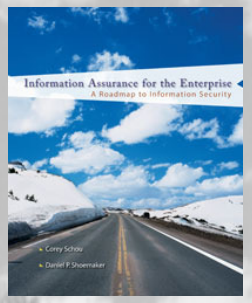

Chapter 7

Personnel Security

Objectives

At the end of this unit, you will be able to:

- Ensure secure behavior
- Articulate personnel controls
- State the role of human resources in ensuring personnel security
- Define contractor control

Predictability is key

- Predictability Information assurance process involves
  1. Technology
  2. Processes
  3. People
- Any of these can cause a security breakdown, however:
  - Technology is predictable
    - Well-designed processes are consistent
  - Human behavior is hard to predict and control
- Disastrous effects of employee-based actions:
    - Organizations should have mechanisms in place to ensure secure employee behavior

First Steps, First

- Origin of threats
  - Outsiders –commonly recognized
  - Insiders – fraud, misuse, theft, and human error
    - More serious threat than outsiders
- Access and security control
  - Establishing secure space defined by perimeters
  - Established to ensure the confidentiality, integrity and availability of the information assets
    - Perimeter control

First Steps, First

- Ensuring continuous practice
  - Reliable and repeatable performance of approved security requirements
  - Requirement for disciplined practice implies that attention must be paid to motivation
  - Motivation requires awareness

Ensuring Personnel Security Behavior

- Three categories of personnel security behavior
  - Routine activities
    - Individual actions to secure the space that they control from any threats
  - Operational functions
    - Activities that are performed to ensure the security of the entire system during day-to-day operation
  - Management responsibilities
    - Actions which guarantee that the information assurance and security strategy is implemented properly

Documenting Security Procedures

- Documentation ensures that security activities are recorded and properly understood
  - Personnel security manual – communicates procedures
    - Specifies actions required for ensuring personnel security
    - Serves as a:
      - Basis for feedback
      - Mechanism to build and reinforce awareness of what has to be done
  - Documents corrective actions
  - Members must be aware of recommended practices that apply

Documenting Security Procedures

- At a minimum every documented procedure should specify the:
  - Required steps to be taken and by whom
  - Expected outcomes and some way to determine that they have been achieved
  - Interfaces with other security procedures

Assignment of Individual Responsibility

- Selected managers should be responsible for ensuring that assigned information duties are carried out by:
  - Assigning each worker individual accountability
  - Regular monitoring of routine information assurance and security operations
- Rule of thumb in assigning of responsibilities:
  - Specific accountability for security duties must be delegated in writing to each individual involved
  - Every designated worker must be trained and knowledgeable in all aspects used to perform the duties
    - Should be kept up to date on all related practices used

Users must:

- Be aware of acceptable behavior
- Understand the consequences of noncompliance
  - Consequences should be spelled out and enforced through a set of behavior rules
    - In writing
    - Clearly delineates the responsibilities and expectations for each individual
    - Everyone should understand the rules before they are allowed access
    - Have to be rigorous to ensure security, while giving enough flexibility to perform the jobs properly

Rules of Behavior

- Rules of behavior should define the organizationally sanctioned response to such concerns as:
  - Individual accountability
  - Assignment and limitation of system privileges
  - Networking and Internet use

Role of Awareness and Training

- Training is an effective countermeasure
  - Ensures that users are well versed in system's technical and procedural controls
    - Scheduled, periodic refresher training
    - Specialized training for members responsible for maintaining functions
    - Level of depth and intensity of training linked to potential risk and degree of associated harm
  - Should support the users and help them understand how to obtain help when security incidents occur

Role of Awareness and Training

- Goal of an awareness or training program
  - Ensure acceptable knowledge level about information assurance practice for all who work in secured space
  - Most effective when presented in logical modules or learning stages
    - Cost effective training in the form of interactive computer-based (CBT) training sessions
    - Modern training philosophy leans toward “just-in-time” and “blended” learning approaches

Planning: Ensuring Reliable Control over Personnel

- Information assurance success rests on the ability to guarantee a minimum level of formal personnel control
  - Control defined by a plan
  - Decision makers evaluate information and prepare strategies to mitigate them
  - Aim to:
    - Ensure that adverse personnel actions are anticipated
    - Reliably control by establishing a clearly recognized and understood safeguard

Control Principles

Three principles:

1. Individual accountability
   - Everyone should be held responsible for his or her actions
2. Least privilege
   - Restricting a user's access to the minimum level of access needed to perform his or her job
3. Separation of duties
   - Distribution of the actions to perform a single function among a number of individuals

Personnel Screening

- Assures that individuals with access to protected information are not security risks
- Employed where the information is considered sensitive enough that controls cannot assure security
- Should be done proportionate to the potential risk and magnitude of harm that might originate from a requirement violation

Planning for Personnel Assurance

- Most effective when selected controls and related procedures embedded into day-to-day operations
  - Achieved by making personnel security planning part of overall strategic planning
  - Two areas that personnel security plans must address:
    - Define procedures required to ensure security through staffing
    - Provide procedures to ensure that access for each type of employee is always monitored and controlled

Security and the Human Resources Function

- Control points for employee hiring process can be divided into four stages:

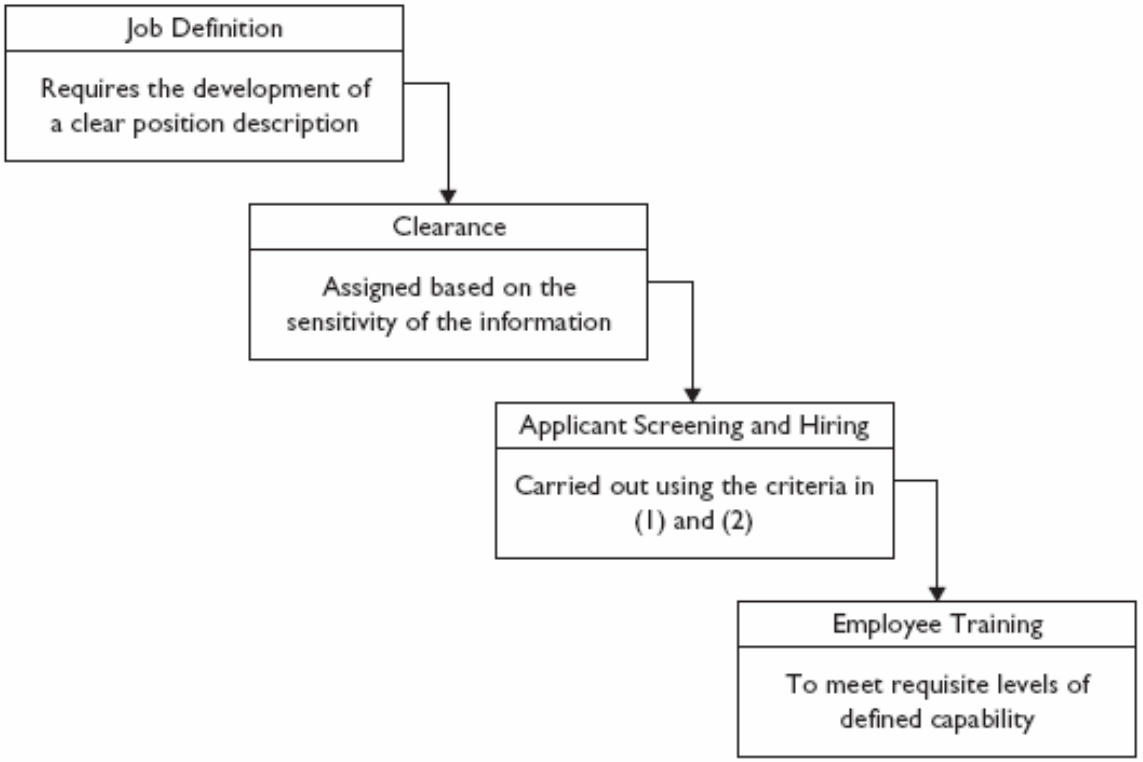

Figure 7-1 Security stages in the employee hiring process

Job Definition

- Embed a set of information assurance and security requirements into the standard task requirements for each position
  - Decide where each position fits in organizational hierarchy
  - Spell out each position's degree of authority and responsibility
  - Determine each position's required access rights and level of trust
  - Document type of sensitivity and associated level of access required for the work

Assignment of Required Trust

- Specification of trust requirements
  - Based on the level of trust and sensitivity requirements
  - Access to different information assets implies different types of restrictions
- Information assurance and security controls should be assigned to regulate each position
  - Based on the potential risks and damage likely to ensue if there were a information assurance breakdown associated with that role

Background Screening and Hiring

- Confirms that prospective employee fits the information assurance criteria for a given position
- Factors that should be examined:
  - History
    - Work
    - Credit
    - Educational
  - Interview or psychographic data
  - Any public evidence of addictive behavior

Employee Awareness Training and Education

- Provide information assurance and security awareness training, and even formal education
  - Communicate an understanding of the procedures required of that position

United States Government Training Standards

- Public Law 100-235
  - "Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency."
- FISMA – The E-Government Act (Public Law 107-347)
  - Recognized the importance of information security to the economic and national security interests of the United States
  - Motivated the establishment of the National Institute for Standards and Technology (NIST) and the Committee for National Security Systems (CNSS)

United States Government Training Standards

- NIST Standard Examples
  - SP 500-172: Computer Security Training Guidelines
  - SP 800-16: Information Technology Security Training Requirements
  - SP 800-53: Recommended Security Controls for Federal Information Systems
- CNSS Training Standards
  - Information Security Professionals (4011)
  - Senior Systems Manager
  - System Administrators
  - Information System Security Officers (4014)
  - System Certifiers
  - Risk Analyst System Security Engineer (4016)

United States Government Training Standards

- DHS and NSA Academic Certification
  - To certify that the curricula of academic institutions meet required standards
- National Information Assurance Education and Training Program (NIETP)
  - Encourages and recognizes universities through its Centers of Academic Excellence in IA Education (CAE) program

Private Sector Security Certification Standards

- No recognized common body of knowledge to use as a point of reference in the development and refinement of accepted practices
  - Range of organizations has sprung up to promote their own view of proper practice
    - Commercial organizations specializing in training for particular technological applications
    - Non-profit organizations, whose certifications are broadly based, such as the:
      - Information Systems Audit and Control Association (ISACA)
      - International Information Systems Security Certification Consortium [(ISC)2]

Assigning Value to Certification

- Certification is the result of a process
  - Some decision criteria that would help provide an accurate picture of the value of a certification are:
    - How long has the certification been in existence?
    - Does the certifying organization's process conform to established standards?
    - Is the organization ISO/IEC 17024 certified?
    - How many people hold the certification?
    - How widely respected is the certification?
    - Does the certificate span industry boundaries?
    - What is the probability that 5 or 10 years from now, the certificate will still be useful?
    - Does the certification span geographic boundaries?

Controlling Access of Employees and Contractors to Restricted Information

- Sound personnel security program must:
  - Define rules that regulate employee access to restricted information
    - Ensure that access is defined and controlled
  - Use the following six factors to determine the shape and outcome of that process:
    1. User account management
    2. Audit and management review procedures
    3. Detection of and response to unauthorized activities
    4. Friendly termination
    5. Unfriendly termination
    6. Knowing your contractors

User Account Management

- Encompasses the practices that an organization employs to:
  - Establish, issue, and close the accounts of individual employees
  - Track employee access behavior
  - Track individual employee access authorizations
  - Manage the employee access control operation

Regular and systematic reviews of user accounts

- Use of those accounts has to be monitored by personal inspection
- Reviews should verify five user characteristics:
  1. Level of access is appropriate to assigned level of privilege for each application
  2. Level of access assigned conforms with the concept of least privilege
  3. Accounts assigned are active and appropriate to the employee's job function
  4. Management authorizations up to date
  5. Required training completed

Procedures should be in place to address employee fraud or misuse

- Countermeasures employed in this area are frequently based on software-enabled monitoring functions
  - IDSs perform that monitoring function by either:
    - Pattern matching: matching system behavior with known patterns of misuse or violation
    - Anomaly detection: set to detect anomalous behavior with respect to a baseline of normal operation
- Procedural methods to detect unauthorized or illegal activity such as:
  - Direct auditing of system logs
  - Procedural analysis using audit trails to detect fraudulent actions

Friendly Termination

- A set of standard procedures to guide outgoing or transferring employees
- Implemented as part of standard human resources function
- Ensure that user account privileges are removed from system in a timely manner
  - Removal of access privileges, computer accounts, authentication tokens
  - Assurance of the continued integrity and availability of data in accounts that each access privilege was granted for
  - Briefing on the continuing responsibility for confidentiality and privacy
  - Securing cryptographic keys
  - Return of organization IS property

Unfriendly Termination

- Greater potential for mischief
- Consider following steps:
  - Resignation on unfriendly terms – terminate system access immediately
  - Termination decision – remove system access immediately after that decision is made
    - Do not allow access after notifying the decision
  - If the employee continues to work for a period after they have been notified – assign duties that do not require system access
  - Extremely unfriendly terminations – expedite their physical removal from the area

Contractor Considerations

- Objective: establish sufficient control over all of the personnel in the organization who are involved in performing work or delivering specific work products
- Some steps:
  - Establish an understanding of the work
  - Perform a thorough job-task analysis of the outsourced work
  - Accountability includes:
    - Monitoring and supervising steps conducted through audits
    - Reviews of the work
    - Implementation of rigorous control functions within automated processes
  - Governed by measurable performance criteria
  - Establish an incident reporting function
    - Computer emergency response team (CERT)

Questions?