CSIT988/CSIT488
Security, Ethics and Professionalism
Week 12: Personnel and Security Law and Ethics

Subject Coordinator: *Dr Khoa Nguyen*

School of Computing and Information Technology

Autumn 2025

Learning Objectives

- Discuss the skills and requirements for InfoSec positions and explore InfoSec professional certifications
- Explore the integration of InfoSec constraints into an organization's human resources processes
- Laws and ethics in InfoSec

References: Chapter 11 and Chapter 12 of the textbook.

Personnel and Security

- Maintaining a secure environment requires that the InfoSec department be carefully structured and staffed with appropriately credentialed personnel
- Proper procedures must be integrated into all human resources activities
  - Including hiring, training, promotion, and termination practices
- We will discuss:
  - InfoSec personnel hiring issues and practices, including information about the most sought-after professional certification credentials
  - Integrating InfoSec policies into general hiring practices

Staffing the Security Function

- Selecting an effective mix of information security personnel
  - ➢ Requires consideration of several criteria: some are within the control of the organization, others are not
- Supply and demand for personnel with critical information security skills
  - ➢ When demand rises quickly, initial supply often fails to meet it
  - ➢ As demand becomes known, professionals enter the job market or refocus their job skills to gain the required skills, experience, and credentials

Qualifications and Requirements

- To move the InfoSec discipline forward, managers should:
  - Learn more about the requirements and qualifications for information security positions and relevant IT positions
  - Learn more about information security budgetary and personnel needs
  - Grant the information security function (and CISO) an appropriate level of influence and prestige

Qualifications and Requirements (cont'd)

- Desired abilities for InfoSec professionals

  - Understand of 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 communicate effectively using both written and verbal communication
  - Acknowledge the role of policy in guiding security efforts

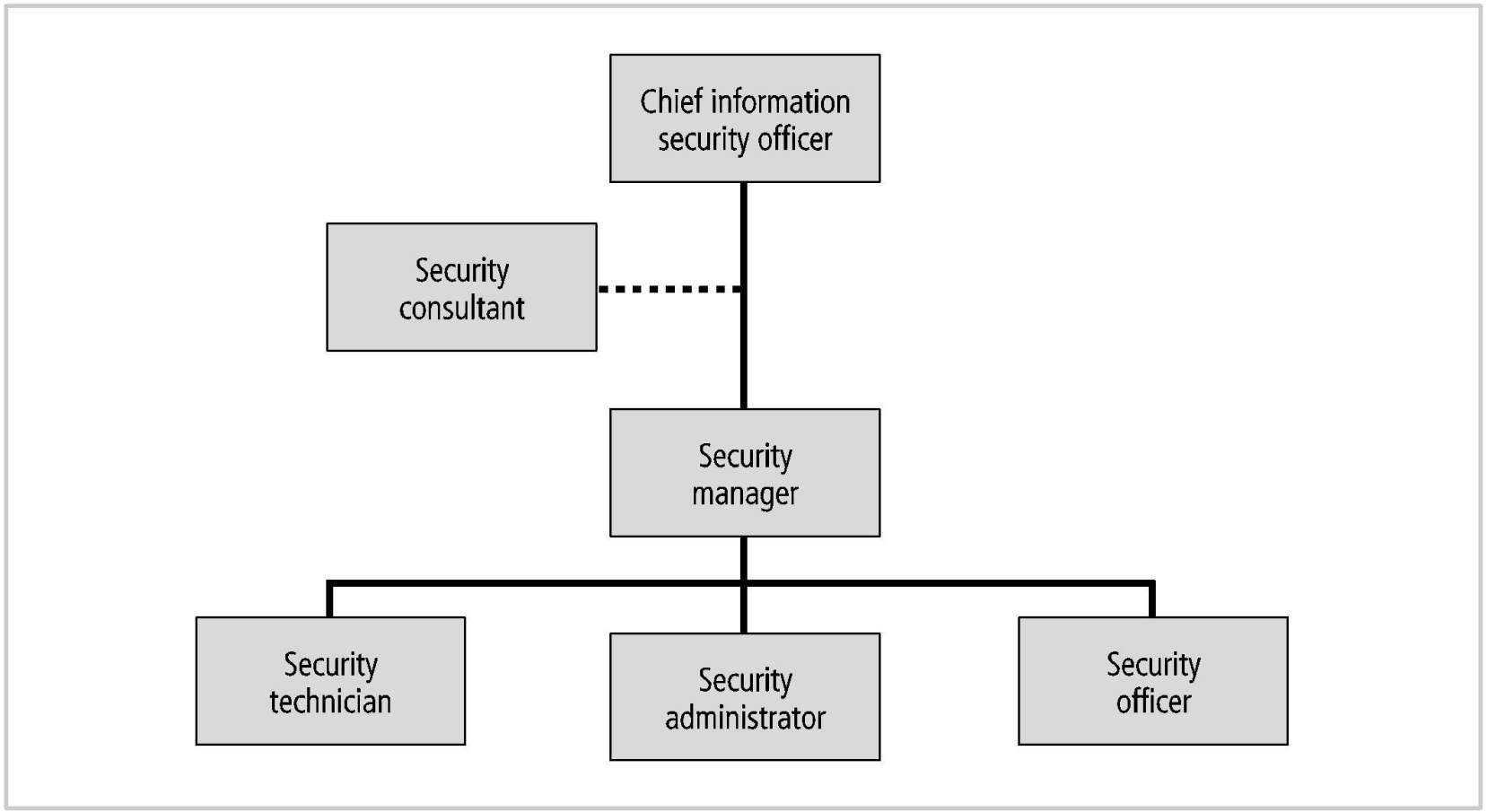
Qualifications and Requirements (cont'd.)

- Desired abilities for information security professionals (cont'd.)
  - ➢ Understand of the essential role of information security education and training
    - ✓ Helps make users part of the solution, rather than part of the problem
  - ➢ Perceive the threats facing an organization
    - ✓ Understand how these threats can become attacks, and safeguard the organization
  - ➢ Understand how to apply technical controls
  - ➢ Demonstrated familiarity with the mainstream information technologies
    - ✓ Including Disk Operating System (DOS), Windows, Linux, and UNIX
  - ➢ Understand of IT and InfoSec terminology and concepts

Information Security Positions

- **Types of InfoSec positions**
  - ➢ Definers provide the policies, guidelines, and standards
    - ✓ People who consult, do risk assessment and develop the product and technical architectures
    - ✓ Senior people with a broad knowledge, but not a lot of depth
  - ➢ Builders are the real techies, who create and install security solutions
  - ➢ Those that administer the security tools, the security monitoring function, and the people who continuously improve the processes

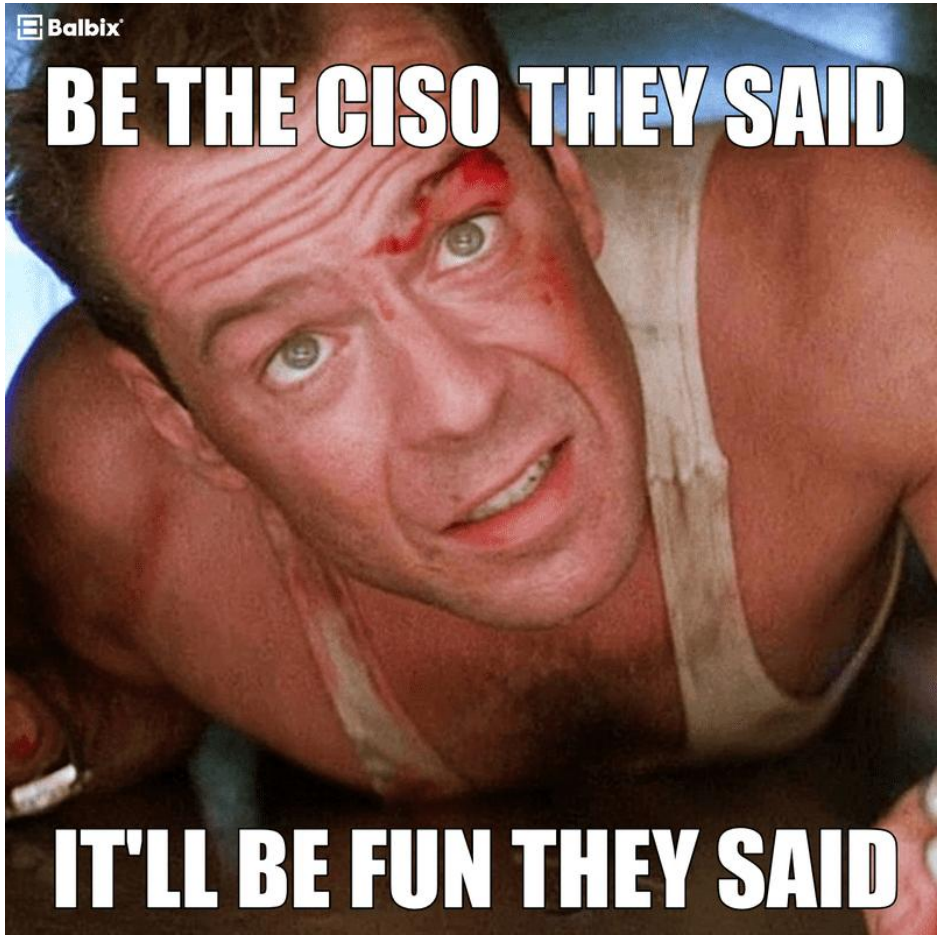
Information Security Positions (cont'd.)



Typical InfoSec positions and reporting relationships

Information Security Positions (cont'd.)

- **Chief Information Security Officer (CISO)**
  - Typically considered the top information security officer in the organization
    - ✓Usually not an executive-level position
    - ✓Frequently reports to the CIO
  - Business managers first and technologists second
  - They must be conversant in all areas of information security
    - ✓Including technology, planning, and policy



The CISO

- Certified Information Systems Security Professional (CISSP)
  - Most common qualification for the CISO
- A graduate degree in criminal justice, business, technology, or another related field is usually required for the CISO
- CISO candidates should have experience in security management, planning, policy, and budgets

Security Managers

- **Security Manager**
  - Accountable for the day-to-day operation of the InfoSec program
  - Accomplishes objectives identified by the CISO and resolves issues identified by the technicians
  - Often assigned specific managerial duties by the CISO
  - Liaise with managers from other departments/divisions
- **Qualifications and Requirements for Security Manager**
  - It is not uncommon for a security manager to have a CISSP
  - Should have experience in traditional business activities, including budgeting, project management, personnel management, hiring and firing
  - Must be able to draft middle/lower-level policies, standards and guidelines
  - Several types exist, tend to be much more specialized than CISOs

Security Technicians

- **Security Technicians**
  - Technically qualified individuals who configure firewalls and IDSs, implement security software, diagnose and troubleshoot problems, and coordinate with systems and network administrators to ensure that security technology is properly implemented
  - Typical information security entry-level position, albeit a technical one

- **Qualifications and Requirements for Security Technicians**
  - Technical qualifications and position requirements for a security technician vary
  - Organizations typically prefer expert, certified, proficient technicians
  - Job requirements usually includes some level of experience with a particular hardware and software package. Experience using the technology is usually required

Information Security Professional Credentials

- Many organizations rely on professional certifications
  - ➢To ascertain the level of proficiency possessed by any given candidate
  - ➢Many certification programs are relatively new
    - ✓Their precise value is not fully understood by most hiring organizations
- Certifying bodies work to educate their constituent communities on the value and qualifications of their certificate recipients

$(ISC)^2$ Certifications

- The International Information Systems Security Certification Consortium ($(ISC)^2$) offers security certifications, including CISSP, SSCP.
- **CISSP**
  - ➢ One of the most prestigious certifications
  - ➢ Recognizes mastery of InfoSec knowledge
  - ➢ Covers 10 domains of InfoSec 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® Certified Information Systems Security Professional

(ISC)^2 Certifications (cont'd.)

- **SSCP**
  - More applicable to an entry-level security manager than a technician
    - ✓Most questions focus on the operational nature of InfoSec
  - Focuses on practices, roles, and responsibilities covering seven domains:
    - ✓Access controls
    - ✓Analysis and monitoring
    - ✓Cryptography
    - ✓Malicious code
    - ✓Networks and Telecommunications
    - ✓Risk, Response and Recovery
    - ✓Security Operations and Administration

ISACA Certifications

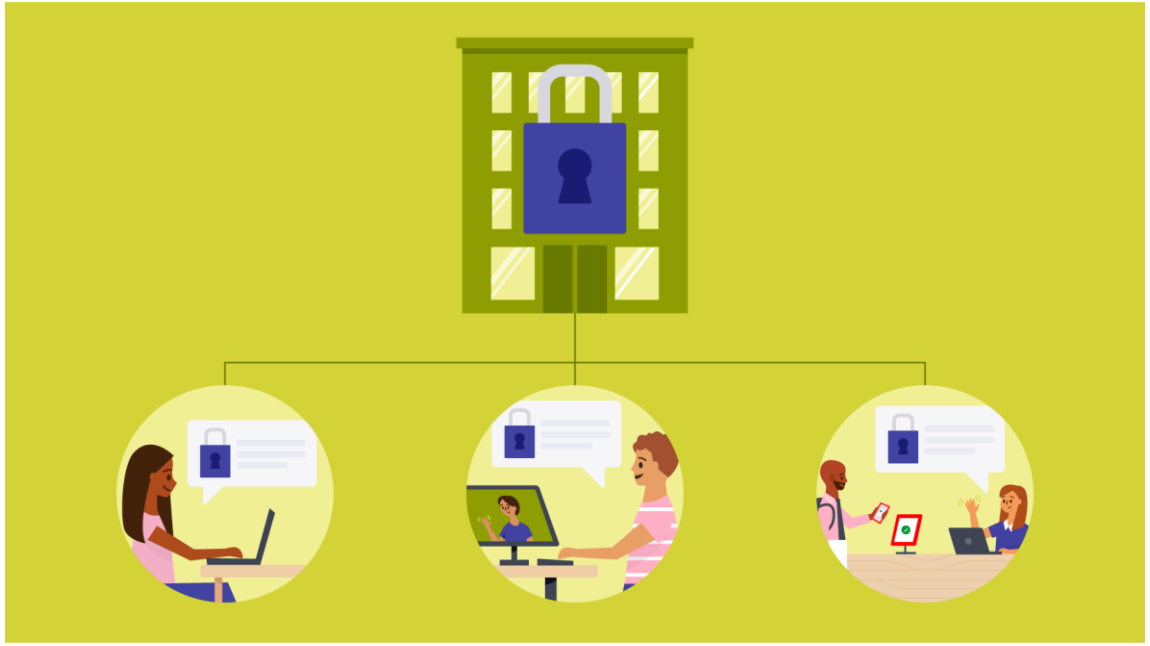
- Information Systems Audit and Control Association (ISACA) sponsors four certifications, including CISA, CISM
- **Certified Information Systems Auditor (CISA)**
  - A certification of the Information Systems Audit and Control Association and Foundation
  - Appropriate for auditing, networking, and security professionals
- **Certified Information Security Manager (CISM)**
  - Geared toward experienced information security managers
  - Assures executive management that a candidate has the required background knowledge needed for effective security management and consulting

Certification Costs

- Preferred certifications can be expensive
- Most experienced professionals find it difficult to do well on the exams without at least some review
- Certifications recognize experts in their respective fields
- The cost of certification deters those who take the exam just to see if they can pass
- Most examinations:
  - Require between two and three years of work experience
  - They are often structured to reward candidates who have significant hands-on experience

Employment Policies and Practices

- Management should integrate solid information security concepts
  - ➢ Across all of the organization's employment policies and practices
  - ➢ Including information security responsibilities into every employee's job description and subsequent performance reviews
    - ✓ Can make an entire organization take InfoSec more seriously



Hiring

- From an InfoSec perspective, hiring employees is laden with potential security pitfalls
- InfoSec considerations should become part of the hiring process
- Job descriptions: Provide complete job descriptions when advertising open positions

Background checks


Certifications

Policies

Covenants and agreements

Contracts

Hiring (cont'd.)

- **Interviews**
  - ➢Information security should advise human resources
    - ✓Limit the information provided to the candidates on the access rights of the position
  - ➢When an interview includes a site visit
    - ✓Tour should avoid secure and restricted sites, because the visitor could observe enough information about the operations or information security functions to represent a potential threat to the organization

Hiring (cont'd.)

- New hire orientation: new employees should receive an extensive information security briefing as part of their orientation
- On-the-job security training
  - ➢ Conduct periodic SETA activities
    - ✓ Keeps security at the forefront of employees' minds and minimizes employee mistakes
- Security checks: Conduct a background check before extending an offer
- Contracts and employment: an important security instrument

Termination Issues

- When an employee leaves an organization, the following tasks must be performed:
  - Disable access to the organization's systems
  - Return all removable media
  - Hard drives must be secured
  - File cabinet and door locks must be changed
  - Keycard access must be revoked
  - Personal effects must be removed
  - Escort the former employee from the premises

Termination Issues (cont'd.)

- Many organizations conduct an exit interview
  - ➢To remind the employee of any contractual obligations
    - ✓ Such as nondisclosure agreements
  - ➢To obtain feedback on the employee's tenure in the organization
- Methods for handling employee outprocessing: hostile and friendly

Termination Issues (cont'd.)

- **Hostile departure**
  - Security cuts off all logical and keycard access before the employee is terminated
  - The employee reports for work, and is escorted into the supervisor's office to receive the bad news
  - The individual is then escorted from the workplace and informed that his or her personal property will be forwarded, or is escorted to his or her office, cubicle, or personal area to collect personal effects

Termination Issues (cont'd.)

- **Friendly departure**
  - ➢The employee may have tendered notice well in advance of the actual departure date
    - ✓Difficult for security to maintain positive control over the employee's access and information usage
  - ➢Employee accounts are usually allowed to continue, with a new expiration date
  - ➢The employee can come and go at will
    - ✓Usually collects any belongings and leaves without escort, dropping off all organizational property before departing

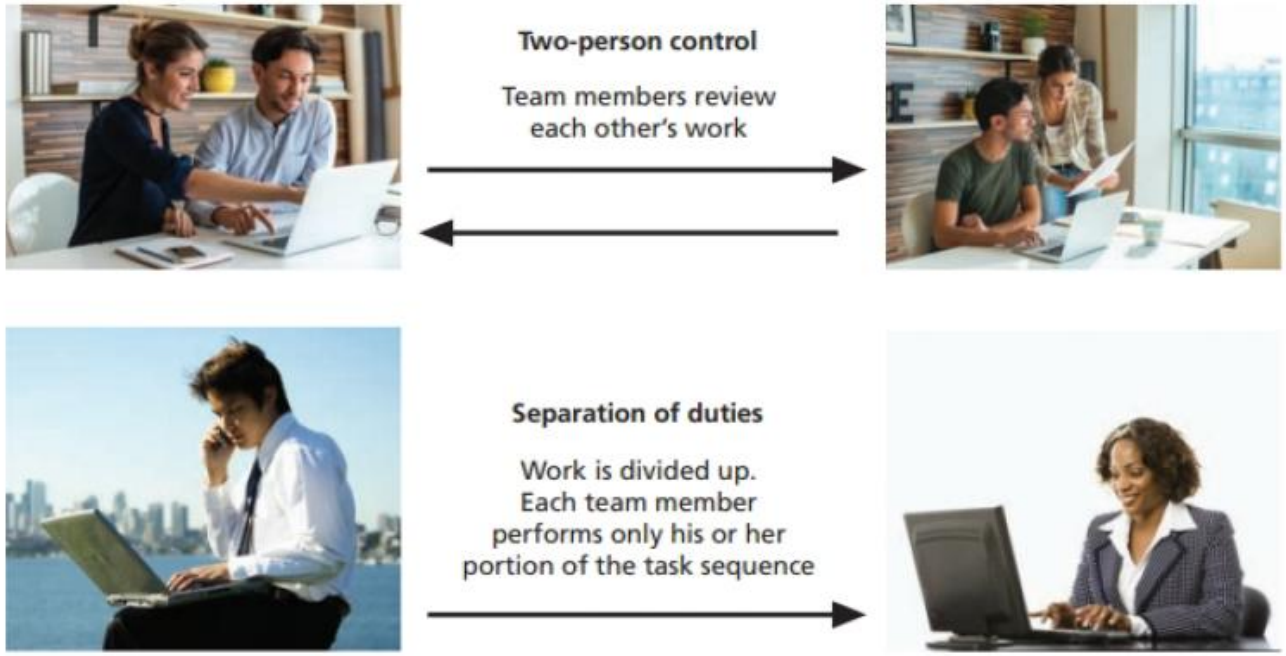
Termination Issues (cont'd.)

- In either circumstance:
  - Offices and information used by departing employees must be inventoried, their files stored or destroyed, and all property returned to organizational stores
  - Departing employees may have collected and taken home information or assets that could be valuable in their future jobs
  - Scrutinizing system logs may allow an organization to determine whether a breach of policy or a loss of information has occurred

Personnel Security Practices

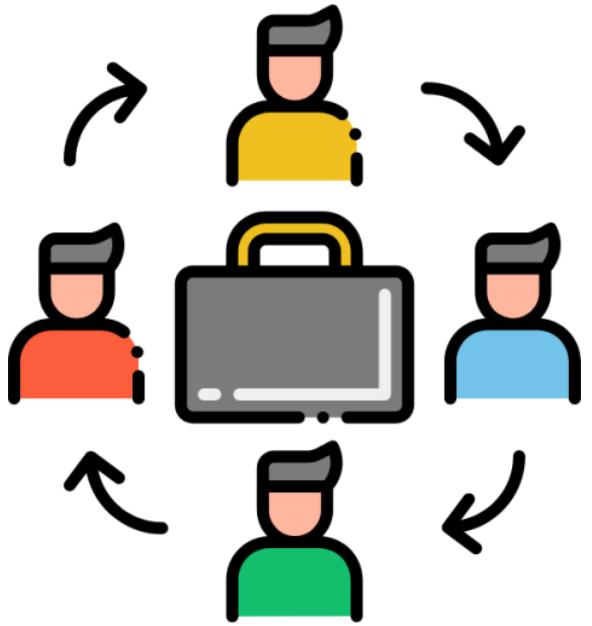
Methods of monitoring and controlling employees to minimize their opportunities to misuse information

- **Separation of duties:** makes it difficult for an individual to violate InfoSec and breach the CIA of information
- **Two-person control:** two individuals review and approve each other's work before the task is considered complete



Personnel Security Practices (cont'd.)

- **Job rotation** is another control used to prevent personnel from misusing information assets: 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
  - Job rotation and task rotation ensure no one employee is performing actions that cannot be knowledgeably reviewed by another employee
- Each employee should be required to take **mandatory vacation**: This policy gives the organization a chance to perform a detailed review of everyone's work



Personnel Security Practices (cont'd.)

- **Limiting access to information**
  - Minimizes opportunities for employee misuse
  - Employees should be able to access only the information they need, and only for the period required to perform their tasks
  - This idea is referred to as the principle of least privilege
    - ✓Ensures that no unnecessary access to data occurs
    - ✓If all employees can access all the organization's data all the time, it is almost certain that abuses will occur

Security of Personnel and Personal Data

- Organizations are required by law to protect sensitive or personal employee information
  - Examples: employee addresses, phone numbers, Social Security numbers, medical conditions, and names and addresses of family members
  - Responsibility extends to customers, patients, and anyone with whom the organization has business relationships

- Personnel data is no different than other data that information security is expected to protect
  - But more regulations cover its protection
- Information security procedures should ensure that this data receives at least the same level of protection as the other important data in the organization

Security Considerations for Nonemployees

- Many individuals who are not employees often have access to sensitive organizational information
  - Relationships with individuals in this category should be carefully managed to prevent threats to information assets from materializing
- **Temporary workers**
  - Not employed by the organization for which they're working
  - May not be subject to the contractual obligations or policies that govern employees
  - Unless specified in its contract with the organization, the temporary agency may not be liable for losses caused by its workers
  - Access to information should be limited to what is necessary to perform their duties

Security Considerations for Nonemployees (cont'd.)

- **Contract employees**
  - Professional contractors may require access to all areas of the organization to do their jobs
  - Service contractors usually need access only to specific facilities
    - ✓Should not be allowed to wander freely
  - In a secure facility, all service contractors are escorted from room to room, and into and out of the facility
- Regulations for service agreements or contracts:
  - Require 24 to 48 hours' notice of a maintenance visit
  - Require all on-site personnel to undergo background checks
  - Require advance notice for cancellation or rescheduling of a maintenance visit

Security Considerations for Nonemployees (cont'd.)

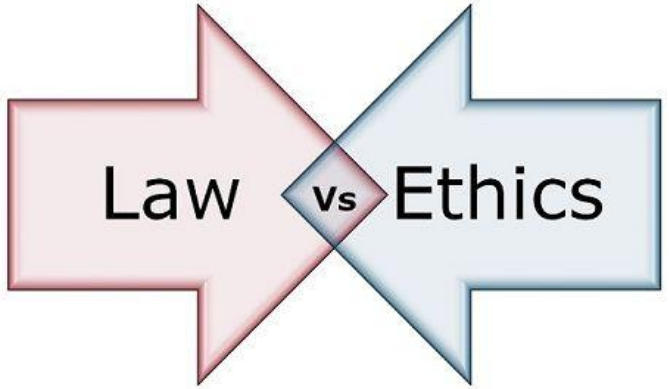
- **Consultants**
  - Have their own security requirements and contractual obligations
    - ✓ Should be handled like contract employees
    - ✓ Special requirements, such as information or facility access requirements, should be integrated into the contract before facility access is granted
  - Protecting your information may not be their number one priority
  - Apply the principle of least privilege

Security Considerations for Nonemployees (cont'd.)

- **Business partners**
  - Strategic alliances with other organizations to exchange information, integrate systems, or enjoy some other mutual advantage
  - A prior agreement must specify the levels of exposure that both organizations are willing to tolerate
  - Security and technology consultants must be prescreened, escorted, and subjected to nondisclosure agreements
  - If the strategic partnership evolves into an integration of the systems of both companies, competing groups may be provided with information that neither parent organization expected
    - ✓ Nondisclosure agreements are an important part of any such collaborative effort
  - Security level of both systems must be examined before any physical integration takes place
    - ✓ A vulnerability on one system becomes vulnerability for all linked systems

Law & Ethics in InfoSec

- **Laws:** are rules adopted and enforced by governments to codify expected behavior in modern society
- **Ethics:** acceptable behaviors that conform to the widely held principles of the members of that society



- Laws are largely drawn from the ethics of a culture.
- Law carries the sanction of a governing authority and ethics do not.
- Ethics are based on cultural mores.

InfoSec and the Law

- InfoSec professionals and managers must possess a rudimentary grasp of the legal framework within which their organizations operate.
- The US has led the development & implementation of InfoSec legislation, including:
  - Computer Fraud and Abuse (CFA) Act of 1986
  - Computer Security Act (CSA) of 1987
  - Federal Privacy Act of 1974
  - Electronic Communications Privacy Act (ECPA) of 1986
  - Health Insurance Portability and Accountability Act (HIPAA) of 1996

- International laws and legal bodies
  - European Council Cybercrime Convention
  - Digital Millennium Copyright Act (DMCA)
  - Australian High Tech Crime

Deterring Unethical and Illegal Behavior

- It is the responsibility of InfoSec personnel to deter unethical and illegal acts
- Three general categories of unethical behavior: ignorance, accident, intent
- Deterrence is the best method for preventing an illegal or unethical activity.
- Laws and policies and their associated penalties only deter if three conditions are present:
  - Fear of penalty
  - Probability of being caught
  - Probability of penalty being administered

Codes of Ethics

- A number of professional organizations have established codes of conduct and/or codes of ethics that members are expected to follow: ACM, $(ISC)^2$, SANS, ISACA, ISSA.

- Codes of ethics can have a positive effect on an individual's judgment regarding computer use.

- It is the individual responsibility of security professionals to act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society.