat detection
- Fire suppression
 - Sprinkler-based
 - Standard, but will further damage equipment
 - Gas-based
 - Halon was used and may still exist in some areas. Halon is being replaced with other gases such as argon, nitrogen, and carbon dioxide. Note that the same danger exists.



Off-Site Storage

- Off-site storage
 - Limits the chance that a natural disaster affecting one area will result in the total loss of the organization's critical data.
 - Also consider backup processing locations along with the back up data.

When considering backup and contingency plans, it is also important to consider backup processing locations in case a disaster not only destroys the data at the organization's primary site but all processing equipment as well.



IEEE 802.11

- Wireless networks are also a security risk.
 - The coverage areas of the access points are not easily controlled.
 - Many publicly accessible areas fall in the range of an organization's access point.
 - The network becomes vulnerable to attack.



Electromagnetic Eavesdropping

- **The van Eck phenomenon**
 - Eavesdropping on what is being displayed on monitors by picking up and decoding the electromagnetic interference (EMI) produced by monitors.
 - With the appropriate equipment, the exact image of what is being displayed can be re-created some distance away.
- To protect against the equipment being monitored, users need to **increase the distance between the target and attacker.**
 - Emanations can be picked up from only a limited distance.



Shielding

- Three ways to prevent the emanations from being picked up by an attacker:
 - Put the equipment beyond the point that the emanations can be picked.
 - Provide shielding for the equipment itself.
 - Provide a shielded enclosure (such as a room) to put the equipment.

- These solutions can be costly.
 - The cost of shielding is so substantial that in most cases, it probably cannot be justified.



Location

- Location plays a significant role in physical security.

- Careful placement of equipment is a possible means to provide security.
 - In a wireless network, place WAP to make it difficult for an attacker to access the network from a publicly accessible area.
 - Place the most sensitive equipment deep inside the facility for electromagnetic emanations.
 - Some facilities will be easier to protect than others, depending on their proximity to other buildings and roads.



Communicating Organization and Technical Direction

- Success of the information assurance process rests on effective communication
 - Participants must understand the rules of behavior
 - Information assurance schemes are complex and subject to change
 - Behavior must be attuned to the situation



Ensuring Organizational Awareness

- To ensure organizational awareness
 - All applicable policy, procedure goals, and nuances of operation must be communicated
 - Communication process must be formally structured and carefully managed
 - Participants should understand the reasons for adequate protection
 - Ensured by an awareness or “buy-in” program prior to establishing the system