

MANAGEMENT 414

SANS +S™

TRAINING PROGRAM

FOR THE CISSP®

CERTIFICATION EXAM

414.6

Physical Security

Lorna Hutcheson, USA
Lawrence Johnson, CISSP No. 25456, USA
Chaiw Kok Kee, CISSP No. 31589, Malaysia
Darrin Lau, CISSP No. 29948, USA
Eliot Leibowitz, CISSP No. 43782, USA
Steven Leong, CISSP No. 30313, Singapore
Chip Meadows, CISSP No. 10070, USA
Sean Mitchell, CISSP No. 36817, USA
Michael Morrell, CISSP No. 36227, USA
Pamela Nottage, CISSP No. 3758, USA
Sanjay Pandit, CISSP No. 44786, USA
John Pao, CISSP No. 29876, USA
Ariya Parsamanesh, CISSP No. 36074, AUS
Stephen Patton, CISSP No. 49746, USA
Robert Pfau, CISSP No. 21572, USA
Gabriel Proulx, CISSP No. 34018, Canada

Jim Purcell, CISSP No. 34519, USA
Andrew Salzman, CISSP No. 25162, USA
Amarottam Shrestha, CISSP No. 41671, AUS
Michael Solomon, CISSP No. 26517, USA
Robert Sorensen, CISSP No. 48304, USA
George Starcher, CISSP No. 34689, USA
Bruce Swartz, CISSP No. 46522, USA
David Taylor, CISSP No. 55890, USA
Brad Towers, CISSP No. 27957, USA
Jill Treu, CISSP No. 43196, USA
Tim Weil, CISSP No. 44250, USA
Deborah Weinstein, CISSP No. 44411, USA
Melody Wilson, CISSP No. 4130, USA
Steven Winterfield, CISSP No. 38096, USA
Kelli Wolfe, USA
Wayde York, CISSP No. 30404, USA

I have had the privilege of the best seat in the house and have really enjoyed working with the CISSP team. I sincerely hope that you benefit greatly from the information in these books and am very interested in your feedback. Please feel free to send me suggestions, corrections or questions to [mqt414\(S\)sans.org](mailto:mqt414(S)sans.org).

Eric Cole, Senior Instructor and Research Fellow
The SANS Institute

10. Physical and Environmental Security

10 Domains of Knowledge

This section covers domain 10, the Physical and Environmental Security domain.

10. Physical Security

- Significance of physical security
- Objectives
 - Personnel safety
 - Authorized access
 - Equipment protection
 - Information protection
 - Availability

Physical Security

In the world of the information security practitioner, physical security is the practice of providing protection to information technology (IT), people, processes, and tools through the implementation of tangible controls. Physical security is the most important, and most often overlooked, principle underlying information security as a whole. By the end of this section, you should have a greater understanding of the role of physical security in an information security program.

Physical measures have always been the first actions that people take to protect their assets. Even as computing became a substantial component of business and military environments in the 1960s and 1970s, the same security thought processes reigned that had dominated for thousands of years: IT facilities got locks and fences. The Corporate Security department appeared in the organizational chart and developed its expertise almost exclusively in physical security controls.

Significance

Physical security is:

- Implicit in every logical security control
- Often overlooked
- Should be:
 - Risk based
 - Focused on critical intellectual property (IP)

In today's newer IT environments, the Information Security department developed out of the IT department with an emphasis on network and system security projects. As a result, many of today's information security specialists are less informed than their predecessors about the options available for physical protection and more, alarmingly, unaware of the susceptibility of their systems to physical compromise. Corporate security and information security must build a partnership to ensure that the company's technology assets are protected.

Objectives

- Confidentiality
- Integrity
- Availability
- Safety

Objectives of the Physical Security Program

Traditionally, information security has been aligned toward the accomplishment of three objectives: Confidentiality, Integrity, and Availability, referred to as C-I-A:

- Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.
- Integrity is the need to ensure that information has not been changed accidentally or deliberately and that it is accurate and complete.
- Availability is the need to ensure that the business purpose of the system can be met. The resource that has been established must be accessible to those who need to use it.

Within the physical security realm, Confidentiality, Integrity, and Availability are assured by the implementation of one general category of control: the access control. In addition to the traditional C-I-A of information security, the physical security realm includes an additional objective: safety.

Types of Systems

Types of systems:

- Static systems
- Mobile systems
- Portable systems

When protecting physical assets there are three general types of systems:

- Static systems
- Mobile systems
- Portable systems

Each system has different types of physical security issues associated with them.

Static systems are typically plugged into one location and are not moved. Mobile systems are often carried around with the user and, hence, are often plugged into a wide range of networks. Mobile systems present the greatest risk because critical data that resides on them can easily be accessible to the outside world through theft of the equipment. Portable systems are typically a hybrid of the two. They are not as mobile as laptops, but can still be moved and plugged into alternate locations.

Counter-Examples

- Authentication
 - Password
 - Two factor
- Encryption
 - Data at rest
 - Disk encryption
 - Data in transit
- Redundancy
 - Local system backup
 - Server redundancy and backup

Information security models often deal directly with the security relationships between each layer and the logical controls and protocols that operate at each layer to ensure that security is maintained throughout a transaction. What is most often neglected is the fact that these controls rely on a basic assumption: The physical layer environment is secure.

Let's see some examples of how this assumption can lead us to a false conclusion that our system is secure. Consider three examples that deal with authentication, encryption, and redundancy, which highlight how generally reliable information-security controls can be rendered ineffective by a physical security compromise.

Authentication

Systems frequently are protected by various passwords, secure tokens, and other methods. An operating system password protects the system by refusing access to the data on the server until the operating system verifies that the user is authenticated and authorized in its user database.

However, many password-based systems can be compromised if an individual obtains physical access to the workstation or server, such as through use of a boot disk (a simple operating system contained on a diskette). Because most systems are still configured to check the local diskette drive before the local hard drive (a troubleshooting convenience), simply inserting a bootable disk and rebooting the system gives the attacker a session with his own operating system, on which he has an administrator-level account. With this access, the attacker can retrieve any unencrypted information on the system.

Additionally, given the opportunity to remove the server from the facility, the intruder can perform any number of attacks on the stolen server to retrieve any information residing on the disk.

Access Control Types

- Deterrent
 - Guard with weapon
- Detective
 - Video surveillance
- Preventive
 - Locks

Access Control Types

Access controls provided by physical measures attempt to prevent unauthorized access by both the accidental and the malicious intruder.

The common types of access control are deterrent measures such as a guard; detective measures such as video surveillance; and preventive measures such as locks.

Administrative Controls

Personnel controls:

- Personnel screening prior to employment
 - Prior employment
 - References
 - Education
 - Criminal record
 - General background checks
- Employee checks
 - Security clearances (if necessary)
 - Performance ratings
 - Supervision
- Post-employment procedures
 - Exit interview
 - Termination of computer accounts
 - Change of passwords
 - Return of laptops and other issued equipment

Administrative personnel controls are usually implemented by the human resources department during employee hiring and firing.

General administrative controls are the following:

- Personnel screening prior to employment
 - Prior employment
 - References
 - Education
 - Criminal record
 - General background checks
- Employee checks
 - Security clearances (if necessary)
 - Performance ratings
 - Supervision
- Post-employment procedures
 - Exit interview
 - Termination of computer accounts
 - Change of passwords
 - Return of laptops and other issued equipment

Safety

- Safety is # 1 !
- Impact on other objectives
 - Personnel safety
 - Authorized access
 - Equipment protection
 - Information protection
 - Availability

Safety

Safety is the need to ensure that the people involved with the company (employees, customers, and visitors) are protected from harm. Generally, safety is the top priority when physical security measures are implemented. Most information-security practitioners consider safety the top priority for their enterprise environment.

Rare exceptions occur in the military or Secret Service, where an individual may be expected to incur injury to protect a physical asset or another person, or in a lights-out facility where the only person inside the facility is assumed to be an attacker because there are NO "authorized personnel."

Safety First

The need to ensure personnel safety requires, in many cases, accepting weaknesses in other objectives. Let's look at two examples where safety concerns take precedence over other physical security priorities:

- Example 1: During a building evacuation, employees will be exiting the building rapidly. Doors may be propped open to facilitate escape. During this scenario, employees would NOT be expected to stand at a reception desk to ensure unauthorized personnel do not access the employee-only areas.
- Example 2: When a fire is detected, automatic sprinklers might deploy to prevent the fire from spreading. This deployment, although protecting the safety of personnel, easily could damage assets required to maintain business function. Employees would not be required—nor would they have the time—to place all-important documents into waterproof containers before the sprinklers would deploy!

Evacuation: Procedures

- Evacuation routes
- Meeting point
- Posting
- Practice

Evacuation

Evacuations have saved thousands of lives in incidents ranging from small building fires to massive regional disasters. For almost any personnel security threat, facility evacuation is effective. In addition, for regional disasters, personnel evacuation is the important first step for families to reconvene and evacuate to another region. Procedures for evacuation should be prepared and practiced. Coordination with Human Resources, Business Continuity and Disaster Recovery Planning, and executive management should be tested and refined.

Every evacuation procedure should include evacuation routes and meeting points. Each procedure should clearly show the route from the current location to the nearest exit and to a second exit. Multiple copies of the procedure document should be posted. Copies should be easy to remove so that evacuees can carry the document to guide them to the exit. The procedure should include instructions for safety techniques, such as remaining close to the floor if smoke is present, testing doors for heat before opening, and counting doors to find the emergency exit.

Meeting Point

Each procedure should identify specific meeting points for personnel evacuating the facility. The meeting points should be within easy walking distance of the respective locations. Simple signs, such as "Meeting Point A," should be visible to guide employees to their meeting places.

Make sure that upper management actively participates in these drills. If the drill does not get the attention of the CEO, others will also "blow it off."

Posting

Procedures should be posted liberally throughout the work area. Remember to also post the procedures in auxiliary areas such as break rooms, restrooms, and lobbies. Signage should be marked clearly and printed in high contrast with a large font size. Use of the color red is highly recommended because this color is associated with emergency procedures. The text should not be colored in a manner that makes it difficult for individuals with red-green color blindness to discern.

Practice

Periodically you should have practice evacuations to ensure employees can execute the procedures in a genuine emergency. Employees should be required to take these drills seriously and should be subject to disciplinary action if they ignore alarms or instructions from personnel managing the drill.

After employee testing has shown that employees can exit the building in an orderly manner and within the timeframe recommended for the facility, the organization can consider conducting drills with emergency services teams. These drills, often conducted by emergency services for their specific practice needs, accept offers of a venue from local businesses.

Evacuation: Roles

- Safety warden
- Meeting-point leader
- Employee

Roles

The safety warden is responsible for checking that each individual in his or her area has begun to evacuate the building. He or she should check the premises for employees who require assistance or do not hear/see the alarm. As soon as the area is clear, the safety warden evacuates the building. The safety warden is typically the last one out, and is often a company officer or executive.

The meeting-point leader is responsible for getting to the meeting point and beginning the process of accounting for all employees. The meeting-point leader should attempt to be the "first one out" to begin the process as rapidly as possible. Often, the meeting-point leader is the individual, such as a personnel manager, who is most likely to know which employees were in the office. As soon as the safety warden arrives, the two leaders should determine who among the employees is not accounted for so that information can be provided to emergency services.

Finally, if not fulfilling a meeting-point leader or safety warden role, the employee has the responsibility to evacuate as quickly and safely as possible. The employee is expected to follow the directions of the safety warden and report to the meeting-point leader immediately after evacuating the building.

Each employee should know how to react in all roles and should know who holds each titled role by default. During drills, different employees should be cross-trained in each role.

Physical Security and Safety

- Smoke and fire
- Toxins
- Water/flood
- Temperature extremes
- Structural failure
- Power failure
- Human actions
- Intentional or unintentional
- Fire and related contaminants
- Explosions
- Loss of utilities
- Toxic materials
- Earthquakes
- Weather
- Malicious acts
- Sabotage
- Strikes

Threats to Safety

Now that we've looked at the most important control, evacuation, let's look at the threats to safety and the specific controls to handle each threat. When examining each of these threats, remember that each one brings with it varying degrees of threat to both physical security and personal safety.

Threats to personnel safety fall into several categories:

- Smoke and fire
- Toxins
- Water/flood
- Temperature extremes
- Structural failures
- Power loss
- External bomb threat, civil unrest

Threats to Physical Security

- The seven major sources of physical loss
(Donn B. Parker, *Fighting Computer Crime*)
 1. Temperature - extreme variations of heat or cold, such as sunlight, fire freezing
 2. Gases - war gases, commercial vapors, humidity, dry air, and suspended particles
 3. Liquids - water and chemicals
 4. Organisms - viruses, bacteria, people, animals, and insects
 5. Projectiles - tangible objects in motion and powered objects

Donn Parker categorized physical threats and potential losses into these seven categories in his book *Fighting Computer Crime*.

These categories are:

1. Temperature - extreme variations of heat or cold, such as sunlight, fire freezing
2. Gases - war gases, commercial vapors, humidity, dry air, and suspended particles
3. Liquids - water and chemicals
4. Organisms - viruses, bacteria, people, animals, and insects
5. Projectiles - tangible objects in motion and powered objects

(continued on next slide)

Threats to Physical Security (2)

- The seven major sources of physical loss
(Donn B. Parker, *Fighting Computer Crime*)
 6. Movement. Collapse, shearing, shaking, vibration, liquefaction, flows, waves, separation, and slides
 7. Energy anomalies - electric surges or failure, magnetism, static electricity, aging circuitry, radiation, sound, light, radio, microwave, electromagnetic, and atomic waves

(continued from previous slide)

6. Movement. Collapse, shearing, shaking, vibration, liquefaction, flows, waves, separation, and slides
7. Energy anomalies - electric surges or failure, magnetism, static electricity, aging circuitry, radiation, sound, light, radio, microwave, electromagnetic, and atomic waves

Smoke and Fire

- Detective
 - Smoke detectors
 - Heat sensors
 - Flame
- Suppressive
 - Sprinklers (chemical, H₂O)
 - Fire extinguishers (ABC, Halon)
- Evacuation

Smoke and fire represent one of the most commonly occurring threats to personnel safety. Fire occurs when combustible fuel of some type is ignited, usually through a high temperature, and burns in the presence of oxygen. Fortunately, many devices are available to detect the threat of fire, principally smoke detectors and heat sensors. There are also many devices to extinguish an actual fire, principally fire extinguishers, sprinkler systems, and Halon fire-suppression systems.

Smoke Detectors

Smoke detectors:

- Detect smoke by virtue of the smoke interfering with a light beam being transmitted to an optical sensor
OR
- Detect smoke as a result of a change in the ionization current generated by a minute radioactive source

There are various ways for smoke detectors to identify the presence of particles that indicate a fire might have begun. Optical sensors include a light beam and detecting plate. If smoke particles enter the detector and obscure the light, the detector will alert. Other smoke detectors operate by sensing the presence of the ionized smoke particles in the air. Heat sensors, such as the typical thermometer, operate by detecting the rise in temperature above a preset acceptable threshold.

These sensors are typically fairly small and inexpensive. They can be implemented easily, even in an existing facility. Such devices emit an audible or visible signal. More sophisticated devices are SNMP-capable (Simple Network Management Protocol) and can send an alert to the console of a network or facility-monitoring station to alert a remote console operator. Each unit can easily be tested with a small smoke source or heater.

Fire Detectors

- Heat Sensors
 - Monitor the temperature in the room
 - Detect the rate of change of temperature in the room
- Flame Detectors
 - Sense the pulsation of the flame

OR

 - Sense the IR energy produced by the flame

You can detect a fire in other ways. Heat sensors and flame detectors are two other methods. It is important to remember that these are actually detection measures, not prevention measures. This means that they will detect only that there is an attack; they do nothing to stop the threat. Therefore, there must be a close tie between a detection device and a prevention device. For example, a water-based sprinkler system might be activated by a heat sensor. The heat sensor would detect the fire and then cause the sprinkler system to activate to put out the fire.

A heat sensor constantly monitors the temperature of a room. If there is a large change in the temperature over a short period of time, the heat sensor deems that there must have been a new heat source to account for this large increase in temperature. Usually, the only thing that could cause this is a fire. This is the method that heat sensors use to detect fires.

A flame detector is designed to detect that there is a flame in a given area. It does this by understanding the properties of a flame and using those properties to determine that a fire is in a specified area. The main property it uses to detect flames is the pulsation of a flame. Flames also have a high IR or infrared energy, which can be used as a means of detection.

Environment/Life Safety:

Fire Classes

1. Common combustibles: Wood products, laminates, etc., (suppress with water or soda acid)
2. Liquid: Petroleum products, coolants, etc., (suppress with gas [Halon], CO₂, soda acid)
3. Electrical: Electronic equipment, wires, etc., (suppress with gas, CO₂)
4. Combustible: Metals (suppress with dry powder)

There are three main classes of fires: Class A, B, and C. These different classifications are based on the cause of the fire. Suppression methods are different for each class of fire.

- A Class A fire is your most common type of fire. This is where wood or other such materials are burning. It is usually caused by some accidental action with a match or cigarette that catches other things on fire. With a Class A fire, water is the most common means for suppression, but soda acid can also be used.

A Class B fire is caused when a petroleum-like product, such as gasoline, catches on fire. These type of fires cannot be put out with water, but soda acid and other gases work to suppress it. There is a common thread between suppressing Class A and Class B fires: soda acid. Because it can handle both types of fires, soda acid is commonly used in portable fire extinguishers.

A Class C fire is an electrical fire, which is usually put out with gas.

A Class D fire involves combustible metals. You would use dry powder to suppress such a fire.

Environment/Life Safety- Suppression Methods

- CO₂ and soda acid remove fuel and oxygen.
- Water reduces temperature.
- Gas (Halon/Halon substitute) interferes with chemical reactions between elements.

There are two main methods for putting out a fire: liquids and gases. The main liquid used is water. It is very effective at putting out certain types of fires. However, water can cause damage and even destroy computer equipment. Gases have the advantage of putting out a fire without causing any damage to computer equipment. However, because they remove the oxygen from the air, they impact human safety. Liquids put out fires by removing the oxygen, but this is the worst of both worlds, because it has an impact to both humans and computers.

Types of Suppression Systems

- Flooding or area coverage: Suppression agent discharged through installed pipes designed to protect personnel and extinguish fire
 - Zones of coverage
 - Time-release
 - HVAC off before activation
 - Water and gas (e.g., Halon/Halon substitute common choices)
 - Water offers conventional or pre-action ("dry pipe") options.
 - Gas best used in pre-action, time-delay mode: Halon concentration of <10% can be breathed.

An important consideration in the design and installation of fire detection and suppression systems is the need to control the suppression agent (e.g., water and gas) to ensure that only the affected area or pieces of equipment are treated with the suppression agent. This can be done with the following:

- Detectors installed in *zones of coverage* to permit quick identification of the specific area in which the alarm originated.
- Automatic fire-suppression systems tied into the detectors that *will delay the release of water or gas for a designated period of time* to permit the investigation of the possible fire and allow time to either evacuate personnel or turn off the system in the event of a false alarm.

Types of Suppression Systems (2)

- Wet pipe
 - This type of sprinkler system is always filled with water up to the sprinkler head. When the temperature in the room reaches or exceeds 165 degrees Fahrenheit, the material holding back the water in the nozzle melts and releases the water under pressure.
- Dry pipe
 - In this type of sprinkler, water is not filled up to the sprinkler head. It is held back at a distance from the sprinkler head by a valve. When the temperature in the room reaches or exceeds 165 degrees Fahrenheit, the valve opens. Air that is in the pipe is expelled and the water begins to flow. In this approach, the delay of the water surge allows computer systems to power down to avoid water damage.

When deploying a sprinkler system, you can deploy many types and methods. The key differentiators are the mechanism used to deploy the device and the proximity of the water to the sprinkler head. With a wet pipe, all the pipes are filled with water all the time. Each sprinkler head that deploys the water has a sensor that activates when the temperature in the room reaches a certain level. In most cases, the sprinkler head is kept off by a piece of plastic. When the temperature becomes high enough, the piece of plastic melts, releasing the water through the sprinkler head.

A dry pipe is a sprinkler system in which the pipes that contain the sprinkler heads do not contain any water. When a fire is detected, the valve turns on and the water is deployed through the sprinkler head to put out the fire.

Types of Suppression Systems (3)

- Pre-action
 - This sprinkler system is a hybrid of the wet and dry pipe systems. When the appropriate temperature is reached, the valve that holds back the water (dry pipe system) is opened and releases water to the nozzle head. Then, the link in the nozzle head melts and releases the water (wet pipe system). This additional delay allows for manual intervention before the water is released.
- Deluge
 - Similar to the dry pipe method, this sprinkler releases a larger amount of water when discharging. Because water can cause serious damage to electronics, this method is not recommended for use around computer systems.

The previous slide mentioned the two basic types of suppression/sprinkler systems: wet pipes and dry pipes. These next two methods are composed of a combination of each. With pre-action, the system is set up with dry pipes. However, once the valve is open and the pipes are filled with water, the sprinkler heads are not activated. Each sprinkler head contains a piece of plastic (just like the wet pipe) that must melt before water is deployed. This method adds a delay that allows intervention to take place, such as shutting down or removing equipment before water is deployed. Because water can cause serious damage to computers, a pre-action system can, in some cases, minimize the damage. However, remember that this is a catch-22. The longer you take to deploy water, the more damage the fire can cause.

A deluge is a dry pipe system that releases a large amount of water. This system is meant for situations in which large fires can break out. Because a large amount of water is deployed, the deluge system can cause excessive damage to computer equipment.

Types of Suppression Systems (4)

- Gas discharge
 - Discharges an inert gas, such as CO₂ or Halon
 - Usually installed under the floor of the computer area

Another way to put out a fire is to release certain gases into the air. The goal of these gases is to remove the oxygen from the air. Because a fire needs oxygen to burn, removing the oxygen causes the fire to go out. Initially, this seems like a clean, easy, and computer-friendly way to put out a fire. The problem is that this method is not friendly to humans because humans need oxygen to survive.

Types of Suppression Systems (5)

- Portable extinguishers to minimize fire damage
 - Filled with an approved/applicable suppression agent
 - Located within 50 feet of any electrical equipment
 - At exits
- Other considerations
 - Clearly marked with unobstructed view
 - Easily reached and operated by average-sized personnel
 - Inspected quarterly

In the case of small or localized fires, put the fire out while it is still small. The longer you let a fire burn, the bigger the fire becomes and the harder it is to put it out. Therefore, having portable extinguishers near flammable devices is critical. This way, if a fire does start, it can be put out quickly with minimal damage. When selecting a portable extinguisher, it is critical that you determine the type of fire that might occur so the proper substance can be loaded into the extinguisher. Make sure you remember that not all substances put out all fires.

Because fires represent a threat to human safety, all devices used to put out a fire must be clearly marked. Most of these devices are a common color and are installed at a consistent height so they can be easily spotted.

Types of Suppression Systems (6)

- Other considerations concerning fire suppression agents
 - Water: The Fire Protection and Insurance industries support the use of water as the primary fire-extinguishing agent for aN business environments, including those dependent on information systems!
 - CO₂: Colorless, odorless, and potentially lethal because it removes oxygen:
 - Gas masks give no protection.
 - Best application is for unattended facilities.
 - Use built-in delay in manned areas.

Remember that the primary goal of physical security is personal safety. The best physical security is not acceptable if it puts human lives at risk or causes harm in protecting a system. Unfortunately, when putting out a fire, there is a direct contradiction between what is good for humans and what is good for computers. To put out a fire, water is user friendly. Water will put out the fire and not cause any long-term harm to humans. However, computers do not do well when they are waterlogged.

Another option for putting out a fire is based on the fact that fire needs oxygen to burn. Therefore, if you remove the oxygen, the fire will go out. Computers do not need oxygen and, therefore, removing oxygen is a computer-friendly way to put out a fire. Unfortunately, humans need oxygen, so this technique could cause loss of life. The most common way to remove oxygen is to use CO₂, which is colorless, odorless, and can be lethal to humans if large amounts are present and remove the oxygen from the room.

One option is to use CO₂ with a built-in time delay. This allows personnel time to exit the area or stop an accidental release of the agent. The problem is deciding on the correct amount of time. Another option is to have the last person who leaves hit a button that releases the CO₂. Again, how does that person know for sure that everyone has left? If they make a mistake, the results can be fatal. For these reasons, water is recommended as the main way to extinguish a fire.

Types of Suppression Systems (7)

- Halon (Halongenated extinguishing agent)
 - Must be thoroughly mixed with air
 - Fastest practical flooding desired
 - **Montreal protocol (1987):** Stopped Halon production 01/01/94 because it released ozone-depleting substances
 - Halon 1301 requires expensive pressurized flooding system
 - Halon 1211 self-pressurizes (used in portable extinguishers)
- FM-200: Most effective alternative; requires 7% concentration (Halon requires 5%)

Halon was originally the main way to extinguish a fire. However, because of environmental concerns, Halon has not been produced since 1994. If you have a Halon device, you can keep using it, but no new systems can use it. Several replacements for Halon work well, and some of the more accepted alternatives include the following:

PFC-410 or CEA-410

PFC-218 or CEA-308

NAF S-III

FE 13

- Argon
- Argonite
- Inergen

Most of these alternatives require a slightly higher percentage of concentration to extinguish the fire, but because they do not have ozone-depleting agents, they are more accepted today.

Floods (Water)

- Detective
 - Detectors (moisture, humidity)
 - Third-party (news, emergency warning system)
- Corrective
 - Bilge pumps (sump)
 - Evacuation

Water in the environment can be detected by both surface moisture detectors and humidity detectors for the presence of water vapor. These detectors are especially important in facilities with high power consumption and cabling because water conducts electricity and can cause significant damage in the event of an electrical short circuit. Water detectors are commonly implemented under raised flooring (because the actual floor surface is out of sight) and in areas susceptible to natural floods. As with airborne threats, staying in touch with potential community threats and National Weather Service warnings is integral to ensuring that these events do not catch the company ill-prepared.

Water and flood threats can be corrected by implementing bilge pumps, which expel water from the protected areas. These pumps are often implemented in the basements of buildings and can be powered on automatically when a water-level alarm is generated. These pumps have a capacity that should be indicated clearly and should be able to expel a specified quantity of water per hour. Properly constructed areas should include a drainage plan that allows excess water to run out of critical areas. No bilge pump or drain, however, is likely to prevent harm resulting from a flash flood or tidal wave. As with the other threats, if the water level is rising too quickly for the pump to control it, evacuation is the appropriate measure to take to protect personnel.

Earthquakes

- Detective
 - Structural assessment
 - Sudden impact
- Corrective
 - Structural reinforcement
 - Evacuation

Structural failure can result from both a gradual structural weakening or from a sudden event. Gradual structural weakening is usually the result of age or of a series of lesser events. When a company considers the structural integrity of a building to be suspect, that company needs to enlist the help of a professional, such as a structural engineer, to assess the building's condition. In the event that the assessment shows a structural weakness, the company must supplement the building with structural reinforcements or evacuate personnel.

Sudden structural failures might result from events such as earthquakes, storms, explosions, or sinkholes. These events are usually detected at their occurrence simply because of the dramatic nature of the event. With rare exception, the only means to reduce the likelihood of harm is to evacuate immediately.

Restricted Area Definition

- Restricted versus non-restricted visitor
- Motion detector to sense activity
- Escort from restricted area
 - Employee
 - Guard
- Perimeter of restricted area
 - Space
 - Time

Restricted Areas

The most important aspect of controlling access is careful and precise definition of the area to be protected. The facility should be separated into restricted and non-restricted areas. Different degrees of restriction can be created if necessary. The environment must be separated into trusted and untrusted zones, establishing the perimeter of control. After this line is established, measures must be implemented to ensure that unwanted access is avoided through deterrent measures and detected if it occurs. Finally, procedures must be implemented to end any breach.

The best method to end the unauthorized access is to escort the intruder from the restricted area. All employees should be instructed to inform physical security management if they have any reason to suspect a person is malicious. In less-sensitive areas, and if the employee is comfortable that the person entered the area unintentionally, it might be acceptable for employees to escort an accidental intruder out of the restricted area. However, if the intruder is perceived to represent a risk, employees should call guards or police to assist in the removal of the individual. As in all physical security concerns, the safety of personnel is the priority.

Detering Unauthorized Access

- Educate
 - "Employees Only" sign
- Discourage
 - Uniformed pseudo-guards
 - "Unauthorized Personnel Will Be Prosecuted" sign

Detering Unauthorized Access

Deterrent controls are implemented to modify the behavior of the individual seeking access. Because unauthorized access is caused by intentional or unintentional human actions, behavior changes can significantly decrease the number of attempted infractions of the restricted area. Thus, deterrent controls play a larger role in physical security than in any other security topic.

Detering unauthorized access relies on the ability to either educate the accidental intruder to avoid the mistake or to discourage the malicious intruder with a threat of some sort of negative consequence, such as being caught.

By educating the unintentional intruder, deterrent controls can curtail an unauthorized behavior. For example, an employee who genuinely wants to comply with company policy will not enter a door marked "IT Personnel Only" unless she is a member of the IT staff. If the door is unmarked, that employee might attempt to enter it. Educating the accidental intruder is generally done by posting information about restricted areas clearly and concisely at any entrance to the restricted area.

Discouraging the malicious intruder is generally done by more visible demonstrations of the company's dedication to physical security. In addition to the visibility of other controls, purely deterrent controls include posting individuals who have the appearance of being guards at entrances, even if the guards are unarmed, untrained, and not expected to prevent an intrusion. Additionally, signs indicating that the company will take action against intruders may also be used.

Locks

- Locks
 - Traditional Key
 - Ward
 - Wafer or disc
 - Pin tumbler
 - Replacement core
 - Cipherlock/combination lock
 - Smart card
 - Smart card with passcode
 - Biometrics
- Lockset components
 - Body
 - Strike
 - Cylinders
 - Low
 - Medium
 - High
 - Key
 - Master lock

Preventing Unauthorized Access with Locks

Preventive controls are controls designed to ensure that unauthorized personnel do not have the ability to enter restricted areas. Most of these controls represent the gateway into the restricted area. Passage through the gateway is limited to those who meet specific criteria. Additionally, the passage of contraband through the gateway must also be prevented. Prevention of unauthorized access consists primarily of presenting some obstacle to the intruder that cannot be passed without some information or tangible item. Examples of preventive controls include the following:

- Locks
- Mantraps
- Fences

Locks

Locks are one of the oldest forms of access control in human history. The basic premise of the lock is that a perimeter is secure from access except at certain specific points. At these points, a barrier is located that can be in an open/unlocked or closed/locked position. Some information or tangible item, such as the corresponding key, is required to move the barrier from the closed/locked position into the open/unlocked form.

We discuss several types of the lock-and-key principle in this section. Many additional variants of the lock-and-key principle have been developed, but this section focuses on the major implementations available today:

- Traditional
- Cipherlock/combination lock
- Smart card (with or without passcode)
- Biometrics

Important factors to be analyzed in the examination of any lock-and-key system are the following:

- Construction and mechanism
- Range of possible keys/uniqueness
- Association with individual
- Copying
- Distribution
- Initial cost and re-keying cost

Keys and Combination Locks

Keys and combination locks: The objective of entrance-door controls is to screen entrants, to deny entrance where appropriate, and to control the flow of materials into and out of the building. Screening can be done in two ways:

- Personal recognition of entrant or acceptance of credentials by guard
- Possession of a suitable device to unlock the door
 - Shortcomings: Keys or combinations can fall into the wrong hands. An intruder can enter immediately behind an authorized entrant (piggybacking).

Locks are a common measure for securing access to a given area. The two basic types of locks are key and combination locks. A key lock requires that someone have some physical entity or key that they use to open the lock. The advantage of locks is that you can control distribution by limiting who can make copies of a given key. However, keys can be lost; if this happens, the person cannot open the lock unless a backup exists somewhere.

A combination lock is based on a series of numbers that someone has to remember. In this case, there is no key to lose, but the problem is that an individual can tell others the combination. Combinations can also be written down and forgotten.

The problem with both types of lock is that there is no accountability. If five people all know the combination or have the key and someone opens the lock, you do not know who did it. Many of the more advanced locks allow you to have multiple different keys or combinations so you can track individual users.

Mantraps

Mantraps:

- Physical control
- Entrance path protected by two doors
- Intruder confined between doors

Mantraps

Mantraps are secure portals that require the individual to provide sufficient identification for the gateway to open toward the restricted area. Typically, the mantrap requires that the user allow himself to be secured in a glass box of sorts before identification is provided. Thus, any user who does not have sufficient identification, but has attempted access, will be imprisoned until released by an outside party. Most mantraps are equipped with sophisticated authentication devices, usually based on biometrics, such as iris scanning or fingerprint identification.

CCTV

- Cameras (CCTV) levels
 - Detection
 - Recognition
 - Identification
- Primary Components
 - Camera
 - Transmission media
 - Monitor
- Secondary Components
 - Pan and tilt units
 - Recorders
 - Controls
 - Multiplexing
 - Mountings
 - Panning devices
 - Infrared devices
- Types
 - Cathode ray tube (CRT)
 - Older technology
 - Charge coupled discharge (CCD)
 - Provides a better picture
- Camera lenses
 - Fixed
 - Zoom
- Iris opens and closes the lenses
- Key design factors:
 - Field of view
 - Depth of field
 - Illumination range
 - lighting

Cameras and Closed Circuit Television (CCTV)

Cameras are traditionally thought of as detective controls. In many cases, if a camera is visible, intruders will not be as inclined to attempt to enter the target area.

There are many key components and considerations to keep in mind when deploying CCTV.

Contraband Checks

Contraband checks:

- X-ray scanners, metal detectors
- Bag inspection

Additional detective measures include contraband checks such as x-ray machines, metal detectors, and bag inspections. These measures are primary detective measures, but can also deter someone from doing something if they know there is a high chance they are going to be caught.

Computer Lock Down

- Servers
- Workstations
- Laptops

Servers

Each server should be placed in some physical location that is protected, such as a server room or locking cabinet. Each server should have some or all of the following: tamper-proof seals, disabled removable media, disabled external ports, and faceplate locks.

Workstations

We must trust that physical access to workstations will be protected by building security. Other prevention measures include floppy locks, disabled removable media, BIOS passwords, tamper-proof seals, visual-perspective limiters (screen filters), idle use screen savers, and password-locked screen savers.

Laptops

Laptops have all the same issues as workstations, without the protection of the location's physical security. Some physical security-compensating controls are PC card biometrics, leash locks, and lockable luggage. Some logical controls are BIOS passwords, multifactor authentication, file encryption, and disk encryption.

Computer Lock Down (2)

- Protection mechanisms
 - Port controls
 - Devices that prevent the use of the physical data ports on a computer
 - PC locking devices
 - Cables that secure a laptop to a desk or table to prevent the theft of a laptop

There are also generic methods for locking down a computer that fall under protection methods. These methods are physical means designed to combat situations in which someone who has physical access to the system can gain access or potentially gain access to a system. Therefore, the best way to protect a system is to stop someone from gaining physical access to a system in the first place.

Computers have external ports connected to the system. Ports such as serial ports, parallel ports, and USB ports are the more common means of connecting external devices to a system. These ports could be used without the knowledge of the user to either extract data from a system or put data onto a system. Therefore, these ports should be locked down and controlled. Remember the principle of least privilege, which states that you should give an entity the least amount of access needed to do a job. If you do not need to use the external ports, you should configure the ports to prevent the system from communicating with them. If this is done, even if someone connects a device to a port, she will be unable to communicate with the system.

Even if you have strong passwords and encryption, someone can still steal your computer and, from the comfort of her own home, try to break into your system. Even if she cannot gain access to your data, she can still use or sell the hardware. From your perspective, even if an attacker cannot gain access to your data, you just lost access to your data, which might cause an availability attack for you. This is why it is important to perform personal backups of your critical data. However, be sure not to store personal backup media in the same carrying case as your laptop. This way, your backup will not be stolen with the laptop.

Computer Lock Down (3)

- Protection mechanisms
 - Switch controls
 - Covers on switches or lockable switches that prevent switches from being operated by an unauthorized user

Anything that controls access to a system must be properly protected with locks. In some environments, the control mechanisms for a computer (keyboard, mouse, and monitor) can be connected to a switch that controls which central processing unit (CPU) is being operated. In some cases, only certain computers can be operated by certain people and, therefore, control to the switch box should be limited or controlled through some locking mechanisms in which only authorized users can gain access.

Intruder Detection

- Manual
 - Security lights/watch tower
 - Dog patrols
- Automatic
 - Motion detector
 - Heat/infrared sensor

Detecting Unauthorized Access

Detecting unauthorized access is a crucial factor in the success of any security program. Despite the implementation of strong preventive and deterrent controls, there is a possibility that unauthorized access will occur. If it does, prompt and precise detection is critical to protecting company assets. The secondary component in detecting unauthorized access is detecting the transportation of contraband into a restricted area. Contraband is material that is defined by policy as not permissible within restricted areas. After this policy is defined, controls to identify and exclude or confiscate contraband must be implemented.

Nighttime detection can be assisted by the use of security lights, which illuminate the perimeter and interior of the restricted area. These lights facilitate the watchfulness of guards and security-conscious personnel. Lights and guards can be positioned on a watchtower to increase the area they can cover. Security lights, which increase the illumination of a general area, include floodlights or searchlights that can be rotated toward an area of interest.

Intruder Detection (2)

- Manual
 - Requires active participation by a human
- Automatic
 - Subject to false alarms or malfunction

Intruder Detection

Manual detection occurs with the use of systems such as closed circuit television (CCTV) and the monitoring of these systems by personnel who determine that an individual within the restricted area is unauthorized. Security cameras are expensive, and organizations on occasion opt to use a combination of dummy cameras and genuine operating devices. Care must be taken in these circumstances to avoid creating liability caused by an expectation of protection. Some case law exists to show that if a crime occurs in the presence of dummy cameras and the victim believed that the camera was active and that security was aware of the situation, the company might be held liable for injury or damage that occurred because of this expectation.

After an intruder has been observed, an audible alarm should be sounded to notify all personnel in the area of the potential risk. If an intruder alarm is sounded, employees should be aware of appropriate lock-down procedures, even those as simple as closing and locking office doors, to reduce the potential of a hostage situation.

In environments where a hostage situation is more likely, for example in a bank branch, those who might be held hostage should be equipped with a means to alert security personnel without necessarily alerting the intruder. These silent alarms or panic buttons are generally located close to an individual workspace, such as a teller's desk, and are hidden from view, such as under a counter.

Facility Controls

- Fences
- Landscape
- Vehicle barriers
- Guards
- Dogs
- Badges
- Lights
- Motion detectors, sensors, and alarms

There are many controls you should put in place to protect your facility. Each control has a different level of effectiveness. However, when you deploy all of them together, they provide a robust level of protection.

Fences are good perimeter controls for keeping someone out of a given area. Fences can also keep someone in a certain area (for example, prisons). However, fences are passive devices. Guards and dogs are more reactive because they can make decisions based on surrounding events. Guards can use more judgment and base their decisions and actions on the specific situation. Dogs are simple "devices" because, in essence, if anyone comes into their area, dogs will attack. A guard, however, can take this to the next level. If someone comes into their area without a badge and they are not on a visitor list, they won't be let in.

Badges can identify and authenticate a given individual, but they do no good if someone or something does not authenticate them. Therefore, either a guard or a badge reader is needed in these situations.

Additional measures of protection can be provided with keys, lights, and motion sensors. These topics are explored in the following slides.

Facility Controls (2)

- Physical protection measures, physical barriers, and intrusion detectors ultimately depend on human intervention. Security guards, whether at a fixed post or on a roving patrol, can help in this area.
 - Duties may include
 - Checking entrance credentials
 - Issuing and recovering visitor badges
 - Monitoring CCTV, intrusion and fire-alarm systems
 - It is important that guards are properly trained and that their orders are complete and clear.
 - Dogs are primarily used for perimeter control.

Whenever you try to protect an asset, such as a building or the computers within the data center of the building, the farther away from that asset you can stop an attacker, the better off you are. If you wait to stop an attacker after he is in the building, even though he has not gained access to the data center he can still cause much damage within your building.

Barriers such as cement walls are a good complement to fences. Trucks and other large mobile devices can run through a fence, but if that fence has 3-foot barriers behind it or roaming guards with weapons, breaching the perimeter becomes much harder. Roaming guards play a critical role because they add an unpredictable measure to your defense. If your protective measures are always the same and never change, it is easier for an attacker to plan a way to defeat them. However, if they are always changing, this task is more difficult.

Fences

Fences:

- Varying heights provide varying levels of protection
 - 3-4 ft / 1 meter (deters casual trespasser)
 - 6-7 ft / 2 meters (too high to easily climb)
 - 8 ft / 2.4 meters + 3 strands of barbed wire (deters determined intruder)
- Considerations
 - Provides crowd control
 - Helps control access to entrances
 - Can be costly
 - May be unacceptably unsightly

Depending on the objective you are trying to achieve, different types of fences are available. In most cases, the higher the fence, the harder it is for someone to breach. On the surface, this makes sense because a 3-foot fence is easier to climb than a 10-foot fence. However, a fence by itself can be defeated with the proper equipment. Therefore, additional measures should be put in place to make fences more difficult to breach.

Barbed wire at the top of the fence makes it harder for someone to climb, but this still allows someone to get to the top of the fence. Therefore, barbed wire can also be put at 3-foot vertical intervals to make the fence even more difficult to climb. Electric fences also serve as a deterrent. However, you must always keep the aspect of human safety in mind.

Gates

Types of gates:

- Class I - residential gate
- Class II - commercial gate
 - Garage
- Class III - industrial gate
 - Loading dock
 - Factory
- Class IV - restricted access
 - Prison
 - Airport

Similar to fences, gates can be used to control access. Gates, however, are designed so that they can open and close.

The following are the key types of gate:

- Class I - residential gate
- Class II - commercial gate
 - Garage
- Class III - industrial gate
 - Loading dock
 - Factory
- Class IV - restricted access
 - Prison
 - Airport

Security Guards

- Availability
 - They cannot exist in environments that do not support human intervention.
- Reliability
 - The pre-screening and bonding of guards is not foolproof.
- Training
 - Guards can be socially engineered, or may not always have up-to-date lists of access authorization.
- Cost
 - Maintaining a guard function either internally or through an external service is expensive.

As with any security measure, you always have to weigh the positive and negative aspects, and guards are no different. A guard can be trained with a complex set of rules and, based on various conditions, can make decisions on who should gain access. Guards can also call for backup and use additional force, such as weapons. However, guards cannot be used in all conditions and can only work a limited number of hours without having a break or getting rest. Because guards are human — and humans get sick, have emergencies, or get into accidents, they are not always available as originally planned. Therefore, planning for redundancy in the guards' schedules and training guards to react to a variety of different situations can be an effective, but very costly, solution.

Dogs

- Dogs are primarily acceptable for perimeter physical control and are not as useful as human guards because they cannot make judgment calls.
- Additional drawbacks include cost, maintenance, and insurance/liability issues.

Compared to humans, dogs are more flexible with respect to the hours they work. It is acceptable to keep dogs outside for 24 hours without a break. Dogs are also capable of sleeping on the job and still being able to perform their duties. Guard dogs can be awakened from a sound sleep when they hear the slightest noise and can perform their task within a moment's notice.

However, dogs have a negative side. Dogs cannot check badges or make decisions. They are essentially binary devices. Attack or do not attack. Dogs are usually used in conjunction with fences. The logic is simple. If someone comes within the boundaries of the fence, attack them. Therefore, from a liability standpoint, companies must pay close attention to posting warnings so someone does not accidentally go into an area and get attacked by a dog.

Badges

Two common card types:

- Photo image
 - Dumb card, requires a guard to make a decision
- Digitally-encoded
 - Smart card, entry decision made electronically
 - Digitally-coded cards: Contain chips or magnetically-coded strips (with or without the photo)
 - Wireless proximity readers: The card reader senses the card in possession of the user in the general area (proximity).

Badges are used as a form of authentication to prove that you are authorized to access a given area. The most basic type of badge is made of some sort of plastic that has information and usually a picture on it. There is no other encoding present on the badge. With these simple badges, usually there must be a human involved who can examine the picture, make sure it matches the person who is holding the badge, and then allow or deny access to that person.

The first problem with a basic badge is it requires a person to verify access. Because of this, digitally-encoded smart cards are becoming more popular. The badge is actually encoded with a magnetic strip or computer chip. The benefit of these badges is that they can be validated by a reader and do not require human involvement.

A drawback to a proximity card is how to handle the issue of a lost card. My proximity card is located on the same dongle as my ID badge. If I lose both, the finder would have my name and work information from my ID badge. He will also have access to the restricted areas I have access to through my proximity card. Unless a mechanism is in place to report and disable my card during on and off hours, the finder can use my ID to learn my physical work location or department through conversation with the PBX operator (social engineering). Armed with location information, it is a simple matter to physically go to the department and use the proximity card to gain physical access to the department and data center. The proximity card is used by all employees to gain entrance to the facility and parking structures. A compensating control could be adding two-factor authentication in the form of a password keypad at sensitive locations, such as at the data center and wiring closets (in addition to proximity card).

Lights

- Outside lighting
 - Floodlights
 - Streetlights
 - Fresnel lenses
 - Searchlights
 - Gaseous discharge
 - Continuous lighting
 - Trip lighting
 - Standby lighting
 - Emergency lighting
- Considerations
 - Security over physical spaces and buildings
 - Safety of personnel
 - Lighting should be used to discourage prowlers and intruders
 - Building critical areas, entrances, and parking areas
 - Critical areas around buildings - Install lighting at least 8 feet (2.4 meters) high and with illumination of 2-foot candles.

We use lighting in everything that we do, but we tend to forget that lighting comes in all different types and lenses, all of which are used for different purposes. Typically, with outdoor lighting, the goal is to either light up an area for building or personal safety. A building that is well-lit is less likely to be burglarized than one that is in the dark. Lit buildings are also easier for a guard to monitor. The guard can quickly see if something is happening that should not be.

From a personal safety standpoint, any walkways that people use should be well-lit so that people can see and not accidentally fall or trip because of the darkness. Well-lit areas also make it more difficult for someone to sneak up on another person. As with most security issues, we have to remember defense-in-depth and always have multiple levels of protection. In addition to a well-lit walkway, there should be no bushes or objects near the path that an attacker could hide behind in order to sneak up on someone.

Fresnel lenses are special lenses that have a thin optical lens of many concentric rings that have the properties of a much thicker, heavier lens. Fresnel lenses are used in cameras, lighthouse beacons, etc. In a really secure facility with high walls, fencing, and guard towers, a searchlight (using a Fresnel lens) might be appropriate at the guard towers (for example, at a prison yard or nuclear facility).

Motion Detectors, Sensors, and Alarms

Four technologies for detecting the presence of an intruder

1. Photometric systems: Passive systems that detect a change in the level of light in an area because of added light sources
2. Motion detection systems: Active, Using Doppler
 - Three types
 - Sonic (audible sound waves)
 - Ultrasonic (high-frequency sound waves)
 - Microwave (radio waves)
3. Acoustical-seismic detection system (audio): Microphone-type device that detects sounds that exceed the ambient noise level of the protected area
4. Proximity: Uses an electronic field that senses the presence of an object or individual

Ideally, you want to prevent someone from gaining access to a given area, but in cases where you cannot prevent access, you want to be able to detect them in a timely manner. Locks and fences are preventive measures. Motion detectors, sensors, and alarms are detective measures. If someone has breached your preventive measures and gained access, you try to detect them before they do any damage.

One means of detecting an intruder is monitoring the level of light in a given area and detecting any change. When someone enters an area, the level of lights in a given area changes through movement and shadows. That change can be detected by special sensors. Motion sensors are also popular for detecting movement in a given area. Motion sensors are a common technology and have undergone significant improvements over the last several years.

There is also a technology that can detect slight noise in a given environment. No matter how quiet intruders think they are, certain noises are generated just by walking and breathing. Acoustical-seismic detection systems detect those noises as exceeding the ambient noise level.

Proximity devices use an electronic field to sense the presence of an object or individual.

The important thing to remember is that there are always ways to defeat a single technology, but deploying several technologies together gives you a more robust solution.

Site Selection Considerations

- Visibility
 - Neighbors
 - External markings
- Local considerations
 - Near hazards
 - Crime rate
- Natural disasters
 - Earthquake fault
 - Weather related (floods, hurricanes, heavy snow)

The physical threats that your facility faces are dictated by the location of the building. Therefore, carefully selecting where you choose to have your data center can greatly increase or decrease a given level of threat. Remember that threats directly map to your vulnerabilities, which help determine your overall risk.

If you provide a service that others might want to destroy or compromise, why would you advertise your location or put your company name on the building? In these situations, you would want to protect the physical location to limit possible threats that someone might launch.

From a local standpoint, knowing the crime rate and facilities that are nearby could also impact the safety of the facility. One company built a new data center and never surveyed the surrounding area. It turned out that the company was very close to a rock quarry and the blasting caused enough damage that it had to relocate within one year.

Regional selection is equally important. Knowing the weather conditions for a given area could impact where you build your data center.

Site Selection Considerations (2)

- Transportation
 - Excessive air, highway, or road traffic
- Joint tenancy
 - Access to environmental and HVAC controls shared
- External services
 - Proximity of fire, police, and hospital

When deciding where to locate your data center, in the words of any good real-estate agent—location, location, location. Understanding your needs will greatly help in the selection process. Being near highways and airports can have its positives and negatives. Excessive noise might not be desirable, but having easy access to the roadways might be worth the drawback.

Depending on the type of work that is being performed, being close to a fire department and hospital might also be desirable qualities. As with the previous items these decisions have both pros and cons; each must be weighed carefully when making a decision.

Facility Design

- Local building construction standards
- IS/IT facility construction standards
 - Light frame
 - Heavy frame
 - Fire rated
- Floor slab
 - Loading
 - Fire rating
- Raised flooring
 - Grounded (static buildup)
 - Nonconductor surface
- Walls
 - Floor slab to ceiling slab
 - Fire rating
 - Adjacencies/exterior
 - Paper/record/tape storage

When designing a facility, it is critical to consult with an architectural expert. There are so many state and local zoning and building codes that it is impossible for you to understand them all. Every floor in a building has a maximum occupancy and fire rating. These ratings dictate what can be put on a given floor in terms of weight and electrical considerations.

Because data centers require a lot of heavy infrastructure, such as a raised floor and heavy equipment that require big electrical draws, most data centers are built on the slab, which essentially means the ground floor or the basement. This overcomes many of the zoning issues, but has the drawback of being on the bottom floor.

Enclosed Areas

<u>Dimension</u>	<u>Examples</u>
• Floor	Raised floors, in-floor ventilation
• Wall	Doors, windows, mail slots, fireplaces, vents
• Ceiling	Ceiling ventilation, crawlspace, light fixtures, sprinkler fittings

After an enclosed space has been labeled as a restricted area, each entry point into this area must be identified and should be assessed in all dimensions. Common areas where this can be breached are floors, walls, and ceilings.

A raised floor could be large enough for someone to be able to gain access to an area where they should not be allowed. A key feature of an enclosed area is to have a slab-to-slab wall, which means the actual walls go from the base floor to the base ceiling so there is no opportunity to sneak in. A common mistake in securing a restricted area occurs in instances in which the wall in a data center goes only from the raised floor to the drop ceiling. This allows an attacker to sneak under the floor to gain access to the data center.

Walls are the common means of access to an area through doors or windows. Because they are meant as access points. Even if they are locked, most people target doors and windows as areas to exploit. Although doors and windows are obvious means for gaining access, there are other less obvious access points. Mail slots meant to slip mail into an area can be used to gather information or as a means to gain access. A small camera attached to a wire can be slipped through a mail slot to take pictures of an area. Also, if the facility has a motion sensor to open the door for internal people, a mail slot can be used to slip in a long wire to trip the motion sensor and open the door.

Wall construction should also be considered. If an area has severe access restrictions and the wall is constructed of drywall, having a large, heavy door is of no consequence. All an intruder needs is a large knife or a heavy object to literally break through the wall.

Ceilings can be used to gain access in a manner similar to the one described for floors if the walls are not slab to slab.

Doors

Doors:

- Interior/exterior
 - Hardware
 - Hinges location
- Directional opening
- Forcible entry (doors and frames)
- Fire rating equal to walls
- Emergency egress (markings/hardware)
- Monitored/alarmed
- Emergency exit (power outage/fire)
- Hollow vs. solid core
- Panic bars

When designing a facility, especially a data center, the devil is in the details. What seems simple when you are building can cause major headaches later. Picking the location of doors is critical. Doors provide an access point into a protected area, but they also provide a means for an attacker to exit or remove equipment without anyone noticing. Based on this fact, one would minimize the amount of doors in your data center. However, human safety must always be addressed. There must be a proper number of doors so someone can exit in an emergency. Also, the way a door is installed is critical. If the hinges to the door are on the outside facing a non-secure area, someone can pop the hinges, remove the door, and gain access to the data center.

From a human-safety standpoint, you should also check which way a door swings to make sure that when it is open, it is not blocking a critical exit point. All exits must be clearly marked and must never be blocked so people can exit in a timely manner.

Windows

Windows:

- Laminated glass
- Wired glass
- Solar window films
- Security film
- Glass breakage
- Bullet proof
- Explosive resistant

Windows can be used as an entry point into a facility.

The following are the general types of windows that can installed:

- Laminated glass
- Wired glass
- Solar window films
- Security film
- Glass breakage
- Bulletproof
- Explosive resistant

HVAC

- Other
 - Water/steam/gas lines
 - Shut-off valves
 - Positive drains
- Heating, ventilation, A/C, refrigeration (HVAC)
 - Dedicated/controllable
 - Independent power/EPO
 - Positive pressure
 - Protected air intakes
 - Environmental monitoring

Computers generate heat and require certain conditions for them to operate in an optimal fashion. Studies show that a computer exposed to extreme temperatures and humidity greatly decreases the life of a computer system. This decrease can cause unpredictable failures that can lead to denial of service attacks for an organization.

Having proper heating and cooling with proper backups is critical in most environments.

Environment/Life Safety

HVAC considerations:

- Maintaining appropriate temperature and humidity levels
- Installing a closed-loop recirculating air conditioning system to maintain air quality
- Positive pressurization and ventilation to control contamination

HVAC stands for heating, ventilation, and cooling. When we walk into a building, HVAC is something we take for granted; but designing a proper HVAC solution can be complicated. The critical problem is maintaining a constant temperature and humidity level year round, regardless of the number of computer systems installed or the outside temperature. You can't control the outside temperature, but it is predictable. And, you can control the number of systems in a data center with proper planning. The key aspect with HVAC is proper planning.

By knowing what systems you are going to put in today and what systems you plan on adding in the future, you can design proper HVAC into your solution.

Temperature and Humidity

- Temperature and humidity
- Temperature range of 70-74° F/21-23° C optimal for system reliability and operator comfort levels
- Relative humidity (RH) between 45% and 50% most suitable for safe data processing
 - High humidity can cause corrosion.
 - Low humidity can cause too much static -20,000 volts possible with low humidity. (17,000 volts can ruin system.)
 - Static equaling 4000 volts is possible under normal humidity conditions on a hardwood or vinyl floor.
 - Static charges due to improper humidity levels can cause damage to electronics.
 - The ideal operating humidity range is defined as 40 percent to 60 percent.

Every piece of computer equipment is different and every vendor makes different recommendations. But in most cases, a proper operating temperature for most systems is between 70-74 degrees F. However, maintaining this temperature can be difficult, so most organizations keep their data centers around 60 degrees. The other main reason for doing this is that by keeping it lower, if the cooling stops working for a short period of time, it will take a while for the room to heat up to over 75 degrees.

Humidity is another variable that you have to be concerned with. Too much humidity is bad, and too little humidity is not a good thing. Therefore, keeping a proper balance is critical. If the humidity is too high, it can actually cause corrosion and decrease the equipment's life. If the humidity is too low, it can cause excessive static buildup, which can damage computer equipment.

Static Charge Voltage Damages

Static Charge in Volts	Will Damage
40	Sensitive circuits and transistors
1,000	Scramble monitor display
1,500	Disk drive data loss
2,000	System shutdown
4,000	Printer Jam
17,000	Permanent chip damage

Static charge voltages and the corresponding damage they can produce if static build-up occurs and is discharged into a circuit are listed here.

Environmental and Life Safety Controls

Humidity:

- Static charge can be reduced by:
 - Maintaining proper humidity level
 - Using anti-static sprays
 - Installing anti-static flooring
 - Grounding buildings and computers properly
 - Using anti-static table coverings
 - Using anti-static floor mats

The idea is to keep static charges from building up and discharging into sensitive electronic components.

The following are ways that static charge can be reduced:

- Maintaining proper humidity level
- Using anti-static sprays
- Installing anti-static flooring
- Grounding buildings and computers properly
- Using anti-static table coverings
- Using anti-static floor mats

Air Quality

Air quality and contamination:

- Airborne particulate levels should be maintained at appropriate levels
 - Dust and other contaminants can impact sustained operations of computer hardware.
 - Excess concentration of certain gasses (ammonia, chlorine, etc.) can accelerate corrosion and cause failure in electronic components.

A clean room is an area where all air flowing in and out of the room is carefully controlled and filtered. Today, a data center does not have to be a clean room, but there should be a proper level of air quality flowing into the room. Did you ever walk into a room and start sneezing or have your eyes start watering? This is caused by a high amount of dust or other airborne particles. You cannot visible see them, but your body reacts. A computer system could be impacted, just as your body was. Too high of a particulate level can decrease the life of the computer.

Electrical Power

- Electrical power
 - Noise: Unwanted electrical signals
 - Electromagnetic interference (EMI) and Radio frequency interference (RFI): Unwanted signals generated by electric motors, fluorescent lighting, computer systems, and so on

It might seem like an obvious statement, but computer equipment needs electricity to properly function. We take for granted that when you plug a system into the wall, you are getting steady voltage. However, all power is not the same. Electrical signals can have spikes and lows that could impact your equipment. Several things can be done at a facility or outlet level to help control the fluctuation in electrical signal.

Electronic devices can also cause interference. I know when I talk on my cell phone and walk by certain TVs or other electronic devices, it can cause those devices to have interference or make clicking noises. All of these could impact the health and reliability of a given piece of equipment.

Electrical Power (2)

- Electrical power
 - Protection measures
 - Shielding
 - Proper grounding
 - Conditioning of power lines
 - Care in routing of cables

For basic home computer equipment, the power that comes across the line is acceptable. However, with high-end equipment for a data center, which could represent a significant amount of revenue, grounding and shielding the electrical power going into a data center is critical.

It is recommended that you carefully run power lines in one area and route cables in a separate area. Having wires near each other can cause interference problems. Most organizations set up separate conduits: one for power and one for data and other cables.

Electrical Power (3)

- Electrical power (continued)

- Definitions

- Fault: Momentary power loss
 - Brownout: Prolonged low voltage
 - Blackout: Loss of all power
 - Spike: Momentary high voltage
 - Sag: Momentary low voltage
 - Surge: Prolonged high voltage
 - Transient: Short duration noise interference

Several definitions refer to non-optimal power. They all deal with either highs or lows in the power. The other differentiating factor is how long the change lasts.

A fault and blackout both deal with power loss, but a fault is for a short period of time while a blackout lasts longer. A sag and brownout both deal with low voltage, but a sag is for a short period of time while a brownout lasts longer. A spike and surge both deal with high voltages, but a spike is for a short period of time while a surge lasts longer.

Object Reuse

- Concept of reusing magnetic storage media after its initial use
- Critical data might remain on the media (data reminiscence)
- Media storage
 - Paper printouts
 - Data backup tapes
 - CDs
 - Diskettes
 - Hard drives
 - Flash drives
- Common storage areas
 - On-site
 - Off-site
- Data reminiscence
 - Residual information remaining on the media after erasure

Depending on the type of external media you are using, it can get expensive to constantly buy new media. Especially when the information on a given piece of media is no longer needed, why not just reuse the media? The problem that occurs is that the original information can probably still be recovered from the media. Therefore, it is important to keep classification levels for data and media and only reuse media within a certain classification.

If a piece of media contains sensitive financial data that is no longer used and that same media is used to store other sensitive financial data, that is less of a concern. However, if the media that contains sensitive data is now given to an external entity, it is a bigger concern because a company's information could be externally leaked.

Object Reuse (2)

- Data destruction and reuse
 - Magnetic media
 - Degaussing
 - Overwriting
 - Formatting a disk multiple times
 - Paper reports
 - Shredding
 - Burning
- Stages of data removal
 - Clearing: overwriting the data multiple times
 - Purging: usually refers to degaussing magnetic media
 - Destruction: physically destroying the media by burning and/or crushing

There is a saying that once a piece of information exists on a computer, you will never be able to get rid of it; it will exist forever. One reason why this is true is that usually a given piece of data is copied and exists in many forms. People forget all the areas that contain copies of their information.

The second reason is because when you delete a piece of information, even though from a human standpoint the data seems to be deleted, it most likely still exists and can be recovered with the proper tools. With external media, a common way to delete a piece of information is to go to the location on the media and overwrite it several times with alternate strings of 1s and 0s.

Physical media can also be destroyed with certain chemicals that actually disintegrate the media.

Summary

- Defenses must be layered - defense-in-depth
- Safety
- Evacuation procedures
- Threats
- Physical access control
- Facility controls
- Site selection
- Facility design
- Biometrics for access control
- Environment/safety issues
- Object reuse

In this section, we looked at the critical areas of physical security. One concept that you must grasp is that defenses must be layered. This creates a defense-in-depth, which is the most effective means of ensuring physical security. Some of the key concepts we covered are :

- Safety
- Evacuation procedures
- Threats
- Physical access control
- Facility controls
- Site selection
- Facility design
- Biometrics for access control
- Environment/safety issues
- Object reuse

Acronym List

Appendix 6-B

Acronym List for SANS Security Essentials

Acronym	Definition
3DES	Triple DES (NIST)
3G	Third Generation (telephony)
ABM	Asynchronous Balanced Mode
ACE	Access Control Entry
ACK	Acknowledgement Field Valid flag (TCP) <i>or</i> Acknowledgement number
ACL	Access control list
ACM	Association for Computing Machinery
AD	Active Directory (Microsoft)
ADCE	Active Directory Client Extensions
ADSL	Asymmetrical Digital Subscriber Line
AES	Advanced Encryption Standard (NIST)
AFS	Andrew File System
AH	Authentication Header (IPsec)
ALE	Annualized Loss Expectancy
ALT	ALTerate
AMAP	Application Mapping tool
AMD	AutoMounteD (Unix)

AMEX	American Express
ANSI	American National Standards Institute
AP	Access Point (WLAN)
APOP	Authenticated Post Office Protocol
ARIN	American Registry for Internet Numbers
ARM	Asynchronous Response Mode
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
AS	Authentication Server
ASAP	As Soon As Possible
ASCII	American Standard Code for Information Interchange
ASIC	Application Specific Integrated Circuit
ASP	Active Server Page (Microsoft)
ASR	Automatic System Recovery
AT	Administration Tools
ATM	Asynchronous Transfer Mode <i>or</i> Automatic Teller Machine
AV	Anti- Virus
AXFR	Zone Transfer
b	Bit

B	Byte (8 bits)
BCP	Business Continuity Plan
BDC	Backup Domain Controller (Microsoft Windows NT)
BER	Bit Error Rate
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BID	BlackICE Defender
BIND	Berkeley Internet Name Daemon
BIOS	Basic Input/Output System (Microsoft)
BITS	Background Intelligent Transfer Service
BMP	Bitmap File Format (Microsoft)
BO	Back Orifice
BOCA	Building Officials and Code Administrators International, Inc (Building Codes)
BOF	Back Officer Friendly
BOOTP	Bootstrap Protocol
Bps, b/s	Bits per second
BS	British Standard
BSD	Berkeley Software Distribution
BSI	British Standard Institute

BSS	Basic Service Set
CA	Certificate Authority (PKI)
CACM	Communications of the ACM
CAST	Carlisle Adams, Stafford Tavares
CAT	Category
CBC	Cipher Block Chaining mode
CCITT	Consultative Committee for International Telegraphy and Telephony
CCTV	Closed Circuit Television
CD	Compact Disk
CDE	Common Desktop Environment
CDFS	Compact Disk File System
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data
CDROM	Compact Disk Read-Only Memory
CEO	Chief Executive Officer
CER	Crossover Error Rate
CERN	A French acronym for the European Laboratory for Particle Physics
CERT	Computer Emergency Response Team (deprecated name)
CFB	Cipher FeedBack mode
CGI	Common Gateway Interface

CHAP	Challenge-Handshake Authentication Protocol
chargen	Character Generation Service
CIA	Confidentiality, Integrity, and Availability
CID	Consensus Intrusion Database
CIDF	Common Intrusion Detection Framework
CIDR	Classless Interdomain Routing
CIFS	Common Internet File System
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CIS	Cerberus Information Security
CLR	Common Language Runtime (Microsoft)
en	Common Name
CNN	Cable News Network
CO	Central Office
COM	Component Object Model (Microsoft)
COMEX	Commodity Exchange
COPS	Community Oriented Policing Services
CPU	Central Processing Unit
CRC	CyclicalRedundancy Check
CRII	Code Red II Worm

CRL	Certificate Revocation List (PKI)
CRYPT	UNIX Password Algorithm
CS	Code Segment
CSE	Communications Security Establishment (Canada)
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSO	Chief Security Officer
Ctrl	Control
CVE	Common Vulnerabilities and Exposures
CWR	Congestion Window Reduced
DAC	Discretionary Access Control
DACL	Discretionary Access Control List
DAD	Destruction, Alteration, and Disclosure
DARPA	Defense Advanced Research Projects Agency (US)
DBS	DOS Boot Sector
dc	Domain Components
DC	Domain Controller (Microsoft)
DCE	Data Communications Equipment
DCT	Discrete Cosine Transform
DDE	Dynamic Data Exchange

DDoS	Distributed Denial of Service
DEA	Data Encryption Algorithm
DEC	Digital Equipment Corp. (now Compaq)
DeCSS	De-Contents Scrambling System
DEFCON	DEFense CONdition
DEL	DELeTe
DES	Data Encryption Standard (NIST)
DESTPORT	DESTination PORT
DF	Don't Fragment flag (IP)
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DLCI	Data Link Connection Identifier
DLL	Dynamic Linked Library
DMZ	Demilitarized Zone
DN	Distinguished Name (PKI)
DNS	Domain Name System or Service
DNSSEC	Domain Name System Security
DOCSIS	Data Over Cable Interface Specification
DOJ	Department of Justice (US)
DoS	Denial of Service

DOS	Disk Operating System (PC)
DRP	Disaster Recovery Plan
DSA	Data Signature Algorithm
DSDM	Dynamic Systems Development Method
DSL	Digital Subscriber Line
DSS	Digital Signature Standard (NIST)
DSSS	Direct Sequence Spread Spectrum
DTE	Data Terminal Equipment
DTK	Deception Toolkit (Cohen)
DVD	Digital Versatile Disc
EAS	Emergency Alert System
EAP	Extensible Authentication Protocol
EBCDIC	Extended Binary Coded Decimal Interchange Code (IBM)
ECB	Electronic Code Book mode
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECE	ECN Echo
ECPA	Electronic Communications Privacy Act

ECN	Explicit Congestion Notification
EDGAR	Education Department General Administrative Regulations
EER	Equal Error Rate
EF	Exposure Factor
EFS	Encrypting File System
EGP	Exterior Gateway Protocol
EGS	European Global System (wireless)
EIA	Electronic Industries Alliance (was Electronic Industries Association)
EICAR	European Institute for Computer Anti-Virus Research
EIGRP	Extended Interior Gateway Routing Protocol (Cisco)
EMS	Enterprise Management System
ERD	Emergency Repair Disk (Microsoft)
ESP	Encapsulating Security Payload (IPsec)
-ESS	Extended Service Set
EU	European Union
EV	Event Viewer (Microsoft Windows NT/2000)
EVT	Event Viewer File Format (Microsoft)
FAA	Federal Aviation Administration (US)

FAQ	Frequently Asked Questions
FAR	False Accept Rate
FAT	File Allocation Table (Microsoft)
FBR	Floppy Boot Record
FC	File Compare Command (DOS)
FCS	Frame Check Sequence
FDDI	Fiber Distribution Data Interface (ANSI)
FEC	Forward Error Correction
FFS	Standard Berkeley Fast File System
FHSS	Frequency-Hopping Spread Spectrum
FIFO	First In, First Out Queue
FIN	Finish Flag (TCP)
FIPS	Federal Information Processing Standard (US)
FQDN	Fully-Qualified Domain Name
FR	Frame Relay
FRS	File Replication Service (Microsoft)
FRR	False Reject Rate
FTP	File Transfer Protocol
FW-1	Firewall-1 (Checkpoint)
FYI	For Your Information

G	Giga; 1,000,000,000 = 10^9 (bit rate) or 1,073,741,824 = 2^{30} (storage) j
GAO	Government Accounting Office (US)
Gb	Giga-bits
GCFW	GIAC Certified Firewall Analyst
GCHQ	Government Communication Headquarters (UK)
GECOS	General Electric Comprehensive Operating System
GHz	Giga-Hertz
GIAC	Global Information Assurance Certification
GIAC-TC	Global Information Assurance Certification-Training Center
GID	Group Identifier (Unix)
GIF	Graphic Interchange Format (CompuServe)
GIG-E	Gigabit Ethernet
GIMP	GNU Image Manipulation Program
GLB	Gramm Leach Bliley Act. (US)
GNU	GNU's Not Unix
GPL	GNU Public License
GPO	Group Policy Object (Microsoft)
grep	Get Regular Expression and Print
GRUB	Grand Unified Bootloader
GSM	Global System for Mobile Communications

GUI	Graphical User Interface
HDLC	High-Level Data Link Control (ISO)
HIDS	Host-based Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HKLM	HKEY_LOCAL_MACHINE (Microsoft)
HMAC	Hashed Message Authentication Code
HR	Human Resources
HSRP	Hot Standby Router Protocol (Cisco)
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL
HUP	Hang-Up
HVAC	Heating, Ventilation, And Cooling
Hz	Hertz; cycles per second
I/O	Input/Output
IANA	Internet Assigned Numbers Authority
IASIW	Institute for the Advanced Study of Information Warfare
IBM	International Business Machines Corp.
IBSS	Independent Basic Service Set
ICE	Information Concealment Engine (Encryption)

ICF	Internet Connection Firewall (Microsoft)
ICMP	Internet Control Message Protocol
ICQ	Internet Call to Quarters, derived from military and ham radio CQ, or "call to quarters" signal; also derived from phrase "I seek you"
ICSA	International Computer Security Association
ICV	Integrity Check Value (IPsec)
ID	Identifier <i>or</i> Intrusion Detection
IDC	International Data Corp.
IDE	Integrated (or Intelligent) Drive Electronics
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detection System
IE	Internet Explorer (Microsoft)
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IHL	Internet Header Length (IP)
IIS	Internet Information Server (Microsoft)
IKE	Internet Key Exchange (IPsec)

IMAP	Internet Message Access Protocol
IOS	Internetwork Operating System (Cisco)
IP	Internet Protocol or Instruction Pointer
IPsec	IP Security Protocol
IPv4	IP Version 4
IPv6	IP version 6
IPX	Internet Work Packet Exchange Protocol (Novell)
IQUERY	Inverse query
IRC	Internet Relay Chat
IRDP	Internet Router Discovery Protocol
ISAKMP	Internet Security Association and Key Management Protocol (IPsec)
ISDN	Integrated Services Digital Network
ISM	Internet Service Manager (Microsoft) or Internet System Manager
ISN	Initial Sequence Number (TCP)
IS	Information Systems
ISO	International Organization for Standardization or Internet Security Officer
ISP	Internet Service Provider
ISS	Internet Security Systems, Inc.
IT	Information Technology

ITU	International Telecommunication Union (formerly CCITT)
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
IW	Information Warfare
JPEG	Joint Photographic Experts Group (ISO)
k,K	kilo; $1,000 = 10^3$ (bit rate; usually 'k') or $1,024 = 2^{10}$ (storage; usually 'K')
KDC	Key Distribution Center (Keberos)
KDE	K Desktop Environment
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
L6	Bell Telephone Laboratories Low-Level Linked List Language
LAN	Local Area Network
LC3	LOphtCrack v3
LDAP	Lightweight Directory Access Protocol
LFSR	Linear Feedback Shift Register
LILO	Linux Loader
LKM	Loadable Kernel Modules
LM	LAN Manager (Microsoft)
LSB	Least Significant Bit
LSOF	List Open Files (tool)

M	Mega; 1,000,000 = 10^6 (bit rate) or 1,048,576 = 2^{20} (storage)
MAC	Mandatory Access Control
MAC	Message Authentication Code
MAC	Media Access Control
MAN	Metropolitan Area Network
MB	Mega Bytes
Mb	Mega-bit
Mbps	Mega-bit per second
MBR	Master Boot Record
MBSA	Microsoft Baseline Security Analyzer
MD2	Message Digest 2
MD4	Message Digest 4
MD5	Message Digest 5
ME	Windows ME
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extensions
MINIX	MINi-unIX
MIT	Massachusetts Institute of Technology
MMC	Microsoft Management Console (Microsoft)
MO	Method of Operations

MOE	Measure Of Effectiveness
MOM	Microsoft Operations Manager
MP3	MPEG Audio Layer 3
MPEG	Motion (or Moving) Picture Experts Group (ISO)
MPLS	Multiprotocol Label Switching
MS	Microsoft
MSAU	Multistation Access Unit
MSB	Most Significant Bits
MTA	Metropolitan Transit Authority (Boston)
MTU	Maximum Transmission Unit
NAI	Network Associates, Inc.
NAPT	Network Address and Port Translation
NASL	Nessus Attack Scripting Language
NAT	Network Address Translation
NCSA	National Computer Security Association (now the ICSA)
NDA	Non-Disclosure Agreement
NDS	NetWare Directory Services (Novell)
NetBIOS	Network Basic Input/Output System (Microsoft)
NFPA	National Fire Protection Association
NFR	Network Flight Recorder

NFS	Network File System
NIC	Network Interface Card
NIDS	Network-Based Intrusion Detection System
NIPC	National Infrastructure Protection Center
NIS	Network Information Service
NIST	National Institute of Standards and Technology (U.S.)
NMAP	Network Mapping Tool
NNTP	Network News Transfer Protocol
NRM	Normal Response Mode
NSA	National Security Agency (U.S.)
NSWC	Naval Surface Warfare Center (U.S. Navy)
NT	Windows NT
NT4SP2	Windows NT 4.0 Service Pack 2
NTFS	Windows NT File System (Microsoft Windows NT/2000)
NTLM	Windows NT LAN Manager (Microsoft)
NTLM2	Windows NT LAN Manager version 2 (Microsoft)
NTP	Network Time Protocol
NVRAM	Non-Volatile Random Access Memory
NYSE	New York Stock Exchange
ODBC	Open Database Connectivity (Microsoft)

OEM	Original Equipment Manufacture
OFB	Output FeedBack Mode
OI	Order Information
ONB	Optimal Normal Base mathematics (encryption)
OOB	Out of Band
OPSEC	Operations Security
OS	Operating System
OSI	Open Systems Interconnect
OSPF	Open Shortest Path First
OSR2	Windows 95 Service Release
OU	Organization Unit
OUI	Organizationally Unique Identifiers
PAE	Port Authentication Entity
PAM	Pluggable Authentication Modules
PAN	Personal Area Network
PAP	Password Authentication Protocol
PARMS	Parallel Algebraic Recursive Multilevel Solver
PBR	Partition Boot Record
PBX	Private Branch Exchange
PC	Personal Computer

PDA	Personal Data Assistant
PDC	Primary Domain Controller (Microsoft Windows NT)
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Email
PGP	Pretty Good Privacy
PHP	PHP: Hypertext Preprocessor
PI	Payment Information
PID	Process Identifier (Unix)
PIM	Personal Information Management
PIN	Personal Identification Number.
PING	Packet InterNet Groper
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
POP	Point Of Presence
POP3	Post Office Protocol v3
POS	Point-of-Sale
POST	Power On Self Test
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSH	Push Flag (TCP)

PSYOP	Psychological Operation
PVC	Permanent Virtual Circuits
PWB	Programmers' Workbench
QA	Quality Assurance
QoS	Quality of Service
qotd	Quote-of-the-Day Service (Unix)
QS	Quality System Requirements
R&D	Research and Development
RA	Risk Analysis <i>or</i> Risk Assessment
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RARP	Reverse Address Resolution Protocol
RAS	Remote Access Server (Microsoft Windows NT/2000)
RC4	Rivest Cipher (or Ron's Code) #4
RC6	Rivest Cipher (or Ron's Code) #6
RDP	Remote Desktop Protocol (Microsoft)
RDS	Remote Data Service (Microsoft)
RF	Radio Frequency
RFC	Request for Comments (IETF)

RFP	Request for Proposal
RIAA	Recording Industry Association of America
RID	Relative Identifier
RIP	Routing Information Protocol
RO	Read-Only
ROI	Return On Investment
ROM	Read-Only Memory
ROT	Rotation Forward (Ciphers)
RPC	Remote Procedure Call
RPII	Radiological Protection Institute of Ireland
RPM	Red Hat Package Manager
RRAS	Routing and Remote Access Service
RSA	Rivest, Shamir, and Adleman
RSBAC	Rule Set Based Access Control
RST	Reset Flag (TCP)
RW	Read-Write
S/KEY	S/KEY One-Time Password System (Bellcore, now Telcordia)
SA	Security Associations
SACL	System Access Control List
SAINT	Security Administrator's Integrated Network Tool

SAM	Security Account Manager (Microsoft Windows NT/2000)
SANS	SysAdmin, Network, Security
SARA	Security Auditor's Research Assistant
SAT	Security Access Token (Microsoft)
SATAN	Security Administrator's Tool for Analyzing
SBS	Small Business Server (Microsoft) <i>or</i> Step-by-Step (SANS)
SCA	Security Configuration and Analysis (Microsoft)
SCAT	Security Configuration and Analysis Tool (Microsoft Windows 2000)
SCCS	Source Code Control System
SCM	Security Configuration Manager
SCO	Santa Cruz Organization
SCSI	Small Computer System Interface (ANSI)
SCU	System Configuration Utility (Microsoft Windows NT/2000)
SDK	Software Development Kit
SDCL	Synchronous Data Link Control
SEC	Securities and Exchange Commission (U.S.)
SEQ	Sequence Number
SESAME	Secure European System for Applications in a Multi-vendor Environment
SET	Secure Electronic Transaction (MasterCard, Visa, et al.)

SF	Syn/Fin Data Flag
SFC	System File Checker
SGI	Silicon Graphics Indy
SHA	Secure Hash Algorithm (NIST)
SHS	Secure Hash Standard (NIST)
SID	Security ID Number (Microsoft)
SIGGEN	Special Interest Group for natural language GENeration
SIP	Session Initiation Protocol
SKC	Secret Key Cryptography
SKEME	Secure Key Exchange Mechanism
SKIP	Simple Key-Management for Internet Protocols (Sun Microsystems)
SLE	Single Loss Expectancy
SLIP	Serial Line IP
SMB	Server Message Block
S/MIME	Secure Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNAPLEN	Snapshot Length
SNAT	Source Network Address Translation
SNMP	Simple Network Management Protocol

SOA	Start of Authority
SOHO	Small Office/Home Office
SOP	Standard Operating Procedure
SP	Service Pack (Microsoft)
SPF	Shortest Path First algorithm
SPI	Security Profile Inspector for Unix Networks
SPID	Service Profile Identifier
SPX	Sequenced Packet Exchange
SQL	Structured Query Language
SSH	Secure Shell
SSL	Server Side Includes
SSID	Service Set Identifier (IEEE 802.11b)
SSL	Secure Sockets Layer (Netscape)
STP	Shielded Twisted Pair
STS	Station To Station
SGID	Set Group Identifier
SUID	Set User Identifier
SUS	Software Update Services (Microsoft)
SVC	Switched Virtual Circuit
SVRX	Unix System V Revision <i>x</i>

SW	Software
SYN	Synchronize Sequence Number Flag (TCP)
Syslog	System Logger
SYSV	System V Unix
TACACS	Terminal Access Controller Access Control System
tar	Tape Archive (Unix)
TCP	Transmission Control Protocol
TFN	Tribe Flood Network
TFN2K	Tribe Flood Network 2000
TFTP	Trivial File Transfer Protocol
TGS	Ticket Granting Server (Keberos)
TGT	Ticket Granting Ticket Request (Keberos)
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOC	Time of Check
TOS	Type of Service (IP)
TOU	Time of Use
TP	Transformation Procedure
TSIG	Transaction signature (DNS)
TTL	Time To Live (IP)

TTY	Teletypewriter
UAPRSF	Urgent, Ack, Push, Reset, Syn, Finish flags (TCP)
UDP	User Datagram Protocol
UID	User Identifier (Unix)
UNC	Universal Naming Convention
UNIX	From UNICS (Uni-plexed Information and Computing System)
UPS	Uninterruptible Power Supply
URG	Urgent Data Flag (TCP)
URL	Uniform Resource Locator
US	United States
UTP	Unshielded Twisted Pair
VAX	Virtual Address extension
VBS	VisualBASIC Script (Microsoft)
VCI	Virtual Channel Identifier
VDSL	Very high bit rate Digital Subscriber Line
VGanyLAN	Virtual Grade any Local Area Network
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over IP
VPI	Virtual Path Identifier

VPN	Virtual Private Network
VxDS	Virtual Device Driver
W	Watt (unit of power)
W2K	Windows 2000
W3C	Word Wide Web Consortium
WAN	Wide Area Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy (IEEE 802.11b)
WINS	Windows Internet Name Service (Microsoft)
WLAN	Wireless Local Area Network
WM97	Word Macro Virus
WMI	Windows Management Instrumentation (WMI)
WMLscript	Wireless Markup Language (WML) Scripting Language
WPA-I	WiFi Protected Access specification I
WSH	Window Scripting Host
WTC	World Trade Center (New York City)
WTLS	Wireless Transport Layer Security
WWW	World Wide Web
XDM	X Display Manager
XDMCP	X Display Manager Control Protocol

XML	Extensible Markup Language
XOR	Exclusive OR
Y2K	Year 2000
YMMV	Your Mileage May Vary
YP	Yellow Pages (Network Information Service)