Lesson 13 – Security Management Practices, Processes and Policies

Network vulnerabilities review

- Highly distributed
  - Too many devices in too many locations (even in a small company)
- Difficult to monitor
  - Too many entry points (both wired and wireless).
  - Not clear boundary
- Many services
  - ftp, telnet, http, smtp, etc.
- Many threats
  - All kind of malware (virus, trojans, rootkits, etc.)
  - Hackers continually inventing new threats

Network attacks 1/2 review

- Social engineering
  - Tricking an authorized user in the network to gain access
- Impersonation
  - Posing as an authorized user to the network
- Data driven
  - Malware
- Denial of service
  - Prevent machine or networks from being used

Network attacks 2/2 review

- Exploits
  - Exploiting a defect or hole in a piece of software or OS
- Infrastructure
  - Exploits infrastructure or protocol bugs or features
- Transitive trust
  - Exploit machine-machine or network-network trust
- Magic
  - New type of attacks (which does not exists today in practice or theory)

Security management

- An organization protects its assets by implementing security management practices
- The security management practices include
  - Identification of
    - Assets
    - Vulnerabilities
    - Threats
    - Risks
    - countermeasures
  - Security controls
  - Information classification
  - Roles and responsibilities

Securing management process

- An organization achieves its desired level of security by:
  - Defining a security policy
  - Implementing the security policy
  - Monitoring for compliance with the security policy
  - Obtaining independent confirmation that the security policy is sufficient and has been properly implemented

Security compliance

- Security compliance means to act according to accepted policies, regulations, standards, and guidelines.
- Security compliance must conforms to
  - documented security policy,
  - industry or government regulations and standards,
  - and all other details of its security program.

Assets

- Asset is a resource, process, product, or system that has value to the organization
- The level of protection depends on
  - the value of the asset,
  - the threats that exist against the asset,
  - how vulnerable the asset is should the threat be exploited.
- Type of assets
  - Tangible
    - Examples: computer hardware, computer data, licensed products, and software applications
  - Intangible.
    - Examples: data privacy and the organization’s public image

Vulnerability

- A vulnerability is a weakness that threatens the CIA model for an asset
- Vulnerabilities are not only deficiencies of software or inappropriate implementation of technical measures
- Examples
    - No virus detection
    - Untrained employees
    - incorrect procedures
    - Missing documentation

Threat

- A threat is any activity that can have an adverse or undesirable effect on an organizational asset
- Threats exploit vulnerabilities
- Examples:
  - Hardware failure,
  - fire,
  - hackers,
  - espionage,
  - malicious code,
  - sabotage,
  - vandalism,
  - weather

Risk

- A risk is the possibility of a threat exploiting a vulnerability
- Risks can be mitigated (but at a cost)
- Risks can never be completely eliminated
- Important to determine
  - How much risk your organization is willing to accept for each asset

Countermeasure

- Countermeasures are security safeguards that mitigate the risk of threats
- Examples
  - Reveal as little information about the system as possible
  - Limit access
  - Disable unnecessary services on all computers
  - Use strong authentication to access internal services
  - Educate users and management
  - Educate users and management
  - Continually monitor and fine-tune the security infrastructure

Security controls

- Tallow or deny the use of a resource, such as a computer, a printer or program, to an individual or a process
    - Similar to authorization but broader
- There are three types of security controls:
    - Physical controls
    - Technical controls
    - Administrative controls

Physical controls

- Protect the security of the physical environment
- Examples
  - Guards
  - Video cameras
  - Locks
  - Alarm systems
  - Uninterruptible power supply

Technical controls

- Use computer hardware and software to implement access control
- Examples
  - Object authority
  - Data authority
  - Encryption

Administrative controls

- Security policy and security procedures implemented as a part of the security program.
- Examples
  - Security policy
  - Security guidelines
  - Security procedures
  - Security training

Information classification

- Information classification assists in assigning a value to data and establishing the correct level of data protection
- The value of the data asset helps determine the necessary level of data protection
- A single value and protection standard cannot be applied across all data
- Common levels of data classification are
  - Confidential
  - Private
  - Sensitive
  - Public

Roles and responsibilities

- Common security-related roles are:
  - Management
  - Security officer
  - Data Owner
  - Data Custodian
  - Technical security specialist
  - System security administrator
  - User
  - Security auditor

Note that organizations may choose to use different role names, and several roles may be assigned to the same individual

Management role

- Senior management is typically the organization’s asset and data owner for business applications
- Senior management should demonstrate its commitment to the organization’s security program by releasing management communication that introduces and supports the security policy

Security officer role

- The security officer develops the corporate security policy
- The security officer ensures that the information system is implemented and run in accordance with the security policy
- Evaluates vulnerabilities and determines enhanced security measures
- Ensures the enforcement of the corporate security policy

Data owner role

- Data owners are typically members of the organization's senior management and can be held personally and financially liable for their negligence in protecting assets and data
- The general responsibilities of a data owner are to decide on the classification level of the data, determine how to protect the data, and define who can access the data
- The data owner usually delegates the daily data owner responsibility for assets and data to a data custodian

Custodian role

- A data custodian is someone who is entrusted with guarding and protecting data and assets
- The custodian is responsible for the regular maintenance and protection of the organization’s assets and data
- This daily responsibility usually includes:
  - Keeping systems operational
  - Protecting system data
  - Validating the confidentiality, availability, and integrity of systems and data
  - Performing system and data backups and restores

Technical security specialist role

- The technical security specialist is usually a member of the IT department
- This person is trained to work with the data owners and data custodians to make sure that the security program is reasonable and that any exposures are acceptable to the data owners

System security administrator role

- Responsible for implementing and maintaining the system security controls required by the security policy
- This includes activities such as:
  - Creating, updating, and deleting user profiles
  - Assigning new users to group profiles
  - Setting an initial password for new users
  - Updating and revoking user privileges as required
- Reviews the security audit logs and monitors the overall security status of the system
  - In case of abnormal activity a security incident report should be open and an investigation should start

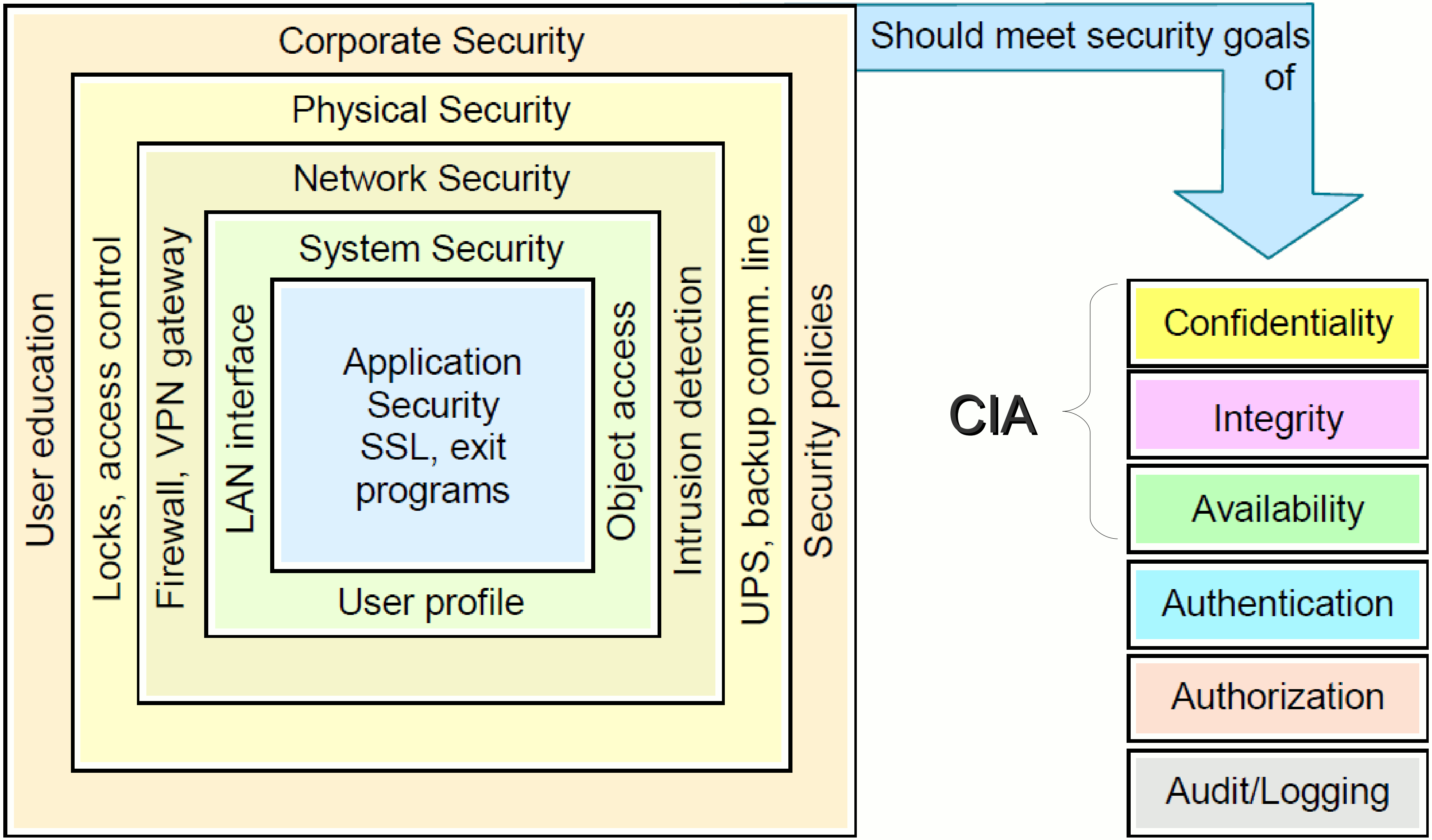
User role

- A user is anyone who uses the organization’s assets and data to fulfill their responsibilities in the organization
- Users must be given the proper and limited access rights to the assets and data to fulfill their responsibilities
- User are responsible for following the organization’s security policy, standards, and procedures

Security auditor role

- A security auditor can be an internal organization auditor or a member of an external auditor organization
- Performs regular and repeated reviews of the organization’s security procedures and control to make sure that they meet the requirements of the security policy, processes, procedures, and guidelines
- A security audit is usually required to satisfy industry, government, or owner responsibilities

Security implementation layers



Application security layer

- Applies to business and system applications
- Include system applications, for example
  - Hypertext Transfer Protocol (HTTP) server
  - Secure Sockets Layer (SSL)
  - Other system services
- Examples
  - Application authentication
  - Application enforces authorization

System security Layer

- Operating System security
- Examples
    - User logon (authentication)
    - Files access control lists (authorization)

Network security layer

- Network security includes controls such as firewalls, virtual private networks (VPNs), and gateways

Physical security layer

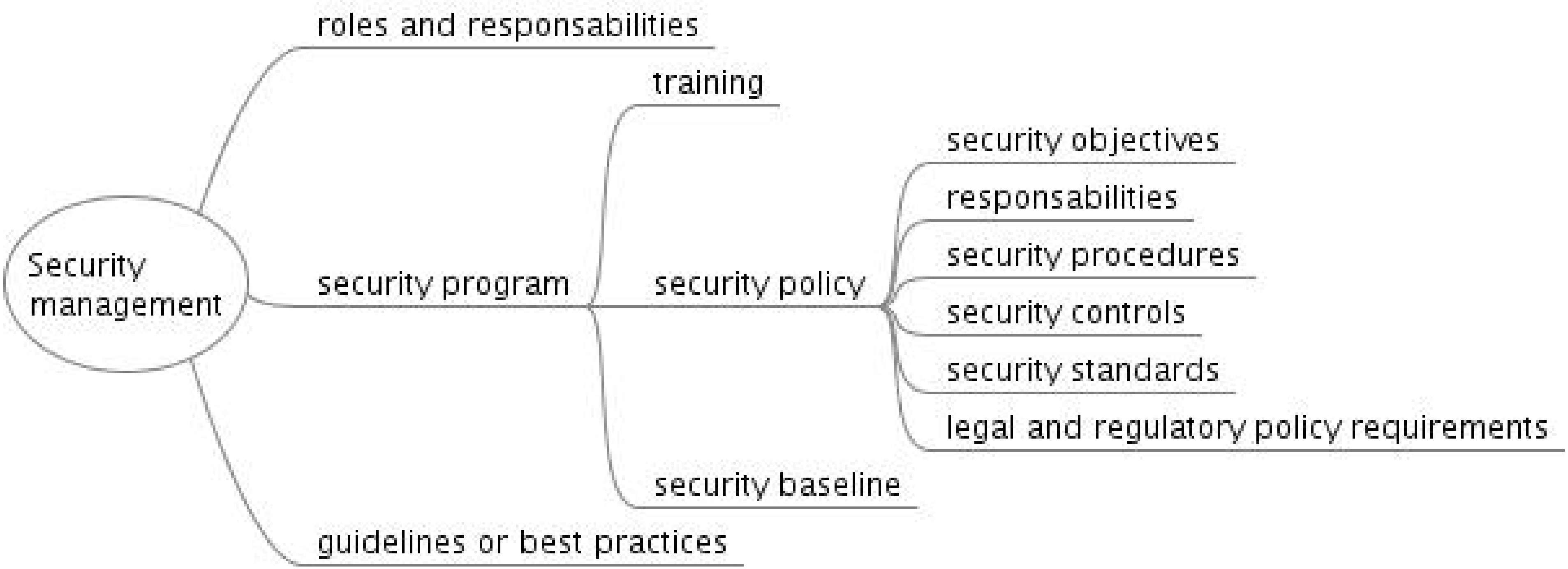
- Physical security includes protecting assets such as the system, devices, and backup media from accidental or deliberate damage
- Examples
  - Access controls
  - Uninterruptible power supplies
  - Redundant capabilities such as backup communications lines

Corporate security layer

- Corporate security is responsible for all aspects of an organization’s security program
- Examples
  - Organization’s security policies
  - Security training
  - Planning for and managing disaster recovery

Security management

Organizations must manage security using multiple means



Security program

- The security program should include all areas that might be part of the organization’s security
- The security program includes
  - Procedures,
  - Documents,
  - Standards
  - Compliance enforcement measures
  - Devices
  - Software
  - Training

Security policy

- A formal set of rules regarding an organization’s technology and information assets, which users must follow
- A security policy combines the policies required by senior management with any regulatory policy requirements
  - Senior management policies identify security objectives, responsibilities of management and users, and laws
  - Identify regulations that governs the organization, legal issues, liability issues, and any general requirements and security controls.

Baselines

- Baselines establish the minimum level of required security for an organization
- Examples
  - Every laptop must have installed YYY anti-virus
  - Every laptop must have a user and password
  - Passwords must be eight characters long

Standards

- Standards are rules that might indicate what an organization’s employees should and should not do, how specific hardware can be used, and what are acceptable configurations for software products or applications
- Standards are mandatory requirements
- Standards further define, support, and enforce the security policy

Guidelines

- Guidelines (or best practices) are recommendations for organizations that need help getting started with their security program

Procedures

- Procedures are the documented step-by-step instructions about how to implement the directives in the security policy and security standards
- They are usually documented as desk procedures for security officers, system operators, and system administrators
- Procedures help to make sure that, regardless of who makes a change, if the procedure is followed, then the change is performed in a standardized, accepted, and repeatable manner

The End