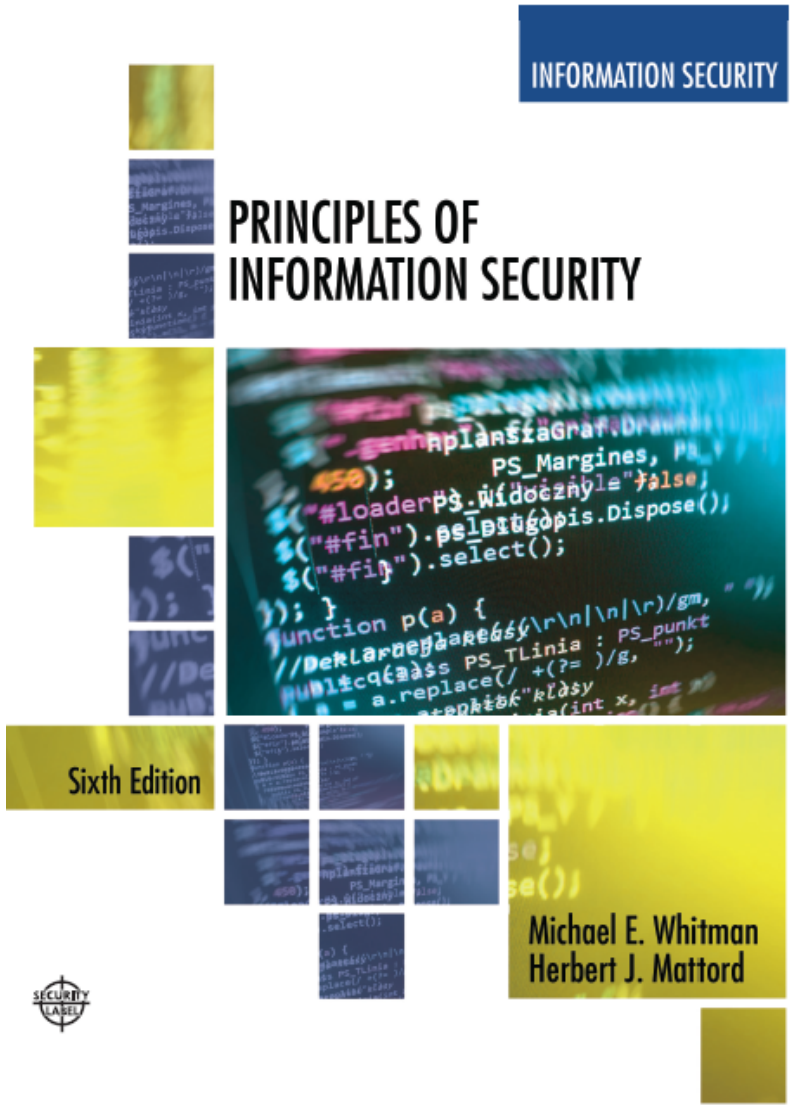


Source: Principles of Information Security

Chapter 11

Security and Personnel

Dr. Ibrahim Waziri Jr.

Learning Objectives

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

- Describe where and how the information security function should be positioned within organizations
- Explain the issues and concerns related to staffing the information security function
- List and describe the credentials that information security professionals can earn to gain recognition in the field
- Discuss how an organization's employment policies and practices can support the information security effort
- Identify the special security precautions that must be taken when using contract workers
- Explain the need for the separation of duties
- Describe the special requirements needed to ensure the privacy of personnel data

Introduction

When implementing information security, there are many human resource issues that must be addressed.

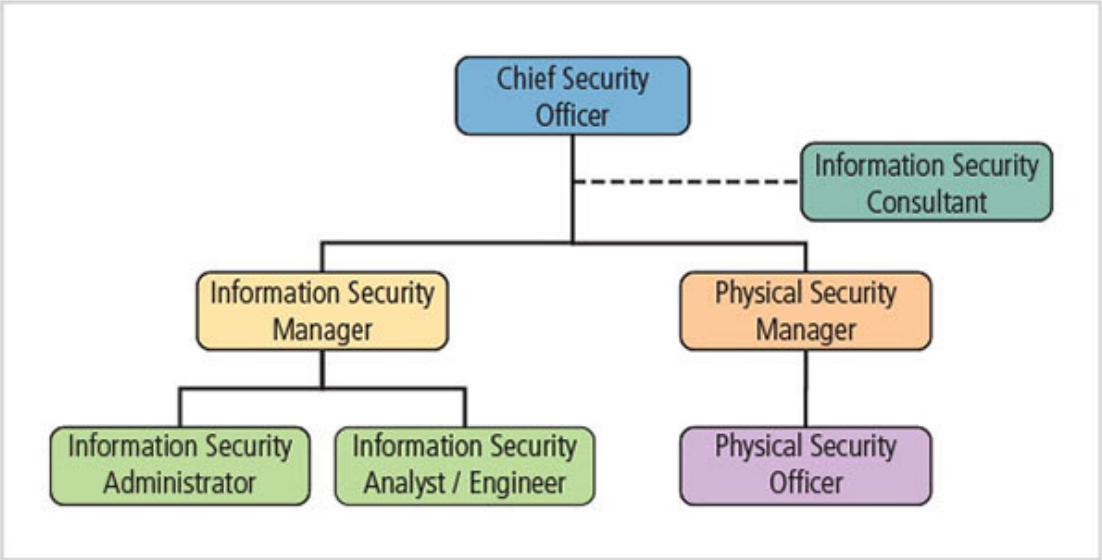
- Positioning and naming the security function
- Staffing for or adjustments to the staffing plan
- Assessing the impact of information security on every IT function
- Integrating solid information security concepts into personnel management practices

Employees often feel threatened when an information security program is being created or enhanced.

Positioning and Staffing the Security Function

- The security function can be placed within:
  - IT function
  - Physical security function
  - Administrative services function
  - Insurance and risk management function
  - Legal department
- **Staffing the Security Function**
  - Qualifications and requirements
  - Entry into the information security profession
  - Information security positions

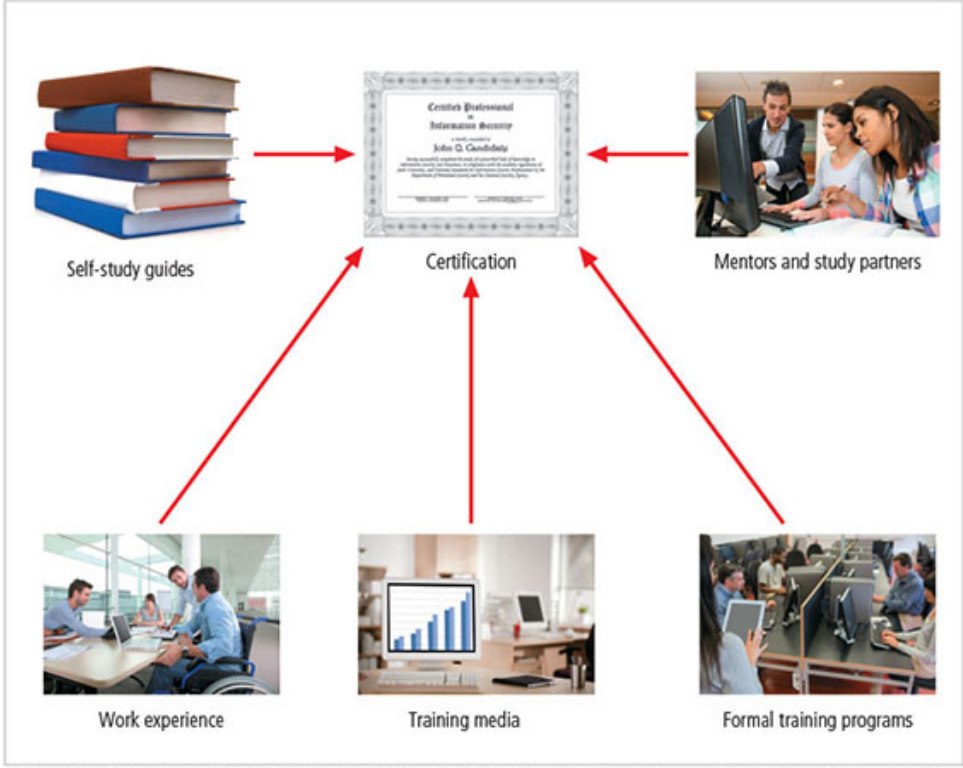
Information Security Positions



- Chief information security officer (CISO)
  - Top information security officer; frequently reports to chief information officer (CIO)
- Chief security officer (CSO)
  - CISO's position may be combined with physical security responsibilities
- Security manager
  - Accountable for day-to-day operation of information security program
- Security technician
  - Technically qualified employees tasked to configure security hardware and software

Information Security Certifications

Many organizations seek industry-recognized certifications.



- (ISC)^2 Certifications: CISSP, SSCP, CSSLP, CCFP, HCISPP, CCSP
  - CISSP Concentrations: ISSAP, ISSEP, ISSMP
- ISACA Certifications: CISM, CISA, CGEIT, CRISC
- SANS Global Information Assurance Certification (GIAC)
- EC Council Certified CISO (ClCISO)
- CompTIA's Security+
- Certified Computer Examiner (CCE)

Resource: https://www.cyberseek.org/

Employment Policies and Practices

An organization should make information security a documented part of every employee's job description.

Management community of interest should integrate solid concepts for information security into the organization's employment policies and practices.

Considerations:

- Job Descriptions
- Interviews
- Background Checks
- Employment Contracts
- New Hire Orientation
- On-the-job security training
- Performance Evaluation
- Termination

Security Considerations for Temporary Employees, Consultants, and Other Workers

Individuals not subject to screening, contractual obligations, and eventual secured termination often have access to sensitive organizational information.

Relationships with these individuals should be carefully managed to prevent possible information leak or theft.

- Temporary Employees
- Contract Employees
- Consultants
- Business Partners

Internal Control Strategies

- Separation of duties
- Two-man control
- Job rotation
- Garden leave

In some organizations, employees are required to sign a covenant not to compete (CNC) or non-compete clause (NCC), which prevents them from working for a direct competitor within a specified time frame.

- Need-to-know
- Least privilege

Privacy and the Security of Personnel Data

- Organizations required by law to protect sensitive or personal employee information.
- Includes employee addresses, phone numbers, Social Security numbers, medical conditions, and family names and addresses.
- Information security groups should ensure these data receive at least the same level of protection as other important organization data.

Summary

- Positioning the information security function within organizations
- Issues and concerns about staffing information security
- Professional credentials of information security professionals
- Organizational employment policies and practices related to successful information security
- Special security precautions for nonemployees
- Separation of duties
- Special requirements needed for the privacy of personnel data