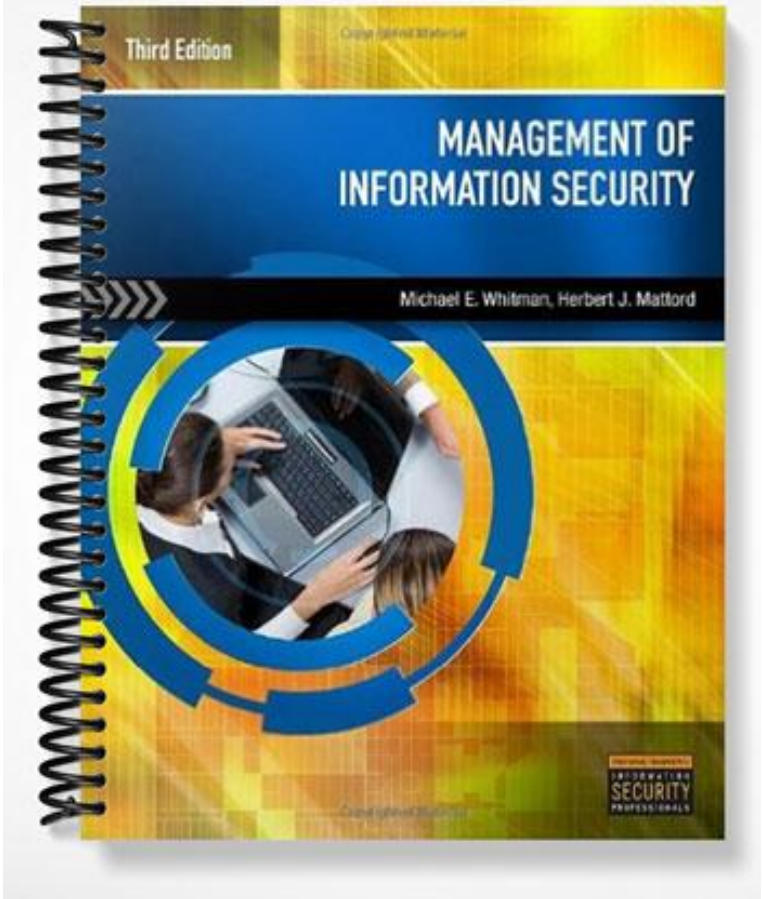
SOLUTIONS MANUAL



Management of Information Security, 3rd Edition

Chapter 2 – Planning for Security

Review Questions

1. Describe the essential parts of planning. How does the existence of resource constraints affect the need for planning?
   Answer: Planning is the preparation, application, and control of a sequence of action steps to achieve specific goals. Each organization must balance the benefits of the chosen planning effort against the cost of the effort.

2. What are the three common layers of planning? How do they differ?
   Answer: Tactical planning—Tactical planning has a shorter focus than strategic planning, usually one to three years and breaks down each applicable strategic goal into a series of incremental objectives. Strategic planning—the basis for long-term direction for the organization. Operational planning—includes clearly identified coordination activities across department boundaries, communications requirements, weekly meetings, summaries, progress reports, and associated tasks..

3. Who are the stakeholders? Why is it important to consider their views when planning?
   Answer: Stakeholders are people that will gain or lose (usually money) depending on the success or failure of the organization. Stakeholders provide a lot of the support for a business so they need to be consulted.

4. What is a mission statement? What is a vision statement? What is a values statement? Why are they important? What do they contain?
   Answer: The mission statement explicitly declares the business of the organization, as well as its intended areas of operations. The mission statement must explain what the organization does and for whom. The vision statement expresses what the organization wants to become. Vision statements should be ambitious; after all, they are meant to express the aspirations of the organization and to serve as a means for visualizing its future. Values statement is an established formal set of organized principles, standards and qualities as well as benchmarks for measuring behavior against published values. The values statement in an organization makes conduct and performance standards clear to its employees and the public.

5. What is strategy?
   Answer: Strategy is the basis for long-term direction for the organization. Strategy normally sets guidelines for organizations efforts and focuses resources toward specific clearly defined goals.

6. What is information security governance?
   Answer: Information security governance includes all of the accountabilities and methods undertaken by a board of directors and executive management to provide strategic direction, establishment of objectives, measurement of progress toward those objectives, verification that risk management practices are appropriate, and validation that the organization's assets are used properly.

7. What should a Board of Directors recommend as an organization's information security objectives?
   Answer: 1. Inculcating a culture that recognizes the criticality of information and information security to the organization 2. Verifying that management's investment in information security is properly aligned with organizational strategies and the organization's risk environment 3. Assuring that a comprehensive information security program is developed and implemented 4. Demanding reports from the various layers of management on the information security program's effectiveness and adequacy.

8. What are the five basic outcomes that should be achieved through information security governance?
   Answer: 1. Strategic alignment of information security with business strategy to support organizational objectives 2. Risk management by executing appropriate measures to manage and mitigate threats to information resources 3. Resource management by utilizing information security knowledge and infrastructure

efficiently and effectively 4. Performance measurement by measuring, monitoring, and reporting information security governance metrics to ensure that organizational objectives are achieved 5. Value delivery by optimizing information security investments in support of organizational objectives.

9. Describe top-down strategic planning. How does it differ from bottom-up strategic planning? Which is usually more effective in implementing security in a large, diverse organization?

Answer: Top down strategic planning involves high level managers providing resources and giving directions. Directors issue polices, procedures and processes and dictate the goals and expected outcomes of the project, and also determine whose is accountable for each of the required actions. In top-down planning managers give directions on how projects should be handled, while in bottom-up planning system administrators give directions on how on how projects should be handled. Of the two, top-down planning is the more effective security strategy, since it encompasses critical features such as coordination between departments, coordinated plans from top management, provision of sufficient resources, and support from end users.

10. How does the SecSDLC differ from the more general SDLC?

Answer: The SecSDLC is more closely aligned with risk management practices and involves extensive effort in identification of specific threats and risks and subsequent design and implementation of specific controls to counter those threats and assist in management of the risk, while SDLC involves the general methodology for design and implementation of an information system in an organization.

11. What is the primary objective of the SecSDLC? What are its major steps, and what are the major objectives of each step?

Answer: The SecSDLC involves the identification of specific threats and the risks that they represent, and the subsequent design and implementation of specific controls to counter those threats and assist in the management of the risk. The major steps and their objectives are:

- Investigation – Teams of managers, employees, and contractors are assembled to analyze problems, define their scope, specify goals, and objectives and identify any additional constraints not covered in the enterprise security policy.
- Analyze – The documents from the investigation phase are studied.
- Logical Design – The team members create and develop the blueprint for security, and examine and implement key policies that influence later decisions.
- Physical Design – Team members evaluate the technology needed to support the security blueprint, generate alternative solutions, and agree upon a final decision.
- Implementation – The security solutions are acquired, tested, implemented, and tested again.
- Maintenance – Information systems are constantly monitored, tested, modified, updated, and repaired. This is the most important phase.

12. What is a threat in the context of information security? How many categories of threats exist as presented in this chapter?

Answer: A threat is an object, person, or other entity that represents a constant danger to an asset. Twelve categories are listed: Acts of human error or failure, compromises to intellectual property, deliberate acts of espionage or trespass, deliberate acts of information extortion, deliberate acts of sabotage or vandalism, deliberate acts of theft, deliberate software attacks, forces of nature, deviations in quality of service from service providers, technical hardware failures or errors, technical software failures or errors, and technological obsolescence.

13. What is the difference between a threat and an attack?

Answer: An attack is a deliberate act that exploits a vulnerability; a threat is the danger that a system might be attacked.

14. How can a vulnerability be converted into an attack? What label would we give to the entity that performs this transformation?
Answer: A vulnerability can be converted into an attack by a threat agent if it is not addressed

15. What name is given to an attack that makes use of viruses and worms? What name is given to an attack that does not actually cause damage other than wasted time and resources?
Answer: (a) Malicious code (b) Hoax

16. What questions might be asked to help identify and classify information assets? Which is the most useful question in the list?
Answer:
1. Which information asset is the most critical to the success of the organization?
2. Which information asset generates the most revenue?
3. Which information asset generates the most profitability?
4. Which information asset would be the most expensive to replace?
5. Which information asset would be the most expensive to protect?
6. Which information asset would be the most embarrassing or cause the greatest liability if revealed?

The most important is a subjective response, but sound arguments can be made for numbers 2 and 3.

17. What name is given to the process of assigning a comparative risk rating to each specific information asset? What are the uses of such a rating?
Answer: Risk assessment is the name given to the process of assigning a comparative risk rating to each specific information asset. The rating is useful in gauging the relative risk introduced by each vulnerable information asset and allows us to make comparative ratings later in the risk control process.

18. What term is used to describe the provision of rules intended to protect the information assets of an organization?
Answer: Information policy is the term given for the provisioning of rules used to protect the information assets of an organization.

19. What term is used to describe the control measure that reduces security incidents among members of the organization by familiarizing them with relevant policies and practices in an ongoing manner?
Answer: Security education and training program (SETA).

20. What are the three categories of information security controls? How is each used to reduce risk for the organization?
Answer: The three categories of information security controls are managerial controls, operational controls, and technical controls. Managerial controls cover security processes that are designed by the strategic planners and performed by security administration of the organization. Operational controls address personnel security, physical security, the protection of production inputs and outputs, management functions and disaster recovery planning. Technical controls address the specifics of technology selection and acquisition of certain technical components, including logical access controls like identification, authentication, authorization, and accountability.

Exercises

1. Using a Web search engine, find an article from a reputable source published within the past six months that reports on the relative risk that comes from inside the organization as opposed to risk that comes from external sources. If the article notes that this relative risk is changing, how is it changing and to what does the article attribute the change?
   Answer: The solution to this exercise will be unique for each student and will vary over time.

2. Using a Web search engine, find five examples of corporate vision statements, corporate mission statements, and corporate goals. Do these examples express concern for the security of corporate information?
   Answer: The solution to this exercise will be unique for each student and will vary over time.

3. Search your institution's published documents, including its Web pages. Locate its mission statement, vision statement, and strategic goals. Identify any references to information security. Also look for any planning documents related to information security.
   Answer: The solution to this exercise will be unique for each student and will vary over time.

4. Using a Web browser, go to http://gocsi.com. Search for the link offering a free copy of the latest CSI/FBI study. Summarize the key points and bring your summary to class to discuss with your fellow students.
   Answer: The solution to this exercise will be unique for each student and will vary over time.

5. Go to the library and search through recent newspaper articles about your area. How many examples of threats to information security can you find in the last week??
   Answer: The solution to this exercise will be unique for each student and will vary over time.

Case Exercises

1. Create definitions of "Confidential," "Sensitive," and "Public" for RWW. Create a list of examples of documents that should be labeled with each classification.
   Answer: The solution to this exercise will be unique for each student and will vary over time.

2. Design a labeling scheme (cover sheet, stamp, or other scheme) to associate with this classification system.
   Answer: The solution to this exercise will be unique for each student and will vary over time.