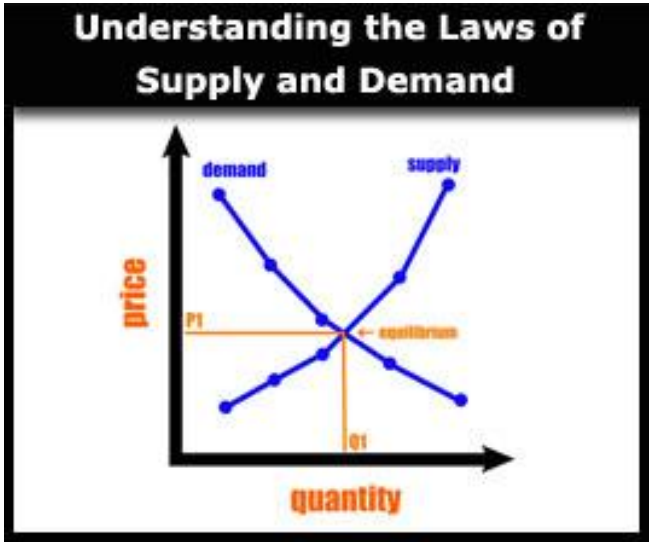
Lecture 11: Personnel & Security

EECS711 Security Management & Audit

Objectives

- Identify the skills and requirements for InfoSec positions
- List the various InfoSec professional certifications and identify which skills are encompassed by each
- Discuss and implement information security constraints on the general hiring processes
- Explain the role of InfoSec in employee terminations
- Describe the security practices used to control employee behavior and prevent misuse of information

Staffing the Security Function



- As long as there are hackers and other security risks, there will be a need for competent InfoSec professionals

- $(ISC)^2$ 2012 Career Impact Survey:
  - 2,256 respondents globally
  - How economic conditions and security threats affected the information security profession?
  - *"Security career opportunities spike while hiring challenges grow*"

Staffing the Security Function

- 2012 Career Impact Survey found:
  - Skilled security professionals are enjoying a nearly full-employment market
    - Less than 4% of survey respondents were unemployed
    - Over 35% of respondents reported changing jobs in 2012
  - Commercial organizations are struggling to find qualified candidates
    - Perception of the security threat is growing
    - Hiring is on the rise; security budgets are increasing
    - Finding the right people is challenging
    - Operations security and security management skills lead hiring requirements

Demand for IA Workspace

- (ISC)2 Global Information Security Workforce Study
  - A Frost & Sullivan Market Survey
  - 2010: Forecast for Information Security Professionals

	2010	2011	2012	2013	2014	2015	2010-2015 CAGR
Americas	920,845	1,058,972	1,214,641	1,393,193	1,570,128	1,785,236	14.2%
EMEA	617,271	703,689	796,576	897,741	1,014,448	1,148,355	13.2%
APAC	748,348	830,666	924,531	1,038,248	1,168,029	1,310,529	11.9%
Total	**2,286,464**	**2,593,327**	**2,935,748**	**3,329,183**	**3,752,605**	**4,244,120**	13.2%

  - 2015 survey: 14,000 information security professionals worldwide
    - More than 60 percent of respondents said their organizations currently have too few information security workers
    - **The expected shortfall** in 5 years: the difference between the projected workforce demand and the number of professionals predicted to actually be in the field is 1.5 million

Qualifications and Requirements

- Which qualifications competent InfoSec personnel should have?
- Organizations should take the following steps:
  - **General management** should learn more about the requirements and qualifications for both InfoSec and relevant IT positions
  - **Upper management** should learn more about InfoSec budgetary and personnel needs
  - **The IT and general management** should grant the InfoSec function an appropriate level of influence and prestige

Qualifications and Requirements

- Organizations look for InfoSec professionals who:
  1. Understand how organizations are structured and operated
  2. Recognize that InfoSec is a management task that cannot be handled with technology alone
  3. Work well with people and have strong written and verbal communication skills
  4. Acknowledge the role of policy in guiding security efforts
  5. Understand the essential role of InfoSec education and training

Qualifications and Requirements

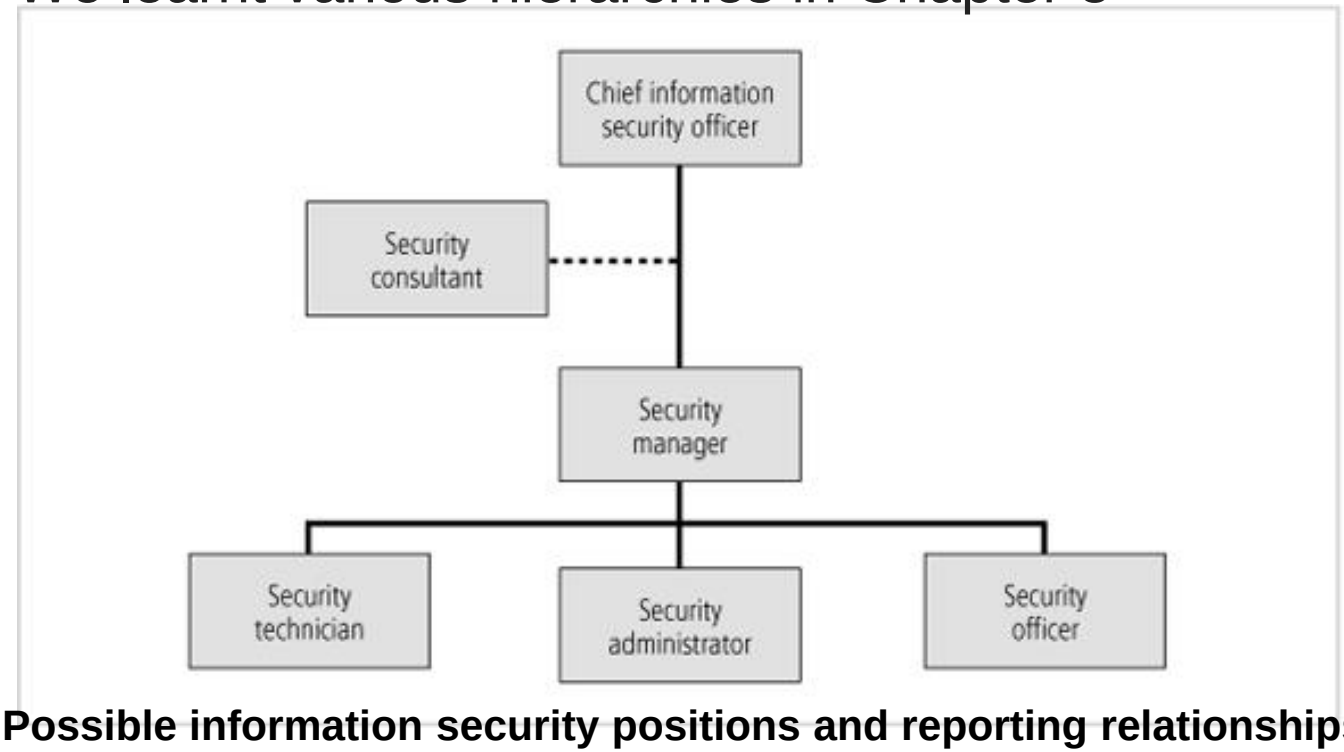
- Organizations look for InfoSec professionals who:
  6. Perceive the threats facing an organization, understand how these threats can become transformed into attacks, and safeguard the organization from InfoSec attacks
  7. Understand how technical controls can be applied to solve specific InfoSec problems
  8. Demonstrate familiarity with the mainstream information technologies
  9. Understand IT and InfoSec terminology and concepts

Entering the Information Security Profession

- Many InfoSec professionals enter the field from
  - Law enforcement
  - The military
  - Other careers in IT
    - Such as networking, programming, database administration, or systems administration
  - Modern career path includes students with security education
- Organizations foster greater professionalism by:
  - Clearly defining their expectations
  - Establishing explicit position descriptions

Information Security Positions

- Typical InfoSec job positions and the departmental hierarchy
  - We learnt various hierarchies in Chapter 5



Possible information security positions and reporting relationships

Chief Information Security Officer (CISO)

- **Chief information security officer (CISO)**
  - Often considered the top InfoSec officer in the organization
  - Frequently reports to the CIO or the CSO
  - Business managers and technologists
  - Must knowledgeable in all areas of InfoSec, including technology, planning, and policy
- Qualifications and Position Requirements
  - Certified Information Systems Security Professional (CISSP)
  - Certified Information Security Manager (CISM)
  - A graduate degree in business, technology, criminal justice, …

Chief Information Security Officer (CISO)

- Charles Cresson Wood's Information Security Roles and Responsibilities Made Easy, Version 3
  - Defines the CISO position on pages 405-408
- CISO's should follow six key principles:
  - Business engagement
  - Focus initiatives on what is learned
  - Align, target, and time initiatives
  - Service delivery
  - Credibility
  - Relationship management

Security Manager

- **Security manager**
  - Accountable for the day-to-day operation of all or part of the InfoSec program
  - Assigned specific managerial duties by the CISO
    - Policy development, risk assessment, contingency planning, operational and tactical planning
  - Resolve issues raised by technicians
  - Often liaise with managers from other departments in joint planning and development
  - Managing instead of administrating technologies
    - Given responsibility for specific tasks and held responsible and accountable for the accomplishment of those tasks

Security Manager Duties

- Providing InfoSec oversight:
  1. Maintain current and appropriate body of knowledge necessary to perform InfoSec management
  2. Effectively apply InfoSec management knowledge to enhance the security of networks and systems
  3. Maintain working knowledge of applicable legislative and regulatory initiatives
  4. Develop appropriate InfoSec policies, standards, guidelines, and procedures
  5. Provide reports for higher management
  6. Participate in short-term and long-term planning
  7. Monitor the InfoSec program measurement process and evaluate compliance effectiveness

Security Manager Duties

6. Oversee and conduct InfoSec reviews
7. Coordinate and perform reviews of contracts, projects, and proposals
8. Manage InfoSec office personnel

- Managing InfoSec personnel:
  1. Determine positions and personnel
  2. Develop meaningful job descriptions
  3. Prioritize and assign tasks
  4. Provide feedback to staff and apprise performance

Security Manager

- Qualifications and Position Requirements
  - CISSP or CISM certification is preferable
  - More specialized, experience in:
    - Budgeting
    - Project management
    - Personnel management
    - Hiring and firing
  - Can draft middle-level and lower-level policies, standards and guidelines
  - Experience with BCP

Security Technician

- **Security technician**
  - A technically qualified individual
  - Typically an entry-level position
  - Specialized with certain level of technical skill:
    - Configure firewalls and IDPS
    - Implement security software
    - Diagnose and troubleshoot problems
    - Coordinate with systems and network administrators to ensure security technical controls are properly implemented

Security Technician

- Qualifications and Position Requirements vary
- Job requirements usually include:
  - Some level of experience with a particular hardware and software package
  - Familiarity with a particular technology

Other Position Titles

- Many non-InfoSec job descriptions should include InfoSec roles and responsibilities
  - InfoSec community
    - CSO, InfoSec department manger, access control system administrator, InfoSec consultant, engineer, contingency planner, …
  - IT community
    - CIO, CTO, InfoSys analyst, system programmer, computer operation manager, data librarian, help desk specialist, telecommunication manager, …
  - General business community
    - Physical security department manager, building & facility guard, InfoSys auditor, Ethics officer, chief legal officer, HR, …

Information Security Professional Credentials

- Many organization's rely on professional certifications
  - To ascertain the level of proficiency possessed by a candidate
- Employers struggle to match certifications to position requirements
- InfoSec workers try to determine which certification programs will help them in the job market

Get Certified

- It has been discovered that a former member of the IT department who switched to the development team still has administrative access to many major network infrastructure devices and servers. Which of the following mitigation techniques should be implemented to help reduce the risk of this event recurring?

A. DLP
B. Incident management and response policy
C. Change management notifications
D. Regular user permission and rights reviews

Get Certified

- You have implemented a backup plan for your critical file servers, including proper media rotation, backup frequency, and offsite storage. Which of the following must be performed on a regular basis to ensure the validity and integrity of your backup system?

A. Periodic testing of restores
B. Multiple monthly backup media
C. Purchasing of new media
D. Updating the backup application software

Get Certified

- When you connect to a secure HTTPS web page, which of the following actions is performed first?

A. The username and password are sent for authentication.
B. A digital certificate establishes the web site identity to the browser.
C. The web page is displayed, and then authentication is performed.
D. The client establishes its identity to the web server.

Get Certified

- You have had a rash of hacking incidents where weak employee passwords are being hacked through brute-force methods and unauthorized users are gaining access to the network. Which of the following security policies is most efficient for preventing brute-force hacking attempts on employee passwords?

A. Password rotation
B. Password length and complexity restrictions
C. Password expiration
D. Limiting logon attempts

Get Certified

- An executive is traveling with his laptop computer to a conference. The contents of his laptop contain very confidential product information, including development specifications and product road maps. Which of the following techniques can be implemented to protect the confidentiality of the data on the laptop?

  A. Make sure all software is up to date.
  B. Password-protect the laptop BIOS.
  C. Move the confidential documents to a USB key.
  D. Encrypt the hard drive using a TPM.

Get Certified

- You are designing a new web application service for your company. After an initial design review, it is discovered that a number of attack surfaces have been revealed that go well beyond the initial baseline proposed for the application, including unneeded network services that are enabled. What should you do?

A. Rework the initial baseline.
B. Perform a black box test.
C. Reduce attack surfaces by removing unneeded services from the design.
D. Reduce the attack surfaces during actual coding.

Get Certified

- The NIST organization has defined best practices for creating continuity plans. Which of the following phases deals with identifying and prioritizing critical functions and systems?

  A. Identify preventive controls.
  B. Develop the continuity planning policy statement.
  C. Develop recovery strategies.
  D. Conduct the business impact analysis.

(ISC)² Certifications

- International Information Systems Security Certification Consortium (ISC)²
  - Exam offered each year in May
- Offers three security certifications:
  - Certified Information Systems Security Professional (CISSP)
  - Systems Security Certified Practitioner (SSCP)
  - Certified Secure Software Lifecycle Professional (CSSLP)

$(ISC)^2$ Certifications – CISSP

- CISSP – considered to be the *most prestigious* certification for security managers and CISOs
- To sit for the CISSP exam, the candidate must have:
  - At least five years of direct, full-time security professional work experience in two or more of 10 domains
  - Four years of direct security work experience in two or more of 10 domains and a four-year college degree
- Complete an exam with 250 questions in 6 hours
- Retaining certificate requires continuous education credits

$(ISC)^2$ Certifications – CISSP

- Exam covers 10 domains of knowledge:
  - Access control
  - Business continuity and disaster recovery planning
  - Cryptography
  - InfoSec governance and risk management
  - Legal, regulations, investigations, and compliance
  - Operations security
  - Physical security
  - Security architecture and design
  - Software development security
  - Telecommunications and network security

CISSP Concentrations

- A number of concentrations are available for CISSPs to demonstrate advanced knowledge beyond the CISSP common body of knowledge (CBK)
  - ISSAP®: Information Systems Security Architecture Professional
  - ISSEP®: Information Systems Security Engineering Professional
  - ISSMP®: Information Systems Security Management Professional Enterprise Security Management Practices

$(ISC)^2$ Certifications – SSCP

- SSCP certification – more applicable to the security manager than to the technician
  - Focuses on practices, roles, and responsibilities
  - 1-year experience, complete 125 questions in 3 hours
- Covers 7 domains:
  - Access controls
  - Cryptography
  - Malicious code and activity
  - Monitoring analysis
  - Networks and telecommunications
  - Risk, response, and recovery
  - Security operations and administration

$(ISC)^2$ Certifications – CSSLP

- Certified Secure Software Lifecycle Professional (CSSLP) – a new (ISC)2 certification
  - Focused on the development of secure applications
- To qualify for the CSSLP, you must have
  - At least four years of recent experience with the software development life cycle
  - Worked as an expert in four of the seven experience assessment topic areas
  - Must compose an essay in each of your four areas of expertise and submit it as your exam

$(ISC)^2$ Certifications – CSSLP

- Seven experience assessment topics include:
  - Secure software concepts
  - Secure software requirements
  - Secure software design
  - Secure software implementation/coding
  - Secure software testing
  - Software acceptance
  - Software development, operations, maintenance, and disposal

Associate of $(ISC)^2$

- **The Associate program**
  - If you want to take the CISSP or SSCP exams before obtaining the requisite experience for certification
  - Award recognition for those passing one of the certification exams
- $(ISC)^2$ provides certification examinations exclusively via electronic testing
  - Has greatly improved its exam-offering schedules and locations

ISACA Certifications

- Information Systems Audit and Control Association (ISACA)
  - Exam offered each year in June
- Sponsors four certifications:
  - Certified Information Security Manager (CISM)
  - Certified Information Security Auditor (CISA)
  - Certified in the Governance of IT (CGEIT)
  - Certified in Risk and Information Systems Control (CRISC)

ISACA Certifications – CISM

- For experienced InfoSec managers
- CISM exam covers 4 practice domains in 2013:
  1. Information Security Governance (24%)
  2. Information Risk Management and Compliance (33%)
  3. Information Security Program Development and Management (25%)
  4. Information Security Incident Management (18%)
- To be certified, the applicant must:
  - Pass the examination
  - Adhere to a code of ethics promulgated by ISACA
  - Pursue continuing education
  - Document five years InfoSec work experience

ISACA Certifications – CISA

- For networking, audit and security professionals
- CISA requirements:
  - Successful completion of the CISA examination
  - Experience as an InfoSec auditor, with a minimum of five year's experience in information systems auditing, control, or security
  - Agreement to the Code of Professional Ethics
  - Payment of maintenance fees, a minimum of 20 contact hours of continuing education annually, and a minimum of 120 contact hours during a fixed three-year period
  - Adherence to the Information Systems Auditing Standards

ISACA Certifications – CISA

- CISA exam covers 5 areas of information systems auditing in 2013:
  1. The Process of Auditing Information Systems (14%)
  2. Governance and Management of IT (14%)
  3. Information Systems Acquisition, Development and Implementation (19%)
  4. Information Systems Operations, Maintenance and Support (23%)
  5. Protection of Information Assets (30%)

ISACA Certifications – CGEIT

- Certified in the Governance of IT (CGEIT) – targeted at upper-level executives
- The exam covers 5 areas:
  1. Framework for the Governance of Enterprise IT
  2. Strategic Management
  3. Benefits Realization
  4. Risk Optimization
  5. Resource Optimization
- These certifications require a minimum of one year experience in IT governance and experience in at least two of the domains listed

ISACA Certifications – CRISC

- Certified in Risk and Information Systems Control (CRISC)
  - Link IT risk management to enterprise risk management
- The exam covers 5 areas:
  1. Risk Identification, Assessment, and Evaluation
  2. Risk Response
  3. Risk Monitoring
  4. Information Systems Control Design and Implementation
  5. Information Systems Control Monitoring and Maintenance
- Certification requires a minimum of three years experience in risk management and information systems control in at least three of the domains

SANS Certifications

- The SANS Institute (*System Administration, Networking, and Security Institute*)
  - In 1999, developed a series of technical security certifications known as the Global Information Assurance Certification (GIAC)
- GIAC Management Certificates and Certifications:
  - GIAC Information Security Professional (GISP)
  - GIAC Security Leadership Certification (GSLC)
  - GIAC Certified ISO-27000 Specialist (G2700)
  - GIAC Certified Project Manager Certification (GCPM)

SANS Certifications

- GIAC offers three types of certification: Silver, Gold, and Platinum
  - Requirements for Silver are the completion of exams
    - Full certifications require two exams and certificates require a single exam
  - After earning Silver certification, a candidate can apply for a Gold certification
    - Requires a technical paper
  - Platinum certifications require a multiple-choice test, along with a day-long lab to test hands-on skill

EC-Council Certifications

- International Council of Electronic Commerce Consultants
- Offers
  - Certified Ethical Hacker, C|Network Defense Architect, E|Certified Security Programmer, …
  - Certified CISO (C|CISO)
    - Tests not only security domain knowledge but also executive business management knowledge

EC-Council Certifications

- C|CISO domains include 5 domains:
  - Domain 1: Governance (Policy, Legal, and Compliance)
  - Domain 2: IS Management Controls and Auditing Management (Projects, Technology, and Operations)
  - Domain 3: Management (Project and Operations)
  - Domain 4: Information Security Core Competencies
    - Covers the common body of InfoSec knowledge
    - Includes numerous subdomains such as access control, social engineering, physical security, risk management, …
  - Domain 5: Strategic Planning and Finance

CompTIA Certifications

- Computing Technology Industry Association (CompTIA)
- Security+ certification
  - Tests for security knowledge mastery of an individual with two years of on-the-job networking experience, with an emphasis on security
  - Covers industry-wide topics in 6 domains

Domain	Percentage of Examination
1.0 Network security	21%
2.0 Compliance and operational security	18%
3.0 Threats and vulnerabilities	21%
4.0 Application, data, and host security	16%
5.0 Access control and identity Management	13%
6.0 Cryptography	11%

Source: CompTIA[24].

ISFCE Certifications

- International Society of Forensic Computer Examiners (ISFCE)
- Offers two levels of certification
  - Certified Computer Examiner (CCE)
    - A computer forensics certification
    - CCE certification has concentration/endorsements corresponding to various operations systems
  - Master Certified Computer Examiner (MCCE)
    - A CCE who earns three or more of these endorsements

ISFCE Certifications – CCE

- Certified Computer Examiner (CCE)
  - Applicant must:
    - Have no criminal record, meet minimum experience, training, or self-training requirements
    - Abide by the certification's code of ethical standards
    - Pass an online examination
    - Successfully perform actual forensic examinations on three test media
  - Certification process covers
    - Ethics in practice
    - Forensics data seizure procedures
    - Casework and other forensics examination procedures
    - …

Certification Costs

- Certification exams
  - Individual certification exams can cost as much as $750
  - Certifications that require multiple exams can cost more
- Formal training
  - Cost for preparing for the exams can be significant
    - Courses, study sessions, exam review books
- Work experiences
  - Most exams require two or three years work experience
    - Some programs require candidates to document certain minimum experience before they are permitted to sit for an exam

Employment Policies and Practices

- Including InfoSec responsibilities in every employee's job description can make an entire organization take InfoSec more seriously
- Examine many aspects of human resources:
  - Recruiting/hiring
  - Firing
  - Managing
  - Releasing

Hiring

- InfoSec considerations should become part of the hiring process
  - The CISO, in cooperation with the CIO and relevant InfoSec managers, should establish a dialogue with HR

1. Job Descriptions
   - Elements of the job description that describe access privileges should be omitted when advertising open positions

Hiring

2. Interviews
   - Get InfoSec department involved in related positions
   - Limit information on the access rights of the position
   - Site visit should avoid secure and restricted sites
3. New Hire Orientation
   - New employees should receive an extensive InfoSec briefing
   - Orientation should cover policies, security procedures, access levels, and training on the secure use of information systems
4. On-the-Job Security Training
   - Periodic security awareness and training activities should be conducted
   - Formal and informal seminars for InfoSec employees

Hiring

5. Security Checks
   - Background checks should be conducted
     - Identity checks
     - Education and credential checks
     - Previous employment verification
     - Reference checks
     - Worker's compensation history
     - Motor vehicle records
     - Drug history
     - Medical history
     - Credit history
     - Civil court history
     - Criminal court history

Organizations must comply with federal regulations regarding use of personal information in employment practices

Contracts and Employment

- **Monitoring and nondisclosure agreements**
  - Many policies require an employee to agree in writing
  - Important to have these contracts and agreements in place at the time of the hire
- **Employment contingent upon agreement**
  - Job candidates are not offered a position unless they agree to the binding organizational policies
- Once security agreements are signed, the remainder of employment contract may be executed

Security as Part of Performance Evaluation

- Organizations should incorporate InfoSec components into employee performance evaluations
  - To heighten InfoSec awareness and change workplace behavior
  - Motivate employees to take more care when performing these tasks

Termination Issues

- When an employee leaves an organization:
  - Employee's access to the organization's systems must be disabled
  - Employee must return all removable media
  - Employee's hard drives must be secured
  - File cabinet locks must be changed
  - Office door locks must be changed
  - Employee's keycard access must be revoked
  - Employee's personal effects must be removed
  - Employee should be escorted from the premises, once business property has been returned
- Conduct exit interview to remind contractual obligations

Personnel Security Practices

- Monitor and control employees to minimize misuse of information
  - Separation of duties
    - Information security principle
    - Requires significant tasks to be split up in such a way as to require more than one individual for completion
  - Two-person control
    - Requires that two individuals review and approve each other's work before the task is considered complete
  - Job rotation
    - Requires that every employee be able to perform the work of at least one other employee

Personnel Security Practices

- Task rotation
  - All critical tasks can be performed by multiple individuals
  - Both of these ensure that no one employee is performing actions that cannot be knowledgeably reviewed by another employee
- Mandatory vacation policy
  - Requires employees to take at least one week of vacation a year
  - Gives the organization a chance to review everyone's work
- Principle of least privilege
  - Employees should access only the information they need

Security of Personnel and Personal Data

- Organizations are required by law to protect sensitive or personal employee information, such as:
  - Employee addresses and phone numbers
  - Social security numbers
  - Medical conditions
  - Names and addresses of family members
- This responsibility also extends to customers, patients, and anyone with whom the organization has business relationships

Security Considerations for Nonemployees

- Temporary Workers
  - Access to information should be limited to only what is necessary to perform their duties
  - Organizations can attempt to have temps sign nondisclosure agreements and fair use policies, but the temp agency may refuse to go along
- Contract Employees
  - Should not be allowed to wander freely in and out of buildings
  - Typically they are hired via a third-party organization
  - Professional contractors may require access to all areas of the organization

Security Considerations for Nonemployees

- Consultants
  - Have their own security requirements and contractual obligations
  - Their contracts should specify their rights of access to information and facilities
  - Apply the principle of least privilege when working with consultants
- Business Partners
  - A prior business agreement must specify the levels of exposure that both organizations are willing to tolerate
  - Nondisclosure agreements are an important part of any collaborative effort