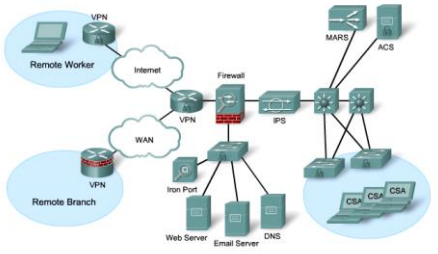
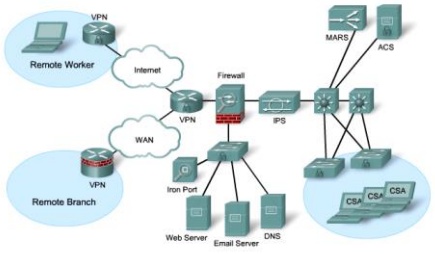
Managing a Secure Network

Secure End-to-End Network Approach



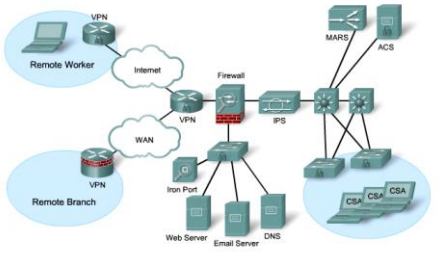
- Secure network devices with AAA, SSH, role-based CLI, syslog, SNMP, and NTP.
  - Secure services using AutoSecure and one-step lockdown.

Secure End-to-End Network Approach



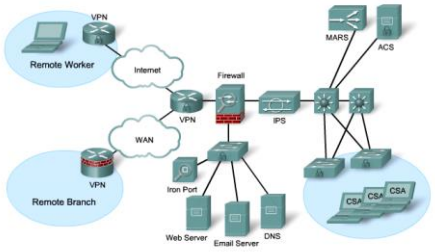
- Protect network endpoints, such as workstations and servers, against viruses, Trojan Horses, and worms with Cisco NAC, Cisco IronPort, and Cisco Security Agent.

Secure End-to-End Network Approach



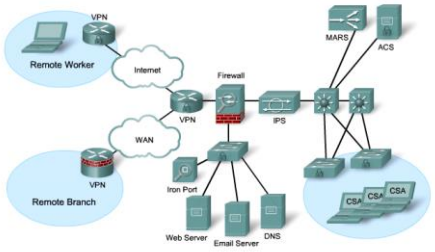
- Use Cisco IOS Firewall and accompanying ACLs to secure resources internally while protecting those resources from outside attacks.

Secure End-to-End Network Approach



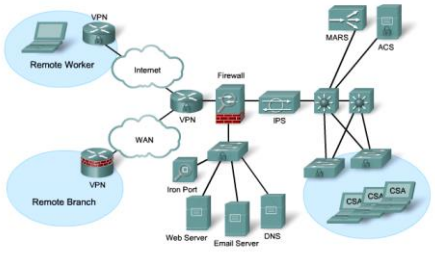
- Supplement Cisco IOS Firewall with Cisco IPS technology to evaluate traffic using an attack signature database.

Secure End-to-End Network Approach



- Protect the LAN by following Layer 2 and VLAN recommended practices and by using a variety of technologies, including BPDU guard, root guard, PortFast, and SPAN.

Secure End-to-End Network Approach



- Where are all of these security approaches documented?

Security Policies!

- Create and maintain security policies to mitigate existing as well as new kinds of attacks.
- These policies enforce a structured, informed, consistent approach to securing the network.
- Security policies must answer to the following:
  - Business needs
  - Threat Identification
  - Risk analysis
  - Security needs
  - Industry-recommended practices
  - Security operations

Security Policies Must Answer …

- Business needs:
  - What does the organization want to do with the network?
  - What are the organizational needs?
- Threat identification:
  - What are the most likely types of threats given the organization's purpose?
- Risk analysis:
  - What is the cost versus benefit analysis of implementing various security technologies?
  - How do the latest security techniques affect the network environment and what is the risk if they are not implemented?

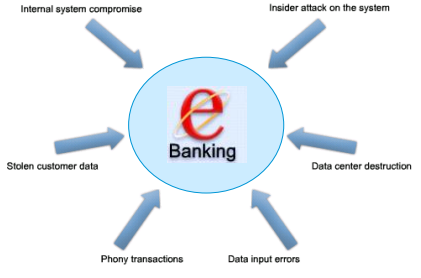
Security Policies Must Answer …

- Security needs:
  - What are the policies, standards, and guidelines needed to address business needs and risks?
- Industry-recommended practices:
  - What are the reliable, well-understood, and recommended security practices that similar organizations currently employ?
- Security operations:
  - What are the current procedures for incident response, monitoring, maintenance, and auditing of the system for compliance?

Identifying Threats and Risk Analysis

Identifying Threats

- When identifying threats, it is important to ask two questions:
  - What are the possible vulnerabilities of a system?
  - What are the consequences if system vulnerabilities are exploited?

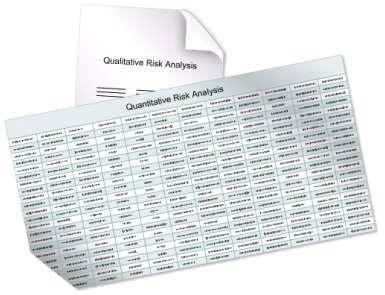


Risk Analysis

- Risk analysis is the systematic study of uncertainties and risks.
  - It identifies the risks, determines how and when those risks might arise, and estimates the impact (financial or otherwise) of adverse outcomes.
- After the threats are evaluated for severity and likelihood, the information is used in a risk analysis.

Risk Analysis

- There are two types of risk analysis in information security:



Qualitative Risk Analysis

- Various ways of conducting qualitative risk analysis exist.
- One method uses a scenario-based model.
  - This approach is best for large cities, states, and countries because it is impractical to try to list all the assets, which is the starting point for any quantitative risk analysis.
  - For example, by the time a typical national government lists all of its assets, the list would have hundreds or thousands of changes and would no longer be accurate.
- With qualitative risk analysis, research is exploratory and cannot always be graphed or proven mathematically.
  - It focuses mostly on the understanding of why risk is present and how various solutions work to resolve the risk.

Quantitative Risk Analysis

- Quantitative risk analysis uses a mathematical model that assigns a monetary figure to:
  - The value of assets
  - The cost of threats being realized
  - The cost of security implementations
- It relies on specific formulas to determine the value of the risk decision variables.

Quantitative Risk Analysis Formulas Include:

SLE = AV * EF

ALE = SLE *ARO

- **Single Loss Expectancy (SLE)**
  - Represents the expected loss from a single occurrence of the threat.
- **Asset Value (AV)**
  - This includes the cost of development / purchase price, deployment, and maintenance.
- **Exposure Factor (EF)**
  - An estimate of the degree of destruction that could occur.
- **Annualized Loss Expectancy (ALE)**
  - Addresses the cost to the organization if it does nothing to counter existing threats.
- **Annualized Rate of Occurrence (ARO)**
  - Estimates the frequency of an event and is used to calculate the ALE.

Quantitative Risk Analysis

SLE = AV * EF

Quantitative Risk Analysis Formula

- AV is the cost of an individual asset.
- EF is the loss, represented as a percentage, that a realized threat could have on an asset.
- SLE is the result of AV * EF, or the cost of a single instance of a threat.

Data entry error

- Exposure Factor is: .001 percent
- AV of the enterprise is: $1,000,000

- SLE is: $1,000,000 * .00001
- SLE is equal to: $ 10

Quantitative Risk Analysis

SLE = AV * EF

Quantitative Risk Analysis Formula

- AV is the cost of an individual asset.
- EF is the loss, represented as a percentage, that a realized threat could have on an asset.
- SLE is the result of AV * EF, or the cost of a single instance of a threat.

Flood threat

- Exposure Factor is: 60 percent
- AV of the enterprise is: $10,000,000

- SLE is: $10,000,000 * .60
- SLE is equal to: $ 6,000,000

Quantitative Risk Analysis

ALE = SLE *ARO

Annualized Loss Expectancy — Annualized Rate of Occurrence

Quantitative Risk Analysis Formula

- ARO represents the estimated frequency that a threat is expected to occur.
- ALE is the expected financial loss that an individual threat will cause an organization. It is a monetary value derived from the formula SLE * ARO.
- ALE is the number used to justify the least-cost security measures.

Data entry error

- SLE is: $ 10
- ARO is: 125,000

- ALE is: $10 * 125,000
- ALE is equal to: $ 1,250,000

Quantitative Risk Analysis

ALE = SLE *ARO

Annualized Loss Expectancy **Annualized Rate of Occurrence**

Quantitative Risk Analysis Formula

- ARO represents the estimated frequency that a threat is expected to occur.
- ALE is the expected financial loss that an individual threat will cause an organization. It is a monetary value derived from the formula SLE * ARO.
- ALE is the number used to justify the least-cost security measures.

Flood threat

- SLE is: $ 6,000,000
- ARO is: .01

- ALE is: $ 6,000,000 * .01
- ALE is equal to: $ 60,000

Quantitative Risk Analysis

- It is necessary to perform a quantitative risk analysis for all threats identified during the threat identification process.
- Then prioritize the threats and address the most serious first.
  - This prioritization enables management to focus resources where they do the most good.

Risk Management and Risk Avoidance

Risk Management and Risk Avoidance

- When the threats are identified and the risks are assessed, a protection strategy must be deployed to protect against the risks.
- There are two very different methods to handle risks:
  - Risk management
  - Risk avoidance

Risk Management

- Method deploys protection mechanisms to reduce risks to acceptable levels.
- Risk management is perhaps the most basic and the most difficult aspect of building secure systems, because it requires a good knowledge of risks, risk environments, and mitigation methods.

Risk Avoidance

- This method eliminates risk by avoiding the threats altogether, which is usually not an option in the commercial world, where controlled or managed risk = profits.

Cisco SecureX Architecture

SecureX Architecture

- This architecture is designed to provide effective security for any user, using any device, from any location, and at any time.
- This new security architecture uses a high-level policy language that can describe the full context of a situation, including who, what, where, when and how.
- With highly distributed security policy enforcement, security is pushed closer to where the end user is working, anywhere on the planet. This architecture is comprised of five major components:
  - Scanning engines
  - Delivery mechanisms
  - Security Intelligence Operations (SIO)
  - Policy management consoles
  - Next-generation endpoints

Context-Aware

- A context-aware scanning element does more than just examine packets on the wire. It looks at external information to understand the full context of the situation: the who, what, where, when and how of security.
- These scanning elements are available as stand-alone appliances, software modules running in a router, or an image in the cloud. They are managed from a central policy console that uses a high level to build context aware policies.
- A context-aware policy uses a simplified descriptive business language to define security policies based on five parameters:
  - The person's identity
  - The application in use
  - The type of device being used for access
  - The location
  - The time of access

Cisco Security Intelligence Operations (SIO)

- Delivers real-time global threat intelligence.
- World's largest cloud-based security ecosystem, using almost a million live data feeds from deployed Cisco email, web, firewall, and IPS solutions. Cisco SIO weighs and processes the data, automatically categorizing threats and creating rules using more than 200 parameters. Rules are dynamically delivered to deployed Cisco security devices every three to five minutes.

SecureX Solutions

- Secure Edge and Branch
  - The goal of the Cisco secure edge and branch is to deploy devices and systems to detect and block attacks and exploits, and prevent intruder access. With firewall and intrusion prevention in standalone and integrated deployment options, organizations can avoid attacks and meet compliance requirements.
- Secure Email and Web
  - Cisco secure email and web solutions reduce costly downtime associated with email-based spam, viruses, and web threats, and are available in a variety of form factors, including on-premise appliances, cloud services, and hybrid security deployments with centralized management.
- Secure Access
  - Secure access technologies are put in place to enforce network security policies, secure user and host access controls, and control network access based on dynamic conditions.
- Secure Mobility
  - Cisco secure mobility solutions promote highly secure mobile connectivity with VPN, wireless security, and remote workforce security solutions that extend network access safely and easily to a wide range of users and devices.
- Secure Data Center and Virtualization
  - Cisco secure data center and virtualization solutions protect high-value data and data center resources with threat defense, secure virtualization, segmentation and policy control.

cisco

Operations Security

Operations Security

- Operations security is concerned with the day-to-day practices necessary to first deploy and later maintain a secure system.
- It starts with the planning and implementation process of a network.
  - During these phases, the operations team proactively analyzes designs, identifies risks and vulnerabilities, and makes the necessary adaptations.
  - After a network is set up, the actual operational tasks begin, including the continual day-to-day maintenance of the environment.

Operations Security – Core Principles

- Separation of duties
- Rotation of duties
- Trusted recovery
- Change and configuration controls

Separation of Duties

- Is the most difficult and sometimes the most costly control to achieve.
- SoD states that no single individual has control over two or more phases of a transaction or operation.
  - Instead, responsibilities are assigned in a way that incorporates checks and balances.
  - This makes a deliberate fraud more difficult to perpetrate because it requires a collusion of two or more individuals or parties.

Rotation of Duties

- Individuals are given a specific assignment for a certain amount of time before moving to a new assignment.
  - It is important that individuals have the training necessary.
- Peer review is built into the practice of rotation of duties.
  - For example, when 5 people do one job in the course of the week, each person is effectively reviewing the work of the others.
- Rotation of duties also prevents boredom and gives individuals a greater breadth of exposure to the entire network operation.
  - This creates a strong and flexible operations department because everyone is capable of doing multiple jobs.

Trusted Recovery

- Systems eventually fail!
  - Therefore a process for recovery must be established.
  - Back up data on a regular basis.
- Backing up data is standard practice in most IT departments.
- Being prepared for system failure is also an important part of operations security:
  - Back up critical data on a regular basis.
  - Evaluate who has access to the files to back them up and what kind of access they have.
  - Secure the backup media.

Configuration and Change Control

- Ensures that standardized methods and procedures are used to efficiently handle all changes.
- It should address three major components:
  - The processes in place to minimize system and network disruption
  - Backups and reversing changes that go badly
  - Guidance on the economic utilization of resources and time
- A few suggestions are recommended to accomplish configuration changes in an effective and safe manner:
  - Ensure that the change is implemented in an orderly manner with formalized testing.
  - Ensure that the end users are aware of the coming change when necessary.
  - Analyze the effects of the change after it is implemented.

5 Steps for Configuration and Change Control

- Step 1. Apply to introduce the change.
- Step 2. Catalog the proposed change.
- Step 3. Schedule the change.
- Step 4. Implement the change.
- Step 5. Report the change to the relevant parties.

Network Security Testing

- Network security testing is testing that is performed on a network to ensure all security implementations are operating as expected.
  - Testing is typically conducted during the implementation and operational stages.
- During the implementation stage, security testing is conducted on specific parts of the security system.
- After a network is fully integrated and operational, a Security Test and Evaluation (ST&E) is performed.
  - ST&E is an examination or analysis of the protective measures that are placed on an operational network.
- Tests should be repeated periodically and whenever a change is made to the system.
  - Test more frequently on critical information or hosts that are exposed to constant threat.

Network Security Testing

- Many tests can be conducted to assess the operational status of the system:
  - Network scanning
  - Vulnerability scanning
  - Password cracking
  - Log review
  - Integrity checkers
  - Virus detection
  - War dialing
  - War driving (802.11 or wireless LAN testing)
  - Penetration testing

Network Security Testing Tools

Continuity Planning

Continuity Planning

- Business continuity planning addresses the continuing operations of an organization in the event of a disaster or prolonged service interruption that affects the mission of the organization.
- These plans address an emergency response phase, a recovery phase, and a return to normal operation phase.

Continuity Planning

- The first step is identifying the possible types of disasters and disruptions.
- A good disaster recovery plan takes into account the magnitude of the disruption, recognizing that there are differences between catastrophes, disasters, and minor incidents.

Large Enterprise Requirements

- Large organizations might require a redundant facility if some catastrophic event results in facility destruction.
- Hot sites:
  - A completely redundant facility with almost identical equipment.
- Warm site:
  - Physically redundant facilities, but software and data are not stored and updated on the equipment.
  - A disaster recovery team is required to physically go to the redundant facility and get it operational.
  - Depending on how much software and data is involved, it can take days before operations are ready to resume.
- Cold site:
  - An empty datacenter with racks, power, WAN links, and heating, ventilation, and air conditioning (HVAC) already present, but no equipment.

Secure Copy

- The primary goal of disaster recovery is to restore the network to a fully functional state. Two of the most critical components of a functional network are the router configuration and the router image files.
- Every disaster recovery plan should include backup and retrieval of these files. Because an organization's network configuration includes private or proprietary information, these files must be copied in a secure manner.
- The secure copy (SCP) feature provides a secure and authenticated method for copying router configuration or router image files.

SCP Server Configuration

- Because SCP relies on SSH for secure transport, before enabling SCP, you must correctly configure SSH, and the router must have an RSA key pair, To configure the router for server-side SCP, perform these steps:
  - Step 1. Enable AAA with the **aaa new-model** global configuration command.
  - Step 2. Define a named list of authentication methods, with the **aaa authentication login {default |***list-name***}** *method1* **[***method2...***]** command.
  - Step 3. Configure command authorization, use the **aaa authorization {network | exec | commands** *level***} {default |** *list-name***}** *method1...***[***method4***]** command.
  - Step 4. Configure a username and password to use for local authentication with the **username** *name* **[privilege** *level***] {password** *encryption-type password***}** command. This step is optional if using network-based authentication such as TACACS+ or RADIUS.
  - Step 5. Enable SCP server-side functionality with the **ip scp server enable** command.

SCP Server Sample Config

```
R1(config)# username scpADMIN privilege 15 password 0 scpPa55W04D
R1(config)# ip domain-name scp.cisco.com
R1(config)# crypto key generate rsa general-keys modulus 1024
R1(config)# aaa new-model
R1(config)# aaa authentication login default local
R1(config)# aaa authorization exec default local
R1(config)# ip scp server enable
R1(config)# exit
```

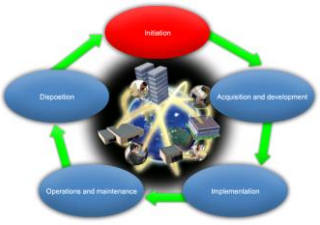

CISCO

SDLC

System Development Life Cycle (SDLC)

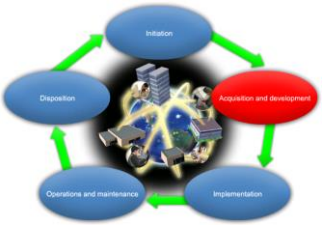
- Five phases of the SDLC:
  - Initiation
  - Acquisition and development
  - Implementation
  - Operation and maintenance
  - Disposition
- When using the SDLC to design a network, each phase should include a minimum set of security requirements.
  - This results in less expensive and more effective security as compared to adding security to an operational system after the fact.

Initiation Phase



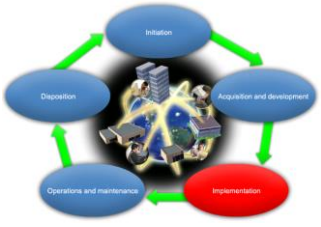
- Consists of two tasks:
  - Security categorization:
    - Define three levels (low, moderate, and high) of potential impact on organizations or individuals if there is a breach of security.
  - Preliminary risk assessment:
    - Initial description of the basic security needs of the system that defines the threat environment in which the system operates.

Acquisition and Development Phase



- Consists of the following tasks:
  - Risk assessment
  - Security functional requirements
  - Security assurance requirements
  - Security cost considerations and reporting
  - Security planning
  - Security control development
  - Developmental security test and evaluation

Implementation Phase

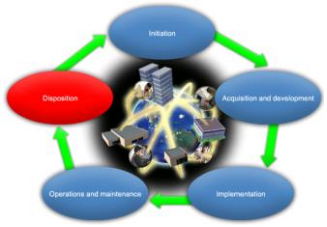


- Consists of the following tasks:
  - Inspection and acceptance
  - System integration
  - Security certification

Operations and Maintenance Phase

- Consists of two tasks:
  - Configuration management and control
  - Continuous monitoring

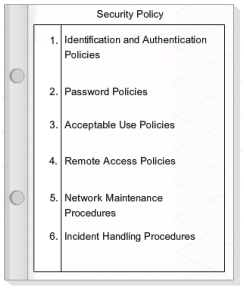
Disposition Phase



- Consists of the following tasks:
  - Information preservation
  - Media sanitization
  - Hardware and software disposal

Security Policy

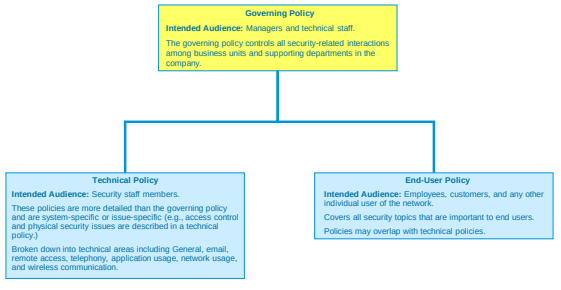
Security Policy



- An organization's set of security objectives which defines the rules of behavior for users and administrators, and system requirements.
  - It is a living document, constantly evolving based on changes in technology, business, and employee requirements.
  - Demonstrates an organization's commitment to security.
  - Sets the rules for expected behavior.
  - Ensures consistency in system operations, software and hardware acquisition and use, and maintenance.
  - Defines the legal consequences of violations.
  - Gives security staff the backing of management.

Structure of a Security Policy

- Policy documents are often broken into a hierarchical structure:



Standard Documents

- One of the most important security principles is consistency and therefore it is necessary for organizations to establish standards.
- Each organization develops standards to support its unique operating environment.
- Device configuration standards are defined in the technical section of an organization's security policy.

Guideline Documents

- Guidelines provide a list of suggestions on how to do things better.
  - They are similar to standards, but are more flexible and are not usually mandatory.
  - Guidelines can be used to define how standards are developed and to guarantee adherence to general security policies.
- A number of guidelines are widely available:
  - National Institute of Standards and Technology (NIST) Computer Security Resource Center
  - National Security Agency (NSA) Security Configuration Guides
  - The Common Criteria Standard

Procedures Documents

- Procedure documents are longer and more detailed than standards and guidelines.
- Procedure documents include implementation details, usually with step-by-step instructions and graphics.
- Procedure documents are extremely important for large organizations to have the consistency of deployment that is necessary for a secure environment.

Roles and Responsibilities

- Chief Executive Officer (CEO)
  - Is ultimately responsible for the success of an organization.
  - All executive positions report to the CEO.
- Chief Technology Officer (CTO)
  - Identifies and evaluates new technologies and drives new technology development to meet organization objectives.
  - Maintains and enhances the enterprise systems, while providing direction in all technology-related to support operations.
- Chief Information Officer (CIO)
  - Responsible for the information technology and computer systems that support enterprise goals, including successful deployment of new technologies and work processes.
  - Small- to medium-sized organizations typically combine the responsibilities of CTO and CIO into a single position.
  - When an organization has both a CTO and CIO, the CIO is generally responsible for processes and practices supporting the flow of information, and the CTO is responsible for technology infrastructure.
- Chief Security Officer (CSO)
  - Develops, implements, and manages the organization's security strategy, programs, and processes associated with all aspects of business operation, including intellectual property.
  - A major aspect of this position is to limit exposure to liability in all areas of financial, physical, and personal risk.
- Chief Information Security Officer (CISO)
  - Similar to the CSO, except that this position has a specific focus on IT security.
  - CISO must develop and implement the security policy, either as the primary author or management of authorship. In either case, the CISO is responsible and accountable for security policy content.

Security Awareness and Training

- Where is the weakest link in any network infrastructure?
  - The User!
- To help ensure the enforcement of the security policy, a security awareness program must be put in place.

Security Awareness Program

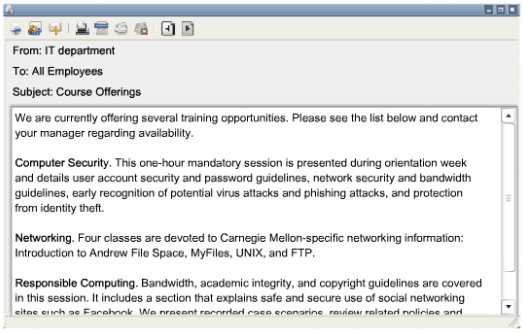
- Specifics:
  - It informs users of their IT security responsibilities.
  - It explains all IT security policies and procedures for using the IT systems and data within a company.
  - It helps protect the organization from loss of intellectual capital, critical data, and even physical equipment.
  - It must also detail the sanctions that the organization imposes for noncompliance.
  - It should be part of all new hire orientation.
- A security awareness program usually has two major components:
  - Awareness campaigns
  - Training and education

Awareness Campaign

Awareness Campaign

- "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information... Awareness relies on reaching broad audiences with attractive packaging techniques." (NIST Special Publication 800-16)
- There are several methods of increasing security awareness:
  - Posters, newsletter articles, and bulletins
  - Lectures, videos
  - Awards for good security practices
  - Reminders, such as login banners, mouse pads, coffee cups, and notepads, etc.

Training and Education



Training and Education

- Awareness campaigns focus an individual's attention on security issues.
- Training teaches skills that allow a person to perform a specific task!
  - The skills learned builds upon the information in security awareness campaigns.
- Following a security awareness campaign with training targeted to specific audiences helps cement the information and skills imparted.
- An effective security training course requires proper planning, implementation, maintenance, and periodic evaluation.

Laws

- A big reason for setting security policies and implementing awareness programs is compliance with the law.
  - You must be familiar with the laws and codes of ethics that are binding on Information Systems Security (INFOSEC) professionals.
- Most countries have three types of laws:
  - Criminal law:
    - Concerned with crimes, and its penalties usually involve fines or imprisonment, or both.
  - Civil law (also called tort):
    - Focuses on correcting situations in which entities have been harmed and an economic award can help.
    - Imprisonment is not possible in civil law.
    - For example: suing for patent infringement.
  - Administrative law:
    - Involves government agencies enforcing regulations.
    - For example: a company might owe its employees vacation pay.

Ethics

- Ethics is a standard that is higher than the law.
- It is a set of moral principles that govern civil behavior and are often referred to as codes of ethics.
- Ethical principles are often the foundation of many of the laws currently in place.
- Individuals that violate the code of ethics can face consequences such as loss of certification, loss of employment, and even prosecution by criminal or civil court.

Ethics

- The information security profession has a number of formalized codes:
  - International Information Systems Security Certification Consortium, Inc (ISC)2 Code of Ethics
  - Computer Ethics Institute (CEI)
  - Internet Activities Board (IAB)
  - Generally Accepted System Security Principles (GASSP)

(ISC)2 Code of Ethics

- Code of Ethics Preamble
  - "Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior. Therefore, strict adherence to this Code is a condition of certification."
- Code of Ethics Canons
  - Protect society, the commonwealth, and the infrastructure.
  - Act honorably, honestly, justly, responsibly, and legally.
  - Provide diligent and competent service to principals.
  - Advance and protect the profession.