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

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 choose, but how they approach the issues. For example, the situation referenced in the opening scenario could potentially fall under the Theft threat category or Sabotage or espionage, depending on the intent. The discussion of threat categories is more theoretical, whereas the situation in the scenario is a potential attack via network connectivity. See the section in the text titled "Some or all of the above" on page 12.

2. How does the exchange between JJ and Paul earlier in this module indicate that this company has thought about contingency planning?

Solution

There is an incident response plan that Paul thinks will cover this issue.

Ethical Decision Making Questions and Solutions

1. Should JJ push the issue or initiate the event review process himself?

Solution

The plan and policy of the company should not be dependent on any one person's reaction or response. Proper responses are detailed in the plan.

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.

4. What is a threat in the context of information security?

Solution

A threat is a category of objects, people, or other entities that pose a potential risk of loss to an asset.

5. What is an asset in the context of information security?

Solution

An asset is an organizational resource that has value and thus needs to be protected.

6. What is an attack in the context of information security?

Solution

An attack is an intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.

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 is a reduced level of service in an element of the critical infrastructure. An example might be a utility that fails to deliver electrical power to its subscribers in a blackout.

11. What is a hacker and what are terms used to describe their skill levels?

Solution

A hacker is a person who accesses systems and information without authorization and often illegally. Most hackers are grouped into two general categories—the expert hacker and the novice hacker.

12. How does a brute force password attack differ from a dictionary password attack?

Solution

In a brute force password attack, the attacker attempts to guess a password by trying every possible combination of characters and numbers in it. In a dictionary password attack, the attacker narrows the range of possible passwords by using a list of common passwords and possibly including attempts based on the target's personal information.

13. What is phishing, and how is spear phishing different?

Solution

Phishing is 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 may lead to a data loss. When a phishing attack is specifically targeted at one person or a few people, it is called spear phishing.

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

More detailed than policy, standards state what must be done to comply with policy.

18. What is an issue-specific security policy?

Solution

An issue-specific security policy (ISSP) addresses specific areas of technology and contains a statement about the organization's position on a specific issue. It requires frequent updates.

19. List the critical areas covered in an issue-specific security policy.

Solution

The critical elements of an ISSP are a statement of policy, authorized access and usage of equipment, prohibited usage of equipment, systems management, violations of policy, policy review and modification, and limitations of liability.

20. What is a systems-specific security policy?

Solution

Systems-specific security policies (SysSPs) are detailed policies that may resemble or include standards and procedures.

21. When is a systems-specific security policy used?

Solution

SysSPs are often used when specifying the configuration or maintenance of systems.

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:

- *Defense—Apply safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability.*
- *Transference—Shift the risk to other areas or to outside entities.*
- *Mitigation—Reduce the impact should the vulnerability be exploited.*
- *Acceptance—Determine the potential consequences and accept the risk without control or mitigation.*
- *Termination—Remove the information asset from the environment that represents a risk to its security.*

Real-World Exercises and Solutions

Exercise 1-1

Go to *www.symantec.com/security-center/threat-report*, then download and review the latest Internet Security Threat Report. According to the report, what threats are currently the most dangerous? Which of these top threats represent problems for you and your use of the Internet? Which of these top threats represent problems for your school or business?

Solution

This exercise will yield varying answers over time, as this is a dynamic report. The intent is to have students gain experience in maintaining situational awareness and practicing critical thinking skills. See the grading rubric provided at the end of this document for scoring guidance.

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.

Exercise 1-4

Open a Web browser and search for the "OWASP Top Ten." Visit the site. What information is provided here? What does it mean? How could a security manager use this information?

Solution

This site offers a broad consensus view of the dominant risk elements in Web application programming. The utility of the site is its ongoing improvements in software assurance and software quality improvement programs.

Exercise 1-5

Open a Web browser and search for "NIST Computer Security Resource Center." Link to the home page. Click the Publications link, then click on the "SP NIST Special Publications" option. Locate SP 800-100. Review the HTML version. What critical information could a security administrator or manager gain from this document? What other documents would be of value to the security manager or technician?

Solution

This document provides a broad overview of the elements of an information security program and assists managers in understanding how to establish and implement an information security program.

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	• Student demonstrates	• Student's response demonstrates a gap	• Student's response is missing or

of the concept. • Student applies the concept appropriately. • Student uses sound critical analysis to develop an insightful and comprehensive response to the prompt.	accurate understanding of the concept. • Student applies the concept appropriately. • Student develops a complete response to the prompt.	in understanding of the concept. • Student applies the concept incorrectly. • Student's response is poorly developed or incomplete.	incomplete. • Student's response demonstrates a critical gap in understanding. • Student is unable to apply the concept.