FINAL PRESENTATION – MANAGEMENT OF INFORMATION SECURITY

BY KEVIN SWAN

CHAPTER 1: INTRODUCTION TO THE MANAGEMENT OF INFORMATION SECURITY

- What is information security?
  - Protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology
  - Specialized areas of security: Physical, operations, communications, cyber, and network security
- The C.I.A. triad is based on three desirable characteristics of information: confidentiality, integrity, and availability
- General management vs. information security management
- Chapter goes over threats facing an organization, (ex: human error, compromises to intellectual property, theft, software attacks, or espionage)
- Leader vs manager: a leader influences employees so that they are willing to accomplish objectives, whereas a manager creates budgets, authorizes expenditures, and hires employees

CHAPTER 2: COMPLIANCE: LAW AND ETHICS

Law vs. Policy

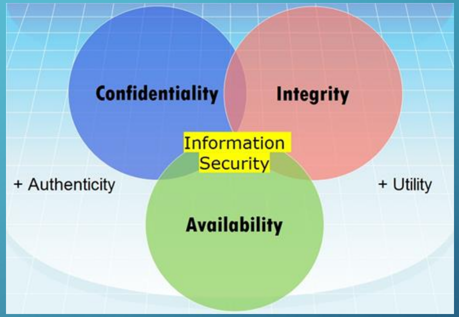
- Categories of Law: Constitutional, statutory, regulatory, common, civil, criminal
- Discusses differences between policy and law
- Ethics: the branch of philosophy that considers nature, criteria, sources, logic, and the validity of moral judgment
- Frameworks of ethics: Normative, meta-ethics, descriptive, applied, deontological
- Covers law enforcement agencies

CHAPTER 3: GOVERNANCE AND STRATEGIC PLANNING FOR SECURITY

- Discusses planning in business management and groups associated with it such as stakeholders
- Strategic planning is when an organization defines their long-term direction (contingency plan covered in ch. 10)
- Goes over different industry frameworks such as NCSP
- Introduces security systems development life cycle
- Provides precise descriptions of role involved in InfoSec such as the CIO, CSO, CISO, etc.
- Systems development life cycles
  - Security systems development life cycle (SecSDLC): a methodology for the design and implementation of an information system

CHAPTER 4: INFORMATION SECURITY POLICY

- I learned about InfoSec policy and how to write, implement, and maintain it. These policies are written instructions from management that inform employees about the proper behavior they should display regarding the use of information and information assets



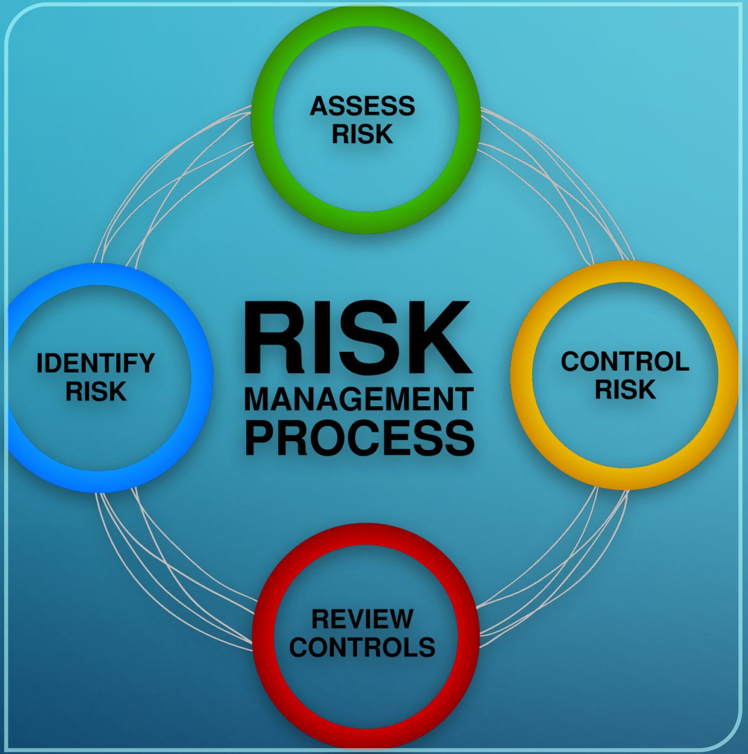
- A InfoSec policy must satisfy several criteria:
  - Policy should never conflict with law
  - Policy must stand up in court when it is challenged
  - Policy must be properly supported and administered
- Three types of InfoSec policy: Enterprise information security policy, issue-specific security policies, and system-specific information security policies

CHAPTER 5: DEVELOPING THE SECURITY PROGRAM

- Information security program: The entire set of activities, resources, personnel, and technologies used by an organization to manage the risks to its information assets
- Four areas of InfoSec functions:
  - Functions performed by nontechnical areas of the organization
  - Functions performed by IT groups
  - Functions performed within the InfoSec department as a customer service
  - Functions performed within the InfoSec department as a compliance enforcement obligation
- Chapter also discusses components of a security education, training, and awareness programs
- Implementation of full-time security personnel within an organization depends on the organization's size

Security Training

CHAPTER 6: RISK MANAGEMENT: IDENTIFYING AND ASSESSING RISK

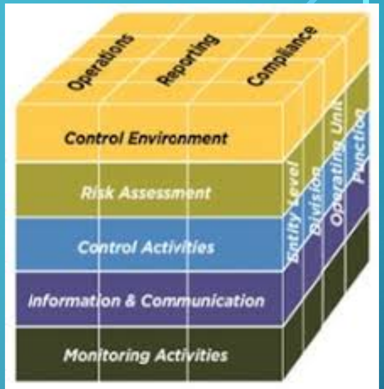


- Risk management: The process of identifying risk, assessing its relative magnitude, and taking steps to reduce it to an acceptable level
- Risk management strategy key components: identification, classification, and prioritization of the organization’s information assets
- Risk identification is the recognition, enumeration, and documentation of risks to an organization’s information assets
- Risks must also be assessed. Risk assessment is a determination of the extent to which an organization’s information assets are exposed to risk
- Risks should also be controlled, as will be seen in the next chapter

CHAPTER 7: RISK MANAGEMENT: CONTROLLING RISK

- Process of controlling a vulnerability:
  - Risk identified -> risk ranked -> strategy to control risk is chosen
  - Strategies to control risk include defense, transference, mitigation, acceptance, and termination
  - Once a control strategy is implemented, the effectiveness of controls should be monitored and measured
- Cost-benefit analysis can determine whether a control alternative is worth the cost that comes with it
- Alternatives to risk management: OCTAVE Method, FAIR, etc.

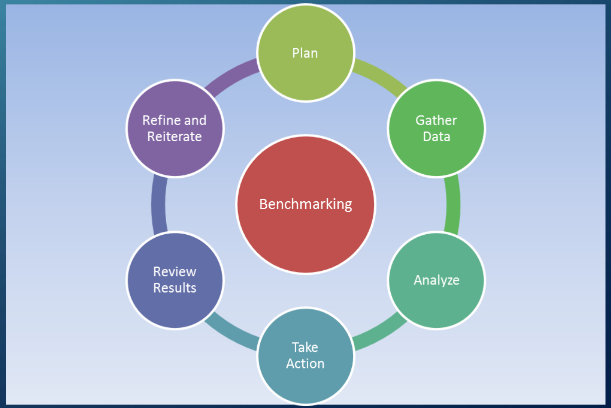
CHAPTER 8: SECURITY MANAGEMENT MODELS



- Frameworks are just the outline of a more thorough blueprint used in the creation of the InfoSec environment. Security models on the other hand are generic blueprints offered by a service organization
- One of the most widely referenced security models is "ISO/IEC 27001: 2005 Information Technology—Code of Practice for InfoSec Management"
- Access controls regulate the admission of users into trusted areas of the organization and are comprised of four elements: identification, authentication, authorization, and accountability
- Chapter also looks over COSO framework, NIST Security publications, and access control models

CHAPTER 9: SECURITY MANAGEMENT PRACTICES

- Security blueprints can be generated with a method known as benchmarking, where your organization follows the recommended practices of a similar organization
  - In most cases, organizations look for a technically qualified InfoSec generalist
- The two categories of benchmarks are standards of due diligence and recommended practices.
- Recommended business practices are efforts that seek to provide a superior level of performance in the protection of information
- Other concepts covered: InfoSec performance management, InfoSec performance measurements, accreditation, and certification



CHAPTER 10: PLANNING FOR CONTINGENCIES

- Contingency planning: the process by which the information technology and information security communities of interest position their organizations to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets, both human and artificial
- Contingency planning has four major components
  - Business impact analysis
  - Incident response plan
  - Disaster recovery plan
  - Business continuity plan

Probability and Impact
Description of Problem
CONTINGENCY PLAN
Scope of Contingency
Workaround of Problem

- Incident classification is process by which the IR team examines an incident candidate and determines whether it constitutes an actual incident
  - It uses three categories of incident indicators: possible, probable, and definite

CHAPTER 11: PERSONNEL AND SECURITY

- The hiring of InfoSec personnel is affected by a number of factors, among them the law of supply and demand
  - In most cases, organizations look for a technically qualified InfoSec generalist
- Many organizations rely on certifications to document the qualifications of current and/or prospective employees, recognizing that a professional association’s assessment of skills and knowledge is a valid way of assessing the quality of these individuals
  - From the closing case I learned that organizations have to be careful not to have any miscommunication between departments on the certifications they are looking for
- Management should integrate InfoSec concepts and practices into the organization’s employment activities

CHAPTER 12: PROTECTION MECHANISMS

- This chapter defines identification, authentication, authorization, and accountability and goes into depth of why they are important
- Firewalls play a key role in InfoSec programs as they prevent a specific type of information from moving between the outside world and the inside world
- Encryption is a protection mechanism that was looked at in the chapter as well as cryptosystems which can help to make e-mail or web browsers more secure