# Management of Information Security, 4th Edition

*Chapter 11*

*Personnel and Security*

# Objectives

- Identify the skills and requirements for information security positions
- List the various information security 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 information security 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
- 2012 Career Impact Survey found:
  - Less than 4 percent of over 2250 survey respondents were unemployed
    - Half of those for reasons other than job availability
  - Over 35 percent of respondents reported changing jobs in 2012
    - But this was mostly due to advancement opportunity or personal preference

# Qualifications and Requirements Part 1

- 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 communities of interest should grant the InfoSec function an appropriate level of influence and prestige

# Qualifications and Requirements Part 2

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

# Qualifications and Requirements Part 3

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

# Entering the Information Security Profession

- Many InfoSec professionals enter the field from law enforcement or the military
  - Or other careers in IT, such as networking, programming, database administration, or systems administration
- Organizations can foster greater professionalism in the InfoSec discipline by:
  - Clearly defining their expectations
  - Establishing explicit position descriptions

# Information Security Positions

- Figure 11-2 shows typical InfoSec job positions and the departmental hierarchy

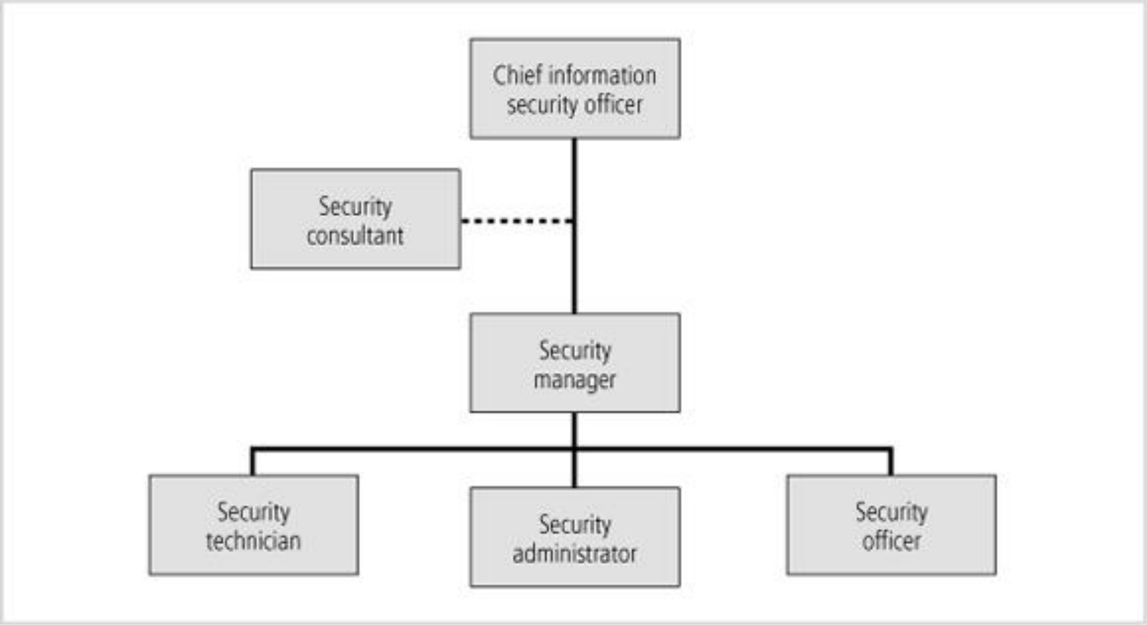


**Figure 11-2** Possible information security positions and reporting relationships

# Chief Information Security Officer (CISO)

- Chief information security officer (CISO) - often considered the top InfoSec officer in the organization
  - Frequently reports to the chief information officer (CIO) or the chief security officer (CSO)
  - Must knowledgeable in all areas of InfoSec, including technology, planning, and policy
- ***Qualifications and Position Requirements***
  - Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) certifications are common qualifications

# Chief Information Security Officer (CISO) (continued)

- 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 Part 1

- **Security manager** - accountable for the day-to-day operation of all or part of the InfoSec program
    - Often assigned specific managerial duties by the CISO, including policy development, risk assessment, contingency planning, and operational and tactical planning for the security function
    - Often liaise with managers from other departments in joint planning and development
    - Given responsibility for specific tasks and held responsible and accountable for the accomplishment of those tasks

# Security Manager Part 2

- List of duties security managers are expected to be competent at:
  - Maintain current and appropriate body of knowledge necessary to perform InfoSec management
  - Effectively apply InfoSec management knowledge to enhance the security of networks and systems
  - Maintain working knowledge of applicable legislative and regulatory initiatives
  - Develop appropriate InfoSec policies, standards, guidelines, and procedures
  - Provide reports for higher management

# Security Manager Part 3

- List of duties security managers are expected to be competent at:
  - Participate in short-term and long-term planning
  - Monitor the InfoSec program measurement process and evaluate compliance effectiveness
  - Oversee and conduct InfoSec reviews
  - Coordinate and perform reviews of contracts, projects, and proposals
  - Manage InfoSec office personnel
- For a complete list of potential duties, see page 410 of the text

# Security Manager Part 4

- ***Qualifications and Position Requirements*** - CISSP or CISM certification is preferable, along with experience in:
  - Budgeting
  - Project management
  - Personnel management
  - Hiring and firing
  - Drafting middle-level and lower-level policies
    - As well as standards and guidelines

# Security Technician

- **Security technician** - a technically qualified individual who may:
  - configure firewalls and IDPSs
  - Implement security software
  - Diagnose and troubleshoot problems
  - Coordinate with systems and network administrators to ensure security technical controls are properly implemented
- The role of security technician is typically an entry-level position

# Security Technician (continued)

- **Qualifications and Position Requirements** - job requirements usually include:
  - Some level of experience with a particular hardware and software package
  - Familiarity with a particular technology
- Charles Cresson Wood’s *Information Security Roles and Responsibilities Made Easy, Version 3*
  - Defines the InfoSec Engineer position on pages 412-414

# Other Position Titles

- Many non-InfoSec job descriptions should include InfoSec roles and responsibilities
- An extensive list of positions with InfoSec elements can be found on pages 414-415 of the text
  - Job description elements have been grouped according to the community of interest

# Information Security Professional Credentials

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

# (ISC)$^2$ Certifications

- International Information Systems Security Certification Consortium (ISC)$^2$ offers security certifications:
  - Certified Information Systems Security Professional (CISSP)
  - Systems Security Certified Practitioner (SSCP)
  - Certified Secure Software Lifecycle Professional (CSSLP)

# 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

# CISSP (continued)

- 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*

# SSCP

- SSCP certification - more applicable to the security manager than to the technician
  - Focuses on practices, roles, and responsibilities
- Covers seven domains:
  - Access controls
  - Cryptography
  - Malicious code and activity
  - Monitoring analysis
  - Networks and telecommunications
  - Risk, response, and recovery
  - Security operations and administration

# 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 and be defined 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

# CSSLP (continued)

- 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 of (ISC)$^2$ program is geared toward individuals who want to take the CISSP or SSCP exams before obtaining the requisite experience for certification
- (ISC)$^2$ has recently begun providing certification examinations exclusively via electronic testing
  - Has greatly improved its exam-offering schedules and locations

# ISACA Certifications

- Information Systems Audit and Control Association (ISACA) 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)

# CISM

- CISM exam covers the following practice domains:
  - *Information Security Governance*
  - *Information Risk Management and Compliance*
  - *Information Security Program Development and Management*
  - *Information Security Incident Management*
- 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

# CISA

- 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

# CISA (continued)

- CISA exam covers the following areas of information systems auditing:
  - *The Process of Auditing Information Systems*
  - *Governance and Management of IT*
  - *Information Systems Acquisition, Development and Implementation*
  - *Information Systems Operations, Maintenance and Support*
  - *Protection of Information Assets*

# CGEIT

- Certified in the Governance of IT (CGEIT) - targeted at upper-level executives
- The exam covers the following areas:
  - *Framework for the Governance of Enterprise IT*
  - *Strategic Management*
  - *Benefits Realization*
  - *Risk Optimization*
  - *Resource Optimization*
- The certification requires a minimum of one year experience in IT governance and experience in at least two of the domains listed

# CRISC

- CRISC exam covers the following areas:
  - *Risk Identification, Assessment, and Evaluation*
  - *Risk Response*
  - *Risk Monitoring*
  - *Information Systems Control Design and Implementation*
  - *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, formerly known as the 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 (continued)

- GIAC offers three types of certification: Silver, Gold, and Platinum
  - Requirements for Silver are the completion of exam(s)
    - 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

- EC-Council offers a Certified CISO (C|CISO) certification
  - Tests not only security domain knowledge but also executive business management knowledge
- C|CISO domains include:
  - *Domain 1: Governance (Policy, Legal, and Compliance)*
  - *Domain 2: IS Management Controls and Auditing Management (Projects, Technology, and Operations)*

# EC-Council Certifications (continued)

- C|CISO domains (cont'd):
  - *Domain 3: Management (Project and Operations)*
  - *Domain 4: Information Security Core Competencies*
    - Covers the common body of InfoSec knowledge
    - Includes numerous subdomains (see page 423)
  - *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
- Security+ covers industry-wide topics:
  - Communication security, infrastructure security, cryptography, access control, authentication, external attack, and operational and organization security

# **Table 11-1** Domains covered in the CompTIA Security+ exam

| 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% |

# ISFCE Certifications

- International Society of Forensic Computer Examiners (ISFCE) offers two levels of certification
- **Certified Computer Examiner (CCE)** - a computer forensics certification where the 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

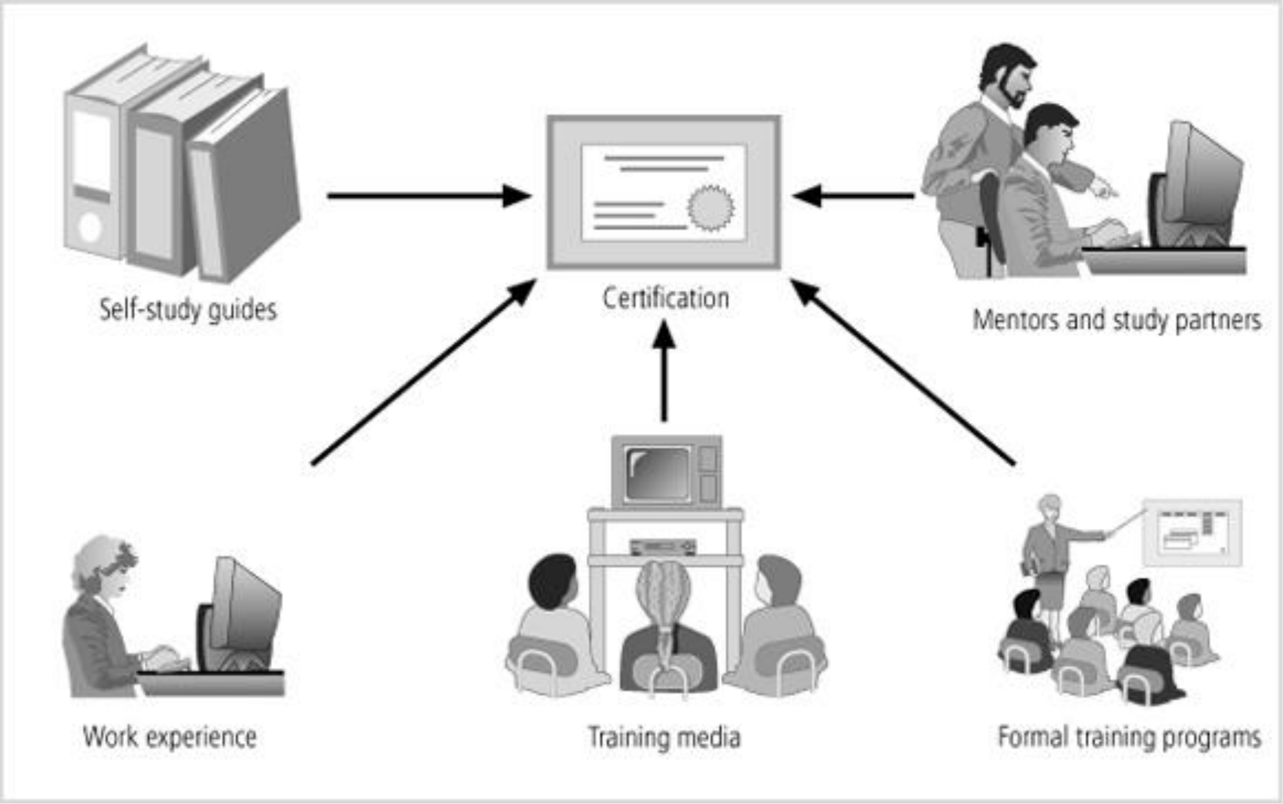
# ISFCE Certifications (continued)

- CCE certification process covers some of the following areas (see page 425 for complete list):
  - Ethics in practice
  - Forensics data seizure procedures
  - Casework and other forensics examination procedures
- CCE certification has concentration/endorsements corresponding to various operations systems
  - A CCE who earns three or more of these endorsements qualifies as a **Master Certified Computer Examiner (MCCE)**

# Certification Costs

- Individual certification exams can cost as much as $750
  - Certifications that require multiple exams can cost thousands of dollars
- Cost for formal training to prepare for the exams can be significant
- Most exams require between two and three years work experience
  - Some programs require candidates to document certain minimum experience  before they are permitted to sit for an exam

# **Figure 11-3** Preparing for security certification



Copyright © 2014 Cengage Learning®.

# Employment Policies and Practices

- Including InfoSec responsibilities in every employee’s job description can make an entire organization take InfoSec more seriously
- The following sections examine many aspects of human resources, including:
  - Recruiting
  - Hiring
  - Firing
  - Managing
  - Releasing

# Hiring Part 1

- The CISO, in cooperation with the CIO and relevant InfoSec managers, should establish a dialogue with human resources personnel
  - So that InfoSec considerations become part of the hiring process
- **Job Descriptions** - elements of the job description that describe access privileges should be omitted when advertising open positions
- **Interviews** - tours of facilities should avoid secure and restricted sites
  - There should be limited discussion of access rights

# Hiring Part 2

- **New Hire Orientation** - new employees should receive an extensive InfoSec briefing
  - Should cover policies, security procedures, access levels, and training on the secure use of information systems
- **On-the-Job Security Training** - periodic security awareness and training activities should be conducted
  - To keep security at the forefront of employees' minds

# Hiring Part 3

- **Security Checks** - background checks should be conducted before an offer is extended to any candidate, regardless of job level
- Common background checks:
  - *Identity checks*
  - *Education and credential checks*
  - *Previous employment verification*
  - *Reference checks*
  - *Worker's compensation history*
  - *Motor vehicle records*

# Hiring Part 4

- Common background checks (cont'd):
  - *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

- Many policies require an employee to agree in writing to monitoring and nondisclosure agreements
  - Important to have these contracts and agreements in place at the time of the hire
- Job candidates can be offered “employment contingent upon agreement”
  - They 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
- Including InfoSec tasks into performance evaluations will motivate employees to take more care when performing these tasks

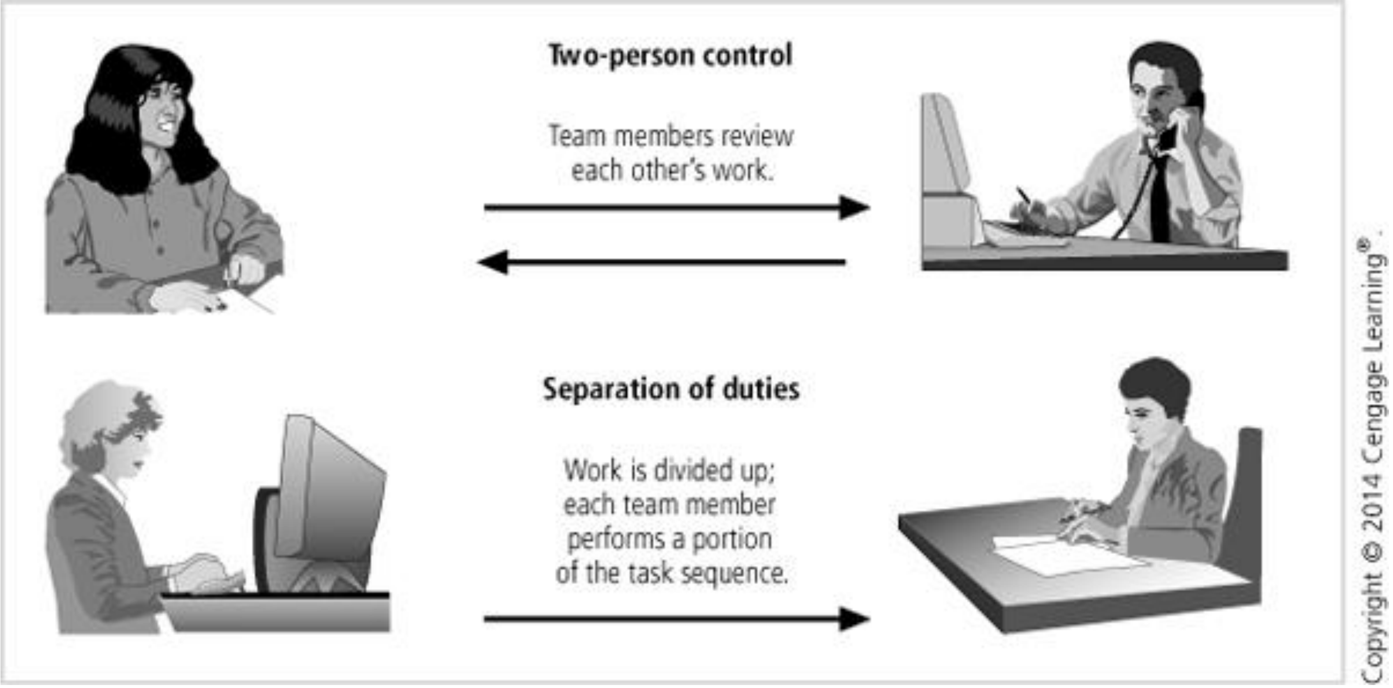
# Termination Issues

- 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

# Personnel Security Practices

- Separation of duties - information security principle that 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

# **Figure 11-5** Personnel security needs


Two-person control
Team members review each other's work.
Separation of duties
Work is divided up; each team member performs a portion of the task sequence.
Copyright © 2014 Cengage Learning®.

# Personnel Security Practices (continued)

- Job rotation - requires that every employee be able to perform the work of at least one other employee
- 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

# 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 (continued)

- **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

# Summary

- The hiring of InfoSec personnel is affected by a number of factors, among them the law of supply and demand
- Many organizations rely on certifications to document the qualifications of current and/or prospective employees
- Many InfoSec professionals enter the field through one of two career paths: 1) former members of law enforcement or the military, or 2) IT professionals
- During the hiring process, applying standard job descriptions can increase the degree of professionalism in the InfoSec field

# Summary (continued)

- Many organizations use recognizable certifications to identify the level of proficiency with security positions
- Management should integrate InfoSec concepts and practices into employment activities
- Organizations need the special services of nonemployees and these relationships must be carefully managed to prevent InfoSec breaches
- Government-mandated requirements for the privacy and security of personnel and personal data must be met by the organization’s InfoSec program