Upon completion of this chapter, you should be able to:

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

- InfoSec department must 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
Staffing the Security Function

- Security technical and managerial skills face supply and demand cycles

To move the InfoSec discipline forward:

- General mgmt should learn qualifications for information security positions and IT positions
- Upper mgmt should learn more about information security budgetary and personnel needs
- IT and general mgmt must grant information security function (and CISO) an appropriate level of influence and prestige
Qualifications and Requirements

- 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 in general, including users, and communicate effectively using both strong written and verbal communication skills
- Acknowledge the role of policy in guiding security efforts
- Understand the essential role of information security education and training, which helps make users part of the solution, rather than part of the problem
Qualifications and Requirements (Continued)

- Perceive the threats facing an organization, understand how these threats can become transformed into attacks, and safeguard the organization from information security attacks

- Understand how technical controls can be applied to solve specific information security problems

- Demonstrate familiarity with the mainstream information technologies, including Disk Operating System (DOS), Windows NT/2000, Linux, and UNIX

- Understand IT and InfoSec terminology and concepts
Entering the Information Security Profession

- Many information security professionals enter the field after having prior careers in law enforcement or the military, or careers in other IT areas, such as networking, programming, database administration, or systems administration.

- Organizations can foster greater professionalism in the information security discipline by clearly defining their expectations and establishing explicit position descriptions.
Figure 10-1
Information Security Career Paths

Traditional Career Path to InfoSec
Military/Law enforcement → Information security → Technology

Modern Career Path to InfoSec
Security education → Information security
Figure 10-2
Information Security Positions and Relationships

Information Assurance Management

Chief information security officer

Security consultant

Security manager

Security technician

Security administrator

Security officer

Possible Information Security Positions and Reporting Relationships
Chief information Security Officer (CISO)

- CISO is typically considered the top information security officer in the organization, although the CISO is usually not an executive-level position and frequently reports to the CIO.

- Although these individuals are business managers first and technologists second, they must be conversant in all areas of information security, including technology, planning, and policy.
CISO: Qualifications and Position Requirements

- Most common qualification for the CISO is the Certified Information Systems Security Professional (CISSP)

- Graduate degree in criminal justice, business, technology, or another related field is usually required as well

- Candidate for this position should have experience as a security manager, as well as in planning, policy, and budgets
Job Competencies for the CISO (1)

Provides organization information security oversight:

- Maintains current and appropriate body of knowledge necessary to perform information security management function
- Effectively applies information security management knowledge to enhance security of open network and associated systems and services
- Maintains working knowledge of external legislative and regulatory initiatives
- Interprets and translates requirements for implementation
- Develops appropriate information security policies, standards, guidelines, and procedures
- Works effectively with other organization information security personnel and the committee process
Job Competencies for the CISO (2)

Provides organization information security oversight (Continued):

- Provides meaningful input, prepares effective presentations, and communicates information security objectives
- Participates in short- and long-term planning
- Monitors information security program compliance and effectiveness
- Works with committees and management professionals to accomplish information security goals
- Coordinates and prioritizes activities of the Office of Information Security in support of the mission
- Acts as a resource for matters of information security
- Provides pertinent and useful information
Job Competencies for the CISO (3)

Provides organization information security oversight (Continued):

- Oversees and conducts information security reviews and liaison visits to organization [system practices]
- Makes recommendations and reports to Regional Practice Administration
- Coordinates and performs reviews of contracts, projects, and proposals
- Assists information technology proponents with standards compliance
- Conducts investigations of information security violations and computer crimes. Works effectively with management and external law enforcement to resolve these instances
- Reviews instances of noncompliance and works effectively and tactfully to correct deficiencies
Job Competencies for the CISO (4)

Manages Office of Information Security personnel

- Determines positions and personnel necessary to accomplish information security goals
- Requests positions, screens personnel, and takes the lead in the interviewing and hiring process
- Develops meaningful job descriptions
- Communicates expectations and actively coaches personnel for success
- Prioritizes and assigns tasks
- Reviews work performed
Job Competencies for the CISO (5) (Continued)

Manages Office of Information Security personnel

- Challenges staff to better themselves and advance the level of service provided
- Provides meaningful feedback to staff on an ongoing basis and formally appraises performance annually
Security Manager

- Security managers are accountable for the day-to-day operation of information security program
- They accomplish objectives identified by the CISO and resolve issues identified by the technicians
- Security managers are often assigned specific managerial duties by the CISO, including policy development, risk assessment, contingency planning, and operational and tactical planning for the security function
- Management of technology requires an understanding of the technology administered, but not necessarily proficiency in its configuration, operation, or fault resolution
Security Manager Qualifications and Position Requirements

- Not uncommon for a security manager to have a CISSP
- These individuals must have experience in traditional business activities, including budgeting, project management, personnel management, and hiring and firing, and they must be able to draft middle- and lower-level policies as well as standards and guidelines
- Several types of information security managers exist, and the people who fill these roles tend to be much more specialized than CISOs
Security Technician

- Security technicians are technically qualified individuals who
  - Configure firewalls and IDSs
  - Implement security software
  - Diagnose and troubleshoot problems
  - Coordinate with systems and network administrators to ensure that security technology is properly implemented
Technician Qualifications and Position Requirements

- Technical qualifications and position requirements for a security technician vary
  - Organizations typically prefer expert, certified, proficient technicians

- Job requirements usually include some level of experience with a particular hardware and software package

- Sometimes familiarity with a particular technology is enough to secure an applicant an interview
  - However, experience using the technology is usually required
Information Security
Professional Credentials
Information Security Professional Credentials

- Many organizations rely to some extent on recognizable professional certifications to ascertain the level of proficiency possessed by any given candidate

- Many of the certification programs are relatively new
  - Precise value is not fully understood by most hiring organizations

- Certifying bodies work diligently to educate their constituent communities on the value and qualifications of their certificate recipients

- Employers struggle to match certifications to position requirements, while potential information security workers try to determine which certification programs will help them in the job market
Certified Information Systems Security Professional (CISSP)

- CISSP is considered most prestigious certification for security managers and CISOs
Systems Security Certified Practitioner (SSCP)

- SSCP certification is more applicable to security manager.
- SSCP focuses “on practices, roles and responsibilities as defined by experts from major IS industries” and covers seven domains:
  - Access controls
  - Administration
  - Audit and monitoring
  - Risk, response, and recovery
  - Cryptography
  - Data communications
  - Malicious code/malware
Global Information Assurance Certification (GIAC)

- SANS sponsors a technical security certification -- GIAC
- GIAC certifications can be pursued independently or combined to earn a comprehensive certification called GIAC Security Engineer (GSE)
- The individual GIAC certifications are:
  - GIAC Security Essentials Certification (GSEC)
  - GIAC Certified Firewall Analyst (GCFW)
  - GIAC Certified Intrusion Analyst (GCIA)
  - GIAC Certified Incident Handler (GCIH)
  - GIAC Certified Windows Security Administrator (GCWN)
  - GIAC Certified UNIX Security Administrator (GCUX)
  - GIAC Information Security Officer—Basic (GISO–Basic)
  - GIAC Systems and Network Auditor (GSNA)
  - GIAC Certified Forensic Analyst (GCFA)
  - GIAC Security Leadership Certificate (GSLC)
Security Certified Program (SCP)

- SCP offers two tracks: Security Certified Network Professional (SCNP) and the Security Certified Network Architect (SCNA)
- Both designed for the security technician
- The SCNP track targets firewalls and intrusion detection, and requires two exams:
  - Network Security Fundamentals (NSF)
  - Network Defense and Countermeasures (NDC)
- The SCNA program includes authentication areas, including biometrics and PKI, and requires two certification exams:
  - PKI and Biometrics Concepts and Planning (PBC)
  - PKI and Biometrics Implementation (PBI)
TruSecure ICSA Certified Security Associate (TICSA)
- “Complementary to CISSP, as a stepping stone toward higher-level security management”

TruSecure ICSA Certified Security Expert (TICSE)
Security+

- CompTIA certification tests for security knowledge mastery of an individual with two years on-the-job networking experience

- Exam covers industry-wide topics including:
  1. General Security Concepts
  2. Communication Security
  3. Infrastructure Security
  4. Basics of Cryptography
  5. Operational/Organizational Security
Certified Information Systems Auditor (CISA)

- Information Systems Audit and Control Association and Foundation (ISACA) touts the CISA as being appropriate for auditing, networking, and security professionals.
Certified Information Security Manager (CISM)

- Geared toward experienced information security managers
- Can assure executive management that a candidate has required background knowledge needed for effective security management and consulting
- Exam covers:
  - Information Security Governance
  - Risk Management
  - Information Security Program Management
  - Information Security Management
  - Response Management
Certified Information Forensics Investigator (CIFI)

- Under development by Information Security Forensics Association
- Will evaluate expertise of those who work with law enforcement, and auditing
Certification Costs

- Certifications can be expensive
- Most experienced professionals find it difficult to do well on them without at least some review
- Most programs require between two and three years of work experience
  - Often structured to reward candidates who have significant hands-on experience
Figure 10-3
Approaches to Prepare for Certification

Information Assurance Management

Self-study guides → Certification

Mentors and study partners → Certification

Work experience → Certification

Training media → Certification

Formal training programs → Certification

FIGURE 10-3 Preparing for Security Certification
Employment Policies and Practices

- General management community of interest should integrate solid information security concepts across 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 information security more seriously.
Hiring

- From information security perspective, hiring of employees is laden with potential security pitfalls.

- CISO, in cooperation with CIO and relevant information security managers, should establish a dialogue with human resources personnel so that information security considerations become part of the hiring process.
Hiring Issues

- **Job Descriptions** - Organizations that provide complete job descriptions when advertising open positions should omit elements of the job description that describe access privileges.

- **Interviews** - Information security should advise HR to limit information provided to candidates on access rights of the position.
  - When an interview includes a site visit, tour should avoid secure and restricted sites → visitor could observe enough information about the operations or information security functions to represent a potential threat to the organization.
Hiring Issues (Continued)

- **New Hire Orientation** - New employees should receive, as part of their orientation, an extensive information security briefing.

- **On-the-Job Security Training** - Organizations should conduct periodic security awareness and training activities to keep security at the forefront of employees’ minds and minimize employee mistakes.

- **Security Checks** - Background check should be conducted before organization extends an offer to any candidate, regardless of job level.
Common Background Checks

- **Identity checks**: Personal identity validation
- **Education and credential checks**: Institutions attended, degrees and certifications earned, and certification status
- **Previous employment verification**: Where candidates worked, why they left, what they did, and for how long
- **Reference checks**: Validity of references and integrity of reference sources
- **Worker’s compensation history**: Claims from worker’s compensation
Common Background Checks (Continued)

- Motor vehicle records: driving records, suspensions, and other items noted in the applicant’s public record
- Drug history: drug screening and drug usage, past and present
- Medical history: current and previous medical conditions, usually associated with physical capability to perform the work in the specified position
- Credit history: credit problems, financial problems, and bankruptcy
- Civil court history: involvement as the plaintiff or defendant in civil suits
- Criminal court history: criminal background, arrests, convictions, and time served
Contracts and Employment

- Once a candidate has accepted a job offer, the employment contract becomes an important security instrument.

- It is important to have these contracts and agreements in place at the time of the hire.
Security as Part of Performance Evaluation

- To heighten information security awareness and change workplace behavior, organizations should incorporate information security components into employee performance evaluations.

- Employees pay close attention to job performance evaluations.
  - Including information security tasks in them will motivate employees to take more care when performing these tasks.
Termination Issues

- When an employee leaves an organization, the following tasks must be performed:
  - Access to organization’s systems must be disabled
  - Former employee must return all removable media
  - Former employee’s hard drives must be secured
  - File cabinet locks must be changed
  - Office door locks must be changed
  - Former employee’s keycard access must be revoked
Termination Issues (Continued)

- Former employee’s personal effects must be removed from the premises.
- Former employee should be escorted from the premises, once keys, keycards, and other business property have been turned over.
- Exit interview to remind employee of any contractual obligations, such as nondisclosure agreements, and to obtain feedback on the employee’s tenure in the organization.
- Two methods for handling employee outprocessing, depending on the employee’s reasons for leaving, are hostile and friendly departures.
Hostile Departure

- Security cuts off all logical and keycard access before employee is terminated
- Employee reports for work and is escorted into supervisor's office to receive bad news
- 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 under supervision
- Once personal property has been gathered, the employee is asked to surrender all keys, keycards, and other organizational identification and access devices, PDAs, pagers, cell phones, and all remaining company property, and is then escorted from the building
Friendly Departure

- Employee may have tendered notice well in advance of actual departure date which can make it much more difficult for security to maintain positive control over employee’s access and information usage

- Employee accounts are usually allowed to continue with a new expiration date

- Employee can come and go at will, usually collects any belongings and leaves without escort

- Employee is asked to drop off all organizational property before departing
Termination Issues Concluded

- 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.
- Possible that departing employees have collected and taken home information or assets that could be valuable in their future jobs.
- Only by scrutinizing system logs during transition period and after employee has departed, and sorting out authorized actions from system misuse or information theft, can the organization determine whether a breach of policy or a loss of information has occurred.
Personnel Security Practices

- There are various ways of monitoring and controlling employees to minimize their opportunities to misuse information
  - Separation of duties is used to make it difficult for an individual to violate information security and breach the confidentiality, integrity, or availability of information
  - Two-man control requires that two individuals review and approve each other’s work before the task is considered complete
**Figure 10-6**

Personnel Security Controls

Information Assurance Management
Personnel Security Practices (Continued)

- Job rotation
  - 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

Both job rotation and task rotation ensure that no one employee is performing actions that cannot be knowledgeably reviewed by another employee.

- For similar reasons, each employee should be required to take a mandatory vacation, of at least one week per year
Personnel Security Practices (Continued)

- Policy gives organization a chance to perform a detailed review of everyone’s work
- Finally, another important way to minimize opportunities for employee misuse information is to limit access to information
- Employees should be able to access only the information they need and only for the period required to perform their tasks
- This policy gives the organization a chance to perform a detailed review of everyone’s work
  - Principle of least privilege
Personnel Security Practices (Continued)

- Similar to the need-to-know concept, 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—possibly leading to losses in confidentiality, integrity, and availability—will occur.
Security of Personnel and Personal Data

- Organizations are required by law to protect sensitive or personal employee information, including personally identifying facts such as employee addresses, phone numbers, Social Security numbers, medical conditions, and even names and addresses of family members.

- This responsibility also extends to customers, patients, and anyone with whom the organization has business relationships.

- While personnel data is, in principle, no different than other data that information security is expected to protect, certainly more regulations cover its protection.

- As a result, information security procedures should ensure that this data receives at least the same level of protection as other important data in the organization.
Security Considerations for Non-employees

- 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

- Because temporary workers are not employed by the organization for which they are working, they may not be subject to contractual obligations or general policies that govern other employees.

- Unless specified in contract, temp agency may not be liable for losses caused by its workers.

- From a security standpoint, access to information for these individuals should be limited to what is necessary to perform their duties.
Contract Employees

- While professional contractors may require access to virtually 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 and out of buildings.

- In a secure facility, all service contractors are escorted from room to room and into and out of the facility.

- Any service agreements or contracts should contain the following regulations:
  - Facility requires 24 to 48 hours’ notice of a maintenance visit.
  - Facility requires all on-site personnel to undergo background checks.
  - Facility requires advance notice for cancellation or rescheduling of a maintenance visit.
Consultants

- Consultants have their own security requirements and contractual obligations.

- Should be handled like contract employees, with special requirements, such as information or facility access requirements, being integrated into the contract before they are given free access to the facility.

- In particular, security and technology consultants must be prescreened, escorted, and subjected to nondisclosure agreements to protect the organization from intentional or accidental breaches of confidentiality.

- Just because you pay security consultants, it doesn’t mean that protecting your information is their number one priority.

- Always remember to apply the principle of least privilege when working with consultants.
In summary

- Introduction
- Staffing the Security Function
- Information Security Professional Credentials
- Employment Policies and Practices
Thank You!

Dr. Nattavee Utakrit