

***Principles of Incident Response and Disaster
Recovery 3rd edition Whitman Solutions Manual***

SKU: 9780357508329-SOLUTIONS

Solution and Answer Guide

Whitman and Mattord, *Principles of Incident Response and Disaster Recovery* 3e, 2022,
ISBN 978-0357508329; Module 1: An Overview of Information Security and Risk Management

Table of Contents

End of Module Exercise Solutions.....	1
Discussion Questions and Solutions	1
Ethical Decision Making Questions and Solutions	1
Review Questions and Solutions	2
Real-World Exercises and Solutions	5
Grading Rubric.....	7

End of Module Exercise Solutions

Discussion Questions and Solutions

1. Look at the section and table in this module on the 12 categories of threats. Which of the categories best fits what is going on in the situation JJ described earlier in the opening scenario of this module?

Solution

This question could generate several different answers; the key point is not which category students

Review Questions and Solutions

1. What is information security?

Solution

Information security is an umbrella term for the many programs and activities that work to ensure the confidentiality, integrity, and availability of information used by organizations. This includes steps to ensure the protection of organizational information systems. Information security (InfoSec) is the protection of the confidentiality, integrity, and availability of information, whether in storage, during processing, or in transmission.

2. How is the CNSS model of information security organized?

Solution

The CNSS model is organized along three axes. The first represents whether the data is being stored, being processed, or in transit. The second axis represents the characteristics of confidentiality, integrity, and availability, which must be protected in each data mode. The third axis represents the controls that implement policy, technology, or education for each mode and characteristic.

3. What three principles are used to define the C.I.A. triad? Define each in the context in which it is used in information security.

Solution

C.I.A. represents confidentiality, integrity, and availability. Information has the characteristic of confidentiality when only the people with the rights and privileges to access it are able to do so. Information has integrity when it has not been exposed (while stored or transmitted) to corruption, damage, destruction, or other disruption of its authentic state; in other words, it is whole, complete, and uncorrupted. Finally, information has availability when authorized users—people or computer systems—are able to access it in the specified format without interference or obstruction.

7. What is a vulnerability in the context of information security?

Solution

A vulnerability is a weakness or fault in the mechanisms meant to protect information and information assets from attack or damage.

8. What is a loss in the context of information security?

Solution

A loss is a single instance of an information asset that suffers damage or destruction, unintended or unauthorized modification or disclosure, or denial of use. As a specific example, when an organization's information is stolen, it has suffered a loss.

9. What is intellectual property? Describe at least one threat to this type of asset.

Solution

Intellectual property (IP) consists of original ideas and inventions created, owned, and controlled by a particular person or organization. IP includes the representation of original ideas. Software piracy or copyright violations are threats to this type of asset.

10. What is an availability disruption? Pick a utility service provider and describe what might constitute a disruption.

Solution

An availability disruption

14. In general terms, what is policy?

Solution

A policy is a plan or course of action used by an organization to convey instructions from its senior management to those who make decisions, take actions, and perform other duties on behalf of the organization. Policies are organizational laws in that they dictate acceptable and unacceptable behavior within the context of the organization's culture.

15. What is an enterprise information security policy, and how is it used?

Solution

An enterprise information security policy (EISP), also known as a general security policy, IT security policy, or information security policy, is a policy based on and directly supportive of the mission, vision, and direction of the organization, and it sets the strategic direction, scope, and tone for all security efforts. It is an executive-level document usually drafted by, or in cooperation with, the chief information officer of the organization.

16. Why is shaping policy considered difficult?

Solution

It requires ongoing discipline by senior management to consistently maintain and apply policy.

17. What are standards? How are they different from policy?

Solution

22. What is risk management?

Solution

Risk management is the process of identifying and controlling the risks to an organization's information assets.

23. What are the two main parts of risk management?

Solution

Risk management consists of two major undertakings: risk identification and risk control.

24. Who is expected to be engaged in risk management activities in most organizations?

Solution

All management levels are engaged in risk management. Among the communities of interest, the general management of the organization must structure the IT and information security functions to lead a successful defense of the organization's information assets, which consist of information and data, hardware, software, procedures, and people.

25. What are the basic strategies used to control risk? Define each.

Solution

The five basic risk treatment strategies are:

Exercise 1-2

Visit your school's Web site and search for any information about a computer policy or Internet security policy used at your academic institution. Compare and contrast this policy with the ones discussed in this module. Are any sections missing? If so, which ones? Does the school's policy contain sections that are not described in this module? Why do you think those sections are included?

Solution

This exercise will yield varying answers based on which institution is being researched. The intent is to have students gain experience in considering policy elements from an idealistic and theoretical perspective, as in the textbook, and the ways they are used in actual practice.

Exercise 1-3

Go to <https://cve.mitre.org>. What type of site is this, and what information can it provide? Now, paste in the URL <https://cve.mitre.org/cve>, then click Search CVE List, and enter "Ransomware" in the search field. Click Search again. What information is provided? How would this be useful? Click on one of the named results. What additional information is provided? How could this be useful?

Solution

Mitre is a cross-industry information sharing site that provides common vulnerability and exposure information for historical and emerging topics. The CVE directory provides names and descriptions of active ransomware vulnerabilities and exposures.

Grading Rubric

Grading Rubric These grading criteria can be applied to open-ended discussion questions, ethical decision making questions, review questions, and real-world exercises.			
3 Exceeds Expectations	2 Meets Expectations	1 Needs Improvement	0 Inadequate
• Student demonstrates accurate understanding of the concept. • Student applies the concept appropriately. • Student uses sound critical analysis to develop an insightful and comprehensive response to the prompt.	• Student demonstrates accurate understanding of the concept. • Student applies the concept appropriately. • Student develops a complete response to the prompt.	• Student's response demonstrates a gap in understanding of the concept. • Student applies the concept incorrectly. • Student's response is poorly developed or incomplete.	• Student's response is missing or incomplete. • Student's response demonstrates a critical gap in understanding. • Student is unable to apply the concept.

Instructor Manual

Whitman and Mattord, Principles of Incident Response and Disaster Recovery, Third Edition, 2022, 978-0-357-508329; Module 1: An Overview of Information Security and Risk Management

Table of Contents

Purpose and Perspective of the Module	2
Cengage Supplements.....	2
List of Student Downloads.....	2
Module Objectives.....	2
Key Terms.....	3
What's New in This Module.....	11
Module Outline	11
Introduction.....	11
An Overview of Information Security	11
Key Information Security Concepts	12
The 12 Categories of Threats.....	12
The Role of Information Security Policy in Developing Contingency Plans	14
Key Policy Components	14
Types of InfoSec Policies.....	14
Guidelines for Effective Policy Development and Implementation	15
Overview of Risk Management.....	16
Knowing Yourself and Knowing Your Enemy	16
Risk Management and the RM Framework	16
The RM Process.....	16
Risk Treatment/Risk Control	

Purpose and Perspective of the Module

The purpose of this module is to provide a brief overview of the broad field of information security as well as the process of risk management.

Contingency planning is an important element of information security, but before management can plan for contingencies, it should have an overall strategic plan for information security in place, including risk management processes to guide the appropriate managerial and technical controls. This module serves as an overview of information security, with special consideration given to risk management and the role that contingency planning plays in both.

Cengage Supplements

The following product-level supplements provide additional information that may help you in preparing your course. They are available in the instructor resources.

- PowerPoint slides
- Cognero test bank
- MindTap assets to support the textbook
- This instructor's manual

List of Student Downloads

Students should download the following items from the Student Companion Center to complete the activities and assignments related to this module:

- Module 1 hands-on projects

Module Objectives

The following objectives are addressed in this module:

Key Terms

In order of use:

contingency planning The actions taken by senior management to specify the organization's efforts and actions if an adverse event becomes an incident or disaster. This planning includes incident response, disaster recovery, business continuity, and crisis management efforts, as well as preparatory business impact analysis.

security A state of being secure and free from danger or harm. Also, the actions taken to make someone or something secure.

information security (InfoSec) 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.

C.I.A. triad The industry standard for computer security since the development of the mainframe. The standard is based on three characteristics that describe the utility of information: confidentiality, integrity, and availability.

confidentiality An attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems.

integrity An attribute of information that describes how data is whole, complete, and uncorrupted.

loss In this context, a single instance of an information asset that suffers damage or destruction, unintended or unauthorized modification or disclosure, or denial of use.

risk The probability of an unwanted occurrence, such as an adverse event or loss.

subjects and objects of attack A computer can be either the subject of an attack—an agent entity used to conduct the attack—or the object of an attack: the target entity.

threat Any event or circumstance that has the potential to adversely affect operations and assets. The term *threat source* is commonly used interchangeably with the more generic term *threat*.

threat agent The specific instance or a component of a threat.

threat event An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.

threat source A category of objects, people, or other entities that represents the origin of danger to an asset—in other words, a category of threat agents.

vulnerability A potential weakness in an asset or its defensive control system(s).

hacker A person who accesses systems and information without authorization and often illegally.

expert hacker A hacker who uses an extensive knowledge of the inner workings of computer hardware and software to gain unauthorized access to systems and information. Also known as elite hackers, expert hackers often create automated exploits, scripts, and tools used by other hackers.

professional hacker A hacker who conducts attacks for personal financial benefit or for a crime organization or foreign government. Not to be confused with a penetration tester.

penetration tester An information security professional with authorization to attempt to gain system access in an effort to identify and recommend resolutions for vulnerabilities in those systems.

novice hackers Relatively unskilled hackers who use the work of expert hackers to perform attacks. Also known as neophytes, n00bs, or newbies. This category of hackers includes script kiddies and packet monkeys.

script kiddies Hackers of limited skill who use expertly written software to attack a system. Script kiddies are also known as skids, skiddies, or script bunnies.

packet monkeys Script kiddies who use automated exploits to engage in denial-of-service attacks.

phishing A form of social engineering in which the attacker provides what appears to be a legitimate communication (usually e-mail), but it contains hidden or embedded code that redirects the reply to a third-party site in an effort to extract personal or confidential information.

spear phishing Any highly targeted phishing attack.

pretexting A form of social engineering in which the attacker pretends to be an authority figure who needs information to confirm the target's identity, but the real object is to trick the target into revealing confidential information. Pretexting is commonly performed by telephone.

information extortion The act of an attacker or trusted insider who steals information from a computer system and demands compensation for its return or for an agreement not to disclose the information. Also known as cyberextortion.

ransomware Computer software specifically designed to identify and encrypt valuable information in a victim's system in order to extort payment for the key needed to unlock the encryption.

sextortion A spear-phishing and blackmail attack that demands payment to preclude the distribution of hacked recordings of the target visiting pornographic Web sites.

hacktivists Hackers who seek to interfere with or disrupt systems to protest the operations

back door A malware payload that provides access to a system by bypassing normal access controls. A back door is also an intentional access control bypass left by a system designer to facilitate development.

trap door See *back door*.

maintenance hook See *back door*.

denial-of-service (DoS) attack An attack that attempts to overwhelm a computer target's ability to handle incoming communications, prohibiting legitimate users from accessing those systems.

distributed denial-of-service (DDoS) attack A DoS attack in which a coordinated stream of requests is launched against a target from many locations at the same time using bots or zombies.

zombie See *bot*.

bot An abbreviation of *robot*, an automated software program that executes certain commands when it receives a specific input. See also *zombie*.

spam Unsolicited commercial e-mail, typically advertising transmitted in bulk.

packet sniffers Software programs or hardware appliances that can intercept, copy, and interpret

standards Detailed statements of what must be done to comply with the policy, sometimes viewed as the rules governing policy compliance. If the policy states that employees must “use strong passwords, frequently changed,” the standard might specify that the password “must be at least 10 characters, with at least one number, one uppercase letter, one lowercase letter, and one special character.”

procedures Step-by-step instructions designed to assist employees in following policies, standards, and guidelines. If the policy states to “use strong passwords, frequently changed,” the procedure might advise that “in order to change your password, first click on the Windows Start button, then....”

practices Examples of actions that illustrate compliance with policies. If the policy states to “use strong passwords, frequently changed,” the practices might advise that “according to X, most organizations require employees to change passwords at least semiannually.”

guidelines Nonmandatory recommendations the employee may use as a reference in complying with the policy. If the policy states to “use strong passwords, frequently changed,” the guidelines might advise that “we recommend you don’t use family or pet names, or parts of your Social Security number, employee number, or phone number in your password.”

enterprise information security policy (EISP) The high-level information security policy that sets the strategic direction, scope, and tone for all of an organization’s security efforts. An EISP is also known as a security program policy, general security policy, IT security policy, high-level InfoSec policy, or simply an InfoSec policy

risk treatment The selection of a strategy to address residual risk in an effort to bring it into alignment with the organization's risk appetite.

residual risk The risk to information assets that remains even after current controls have been applied.

risk appetite The quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility.

risk tolerance The assessment of the amount of risk an organization is willing to accept for a particular information asset, typically synthesized into the organization's overall risk appetite.

risk threshold See *risk tolerance*.

risk appetite statement A formal document developed by the organization that specifies its overall willingness to accept risk to its information assets, based on a synthesis of individual risk tolerances.

risk management plan A document that contains specifications for the implementation and conduct of RM efforts.

risk identification The recognition, enumeration, and documentation of risks to an organization's information assets.

information asset Within the context of risk management, any collection, set, or database of information

risk evaluation The process of comparing an information asset's risk rating to the numerical representation of the organization's risk appetite or risk threshold to determine if risk treatment is required.

risk control See *risk treatment*.

defense risk treatment strategy The risk treatment strategy that attempts to eliminate or reduce any remaining uncontrolled risk through the application of additional controls and safeguards in an effort to change the likelihood of a successful attack on an information asset. Also known as the *avoidance strategy*.

avoidance strategy See *defense risk treatment strategy*.

transference risk treatment strategy The risk treatment strategy that attempts to shift risk to other assets, other processes, or other organizations.

mitigation risk treatment strategy The risk treatment strategy that attempts to reduce the impact of the loss caused by an incident, disaster, or attack through effective contingency planning and preparation.

acceptance risk treatment strategy The risk treatment strategy that indicates the organization is willing to accept the current level of residual risk. As a result, the organization makes a conscious decision to do nothing else to protect an information asset from risk and to accept the outcome from any resulting exploitation.

termination risk treatment strategy The risk treatment strategy that

What's New in This Module

The following elements are improvements in this module from the previous edition:

- Additional material on risk management
- Revised definitions

[\[return to top\]](#)

Module Outline

Introduction

- I. Begin the course by explaining that this text is about being prepared for the unexpected and being ready for such events as incidents and disasters. We call this contingency planning, and the sad fact is that most organizations do not incorporate it into their day-to-day business activities.
- II. Discuss the effects that the September 11, 2001, attacks in New York, Pennsylvania, and Washington, D.C. had on contingency planning.
- III. Introduce the term *information security*.

Teaching Tip: Most people have never thought seriously about dealing with a major disaster. Pose these questions to students to raise their awareness of the need for disaster planning: If you knew that your company was going to burn to the ground tonight, what would you choose to take out of the building? Do you have an evacuation “hot list”? How long would it take before you could be up and running again in a new location?</

Teaching Tip: To learn more about the C.I.A. triad, visit

www.f5.com/labs/articles/education/what-is-the-cia-triad#:~:text=These%20three%20letters%20stand%20for,objectives%20for%20every%20security%20program.

Key Information Security Concepts

- I. Introduce the terms *threat*, *asset*, *attack*, *threat agent*, *vulnerability*, *exploit*, *control*, *safeguard*, and *countermeasure*.

Teaching Tip: Ask students to discuss how an employee might be considered a vulnerability.

The 12 Categories of Threats

- I. Use Table 1-1 to discuss the following threats to information security:
 - a. Esp

- h. Technical Hardware Failures or Errors—Point out that technical hardware failures or errors occur when a manufacturer distributes equipment containing a known or unknown flaw.
- i. Forces of Nature—Discuss why these threats are considered the most dangerous.

Teaching Tip: To read about lessons learned from the 2011 earthquake, tsunami, and nuclear disaster that devastated large parts of the area in and around Sendai, Japan, go to www.pkfindia.in/Value%20Adds/Lessons%20from%20the%20disasters%20in%20Japan.pdf.

- j. Deviations in Quality of Service by Service Providers—Note that Internet service, communication, and power irregularities can dramatically affect the availability of information and systems.

Teaching Tip: Ask students to discuss the impact that the total loss of telephone communications (both landlines and cell phones) would have on their school or company.

- k. Technological Obsolescence—Point out that IT professionals play a large role in the identification of obsolescence.
- l. Information Extortion—Note that extortion is common in credit card number theft.
- m. Some or All of the Previous Categories—Explain that in today's complex attack environment, most threats do not manifest as a simple effort by only

The Role of Information Security Policy in Developing Contingency Plans

- I. Emphasize that high-quality security programs begin and end with policy.

Teaching Tip: Without clearly defined and enforced policies in place, the effectiveness of a contingency plan will be seriously compromised. The organization also may be exposing itself to legal liabilities.

Key Policy Components

- I. Introduce the terms *policy*, *standards*, *procedures*, *practices*, and *guidelines*. Use Figure 1-3 to aid the discussion.

Types of InfoSec Policies

- I. To begin, note that there are three types of information security policies. Each is explained below.
- II. Explain that the enterprise information security policy (EISP) guides the development, implementation, and management of the security program. It contains the requirements to be met by the information security blueprint or framework.

Teaching Tip: Emphasize that policy must not only define actions and expectations, but must define the consequences of failure to

- b. Technical Specification SysSP—While a manager may work with a systems administrator to create managerial policy, the systems administrator may need to create a different type of policy to implement the managerial policy.

Guidelines for Effective Policy Development and Implementation

- I. Point out that policies are living documents that must be nurtured, given that they are constantly changing and growing. They must be properly developed, distributed, read, understood, agreed to, and uniformly applied.

Quick Quiz 2

- 1. True or False: Information security is primarily a technical problem, not a management issue.

Answer: False. Information security is more of a management problem than a technical issue.

- 2. _____ are examples of actions that illustrate compliance with policies.
 - a. Guidelines
 - b. Practices
 - c. Procedures
 - d. Standards

Answer: b. Practices

Overview of Risk Management

- I. Introduce the term *risk management (RM)*.
- II. Risk management involves discovering and understanding answers to some key questions about the risk associated with an organization's information assets:
 - a. Where and what is the risk (risk identification)?
 - b. How severe is the current level of risk (risk analysis)?
 - c. Is the current level of risk acceptable (risk evaluation)?
 - d. What do I need to do to bring the risk to an acceptable level (risk treatment)?

Teaching Tip: Without a formal approach to risk management, a company is highly likely to be unable to mitigate the impact of a major incident.

Knowing Yourself and Knowing Your Enemy

- I. Point out that just because you have a control in place to protect an asset does not necessarily mean that the asset is protected.
- II. Note that it is essential that all stakeholders conduct periodic asset inventories.

Teaching Tip: Point out the importance of including all departments within the company in this process, as people in different areas of activities will have unique insights into various aspects of threats and control strategies.

Risk Management and the RM Framework

II. List and briefly explain the following tasks of the RM process:

- a. Establishing the *context*, which includes understanding both the organization's internal and external operating environments and other factors that could impact the RM process.
- b. Identifying risk, which includes:
 - Creating an inventory of information assets (see Table 1-2 in the text)
 - Classifying and organizing those assets meaningfully
 - Assigning a value to each information asset
 - Prioritizing information assets
 - Assessing threats to the cataloged assets
 - Pinpointing vulnerable assets by tying specific threats to specific assets
 - Using a TVA worksheet
- c. Analyzing risk, which includes:
 - Determining the likelihood that vulnerable systems will be attacked by specific threats
 - Assessing the relative risk facing the organization's information assets so that risk management and control activities can focus on assets that require immediate attention
 - Calculating the risks to which assets are exposed in their current setting
 - Looking in a general way at controls that might come into play for identified vulnerabilities and ways to control the risks that the assets face
 - Documenting and reporting the findings of risk identification and assessment
- d. Evaluating the risk to the organization's key assets and comparing identified uncontrolled risks against its risk appetite
 - Identifying individual risk tolerances for each information asset
 - Combining or synthesizing individual risk tolerances into a coherent risk appetite statement
- e. Treating the unacceptable risk
- f. Summarizing the findings

Risk Treatment/Risk Control

- I. Explain that once the project team for information security development has identified information assets with unacceptable levels of risk, it must choose one of the following five approaches for controlling those risks:
 - a. Defense—Note that there are three common methods of risk defense: defense through application of policy, defense through application of training and education programs, and defense through implementation of technology.
 - b. Transference—This approach attempts to shift the risk to other assets, other processes, or other organizations.
 - c. Mitigation—This approach attempts to reduce the impact of an incident or disaster through planning and preparation.
 - d. Acceptance—This approach chooses to do nothing to protect the information asset. Instead, it accepts the outcome of potential exploitation.
 - e. Termination—The asset is removed from the operating environment; the cost of protecting an asset sometimes outweighs its value.

Quick Quiz 3

1. _____ is the recognition, enumeration, and documentation of risks to an organization's information assets.

Answer: Risk identification

2. _____ is the selection of a strategy to address residual risk in an effort to bring it into alignment with the organization's risk appetite.

Discussion Questions

You can assign these questions in several ways: in a discussion forum in your LMS, as whole-class discussions in person, or as a partner or group activity in class.

These questions are separate from the review questions and exercises in the textbook. For answers to the textbook questions, see the associated solutions for this module.

Additional class discussion options:

1. Does your company or school have a current disaster recovery plan? What are some of the activities involved in it? Do you feel confident that your company or school is prepared to survive a major disaster? Why or why not?
2. Has your company or school been the target of a network or system intrusion? What information was targeted? Was the attack successful? If so, what changes has your company or school made to ensure that this vulnerability has been controlled?

[\[return to top\]](#)

Suggested Usage for Lab Activities

Please see the associated hands-on activities for this module.

[\[return to top\]](#)

Additional Activities and Assign

Additional Resources

Cengage Video Resources

- MindTap Videos:
 - [list]

Internet Resources

- Discussion of the causes of the Chernobyl nuclear reactor disaster:
www.pbs.org/wgbh/pages/frontline/shows/reaction/readings/chernobyl.html
- Cyberterrorism: [www.huffingtonpost.com/dorian-de-wind/cyberterrorism-a-grave b 2867430.html](http://www.huffingtonpost.com/dorian-de-wind/cyberterrorism-a-grave-b-2867430.html)
- Cyberterrorism: http://doras.dcu.ie/501/1/cybert_hype_reality_2007.pdf
- More links are available in the Teaching Tips shown earlier in this document.

[\[return to top\]](#)