# *Management of Cybersecurity 7th edition Whitman Solutions Manual*

SKU: 9798214011738-SOLUTIONS

# Solution and Answer Guide

MICHAEL E. WHITMAN AND HERBERT J. MATTORD, MANAGEMENT OF CYBERSECURITY, 7E, 2026, 9798214011738; CHAPTER 01: INTRODUCTION TO THE MANAGEMENT OF CYBERSECURITY

## TABLE OF CONTENTS

**Review Questions** ..... 1

**Exercises** ..... 5

## REVIEW QUESTIONS

1. What has caused cybersecurity to evolve beyond the responsibility of just the IT department?

   **Solution Guidance:** The evolution of cybersecurity beyond the IT department's sole responsibility is due to technology permeating every facet of the business environment, making business places more fluid and information processing decentralized. This necessitates the involvement of all employees, especially managers, in cybersecurity efforts.

2. How do organizations ensure that their cybersecurity planning and decisions involve the appropriate parties?

   **Solution Guidance:** Organizations ensure their cybersecurity planning and decisions involve the appropriate parties by including three distinct groups of managers and professionals—those in the field of cybersecurity, those in the field of IT, and those from the rest of the organization—working together to reach a consensus on protecting the organization's information assets.

3. What are the key characteristics of information that make it valuable to an organization?

   **Solution Guidance:** The key characteristics of information that make it valuable to an organization are expressed in the C.I.A. triad, which stands for confidentiality, integrity, and availability. Modern extensions of the triad include privacy, authenticity, possession, and utility.

4. What measures can be used to protect the confidentiality of information?

   **Solution Guidance:** Measures to protect the confidentiality of information include information classification, secure document and data storage, the application of general security policies, education, training, and awareness for information custodians and end users, and cryptography (encryption).

5. How is the integrity of information protected against corruption and damage?

© 2026 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.



Management of Cybersecurity 7th edition Whitman Solutions Manual

**Solution Guidance:** The integrity of information is protected by employing a variety of error-control techniques during transmission, including the use of redundancy bits, check bits, algorithms, hash values, and error-correcting codes to ensure the information remains whole, complete, and uncorrupted.

6. What role does authentication play in the access control mechanism of information systems?

   **Solution Guidance:** Authentication plays a critical role by requiring the validation and verification of an entity's asserted identity, ensuring that a user (or system) is the entity it claims to be before granting access to information assets.

7. How does knowing the threats faced by an organization assist in cybersecurity management?

   **Solution Guidance:** Knowing the threats faced by an organization assists in cybersecurity management by enabling informed decisions about protecting the organization's people, applications, data, and information systems from potential adverse effects.

8. What role does Internet connectivity play in the exposure of organizations to external threats?

   **Solution Guidance:** Internet connectivity increases the exposure of organizations to external threats because a typical organization with an online connection faces over 3.7 billion potential hackers, given the extensive number of Internet users worldwide.

9. How do DoS and DDoS attacks affect targeted systems?

   **Solution Guidance:** DoS and DDoS attacks overwhelm a target's ability to handle incoming communications, prohibiting legitimate users from accessing affected systems and potentially leading to system overload and inability to perform ordinary functions.

10. What is the significance of implementing contingency plans for forces of nature in cybersecurity?

    **Solution Guidance:** Implementing contingency plans for forces of nature is significant in cybersecurity because these events usually occur with little warning and are beyond anyone's control, necessitating measures to limit damage and prepare for continued operations through disaster recovery, business continuity, and incident response plans.

11. What role do human errors play in cybersecurity threats, and how can they be mitigated?

    **Solution Guidance:** Human errors play a significant role in cybersecurity threats, as they can lead to the unintentional disclosure, modification, or deletion of data. These errors can often be prevented with training, ongoing awareness activities, and controls to minimize the risk of mistakes leading to security breaches.

12. Why is technological obsolescence considered a cybersecurity threat, and how should organizations address it?

    **Solution Guidance:** Technological obsolescence is considered a cybersecurity threat because outdated infrastructure can lead to unreliable and untrustworthy systems

© 2026 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.



Management of Cybersecurity 7th edition Whitman Solutions Manual

vulnerable to attacks. Organizations should proactively analyze current technology usage, plan for upgrades, and take immediate action to replace obsolete technology and mitigate risks.

13. What is the fundamental difference between management and leadership?

    **Solution Guidance:** The fundamental difference between management and leadership is that management involves administering resources to achieve objectives, while leadership focuses on influencing others to achieve an objective by providing purpose, direction, and motivation.

14. What are the three basic behavioral types of leaders?

    **Solution Guidance:** The three basic behavioral types of leaders are autocratic, who reserve all decision making for themselves; democratic, who seek input from interested parties; and laissez-faire, who allow the process to develop with minimal intervention.

15. How does the POLC management theory framework differ from traditional management theory?

    **Solution Guidance:** The POLC management theory framework differs from traditional management theory by focusing on planning, organizing, leading, and controlling, whereas traditional management theory emphasizes planning, organizing, staffing, directing, and controlling.

16. What is the role of contingency planning within the context of organizational management?

    **Solution Guidance:** Contingency planning plays a role within organizational management by preparing for non-normal business operations and unexpected events, ensuring the organization can continue operations during unforeseen circumstances.

17. How can managers ensure the effectiveness of their chosen solution to a problem?

    **Solution Guidance:** Managers can ensure the effectiveness of their chosen solution to a problem by carefully monitoring its implementation and evaluating its success in solving the problem, making adjustments as necessary.

18. What factors should be considered in the analysis and comparison of possible solutions to a problem?

    **Solution Guidance:** Factors to consider in the analysis and comparison of possible solutions include economic feasibility, technological feasibility, behavioral feasibility, and operational feasibility.

19. Describe a method for generating ideas during the problem-solving process.

    **Solution Guidance:** A method for generating ideas during the problem-solving process is brainstorming, in which a group of individuals rapidly suggests as many ideas as possible without regard for practicality, followed by a review to identify feasible options.

20. What differentiates the goals of the cybersecurity management team from those of the IT management team?

© 2026 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.



Management of Cybersecurity 7th edition Whitman Solutions Manual

**Solution Guidance:** The goals of the cybersecurity management team differ from those of the IT management team in that cybersecurity focuses on ensuring the confidentiality, integrity, and availability of information, which may slow down information flow for security purposes, whereas the IT team's primary focus is the effective and efficient processing of information.

21. What are the "six Ps" that constitute the unique functions of cybersecurity management?

    **Solution Guidance:** The six functions of cybersecurity management are planning, policy, programs, protection, people, and project management.

22. How is the cybersecurity strategy developed within an organization?

    **Solution Guidance:** The cybersecurity strategy is developed by translating the overall company strategy into strategies for each subordinate unit, including IT, and then using them with the IT strategy to develop the cybersecurity strategy in close collaboration with all senior managers.

23. What types of cybersecurity plans are necessary to support both normal and non-normal operations?

    **Solution Guidance:** Types of cybersecurity plans necessary to support both normal and non-normal operations include incident response planning, business continuity planning, disaster recovery planning, policy planning, personnel planning, technology rollout planning, risk management planning, and security program planning.

24. What are the three general categories of cybersecurity policy?

    **Solution Guidance:** The three general categories of cybersecurity policy are program policy, which sets the cybersecurity climate across the organization; issue-specific policies, which define acceptable behavior within specific organizational resources; and system-specific policies, which merge technical and managerial intent for the implementation of a given technology.

25. What role do people play in a cybersecurity program?

    **Solution Guidance:** People play the most critical role in the cybersecurity program, encompassing security personnel (the professional cybersecurity employees), the security of personnel (protection of employees and their information), and aspects of the security education, training, and awareness program.

26. How does project management apply to cybersecurity management?

    **Solution Guidance:** Project management applies to cybersecurity management by identifying and controlling the resources applied to cybersecurity projects, measuring progress, and adjusting the process as necessary to ensure the successful implementation of cybersecurity initiatives.

© 2026 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.



Management of Cybersecurity 7th edition Whitman Solutions Manual

## EXERCISES

1. Consider the information stored in your personal computer. Do you currently have information stored on your computer that is critical to your personal life? If that information became compromised or lost, what effect would it have on you?

   **Solution Guidance:** This answer will be unique to each student. A typical personal computer stores a wide range of information that is critical to the personal and professional life of its owner. This information can include personal identification details, financial records, personal photographs and videos, emails and personal correspondence, work-related documents, and other sensitive data. The compromise or loss of this information can have several effects on the owner, including:

   Identity theft—Personal identification information, such as Social Security numbers, addresses, and bank account details, can be used by cybercriminals to commit identity theft, leading to unauthorized financial transactions and legal implications.

   Financial loss—Compromised financial records, including bank statements, credit card information, and investment details, can lead to direct financial loss. Cybercriminals can use this information to siphon funds from bank accounts or make unauthorized purchases.

   Loss of privacy—Personal photographs, videos, and correspondences, if accessed without authorization, can lead to a significant invasion of privacy. This could result in emotional distress and even reputational damage if such information is made public.

   Professional repercussions—Work-related documents and communications stored on personal computers are often confidential. Their unauthorized access or loss can not only affect the individual's employment but also have legal ramifications for breaching confidentiality agreements.

   Emotional impact—The loss of personal memories, such as photographs or videos, that cannot be replaced can have a profound emotional impact on individuals.

   Data recovery costs—Attempting to recover lost data can be expensive, especially if professional services are required. There's also no guarantee of full recovery, which could compound the loss further.

   Protecting the information stored on personal computers involves implementing robust security measures, including the use of strong, unique passwords, enabling two-factor authentication where possible, regular software updates, and maintaining backups of critical data. Additionally, being vigilant about phishing attempts and other forms of social engineering attacks can help mitigate the risk of data compromise.

2. Using the web, research the malware named Stuxnet. When was it discovered? What kind of systems does it target? Who created it and what is it used for?

   **Solution Guidance:** Stuxnet was discovered in June 2010 by Sergey Ulasen from the Belarusian antivirus company VirusBlokAda. It is a highly sophisticated computer worm that targets Siemens industrial control systems, specifically supervisory control and data acquisition (SCADA) systems used to control and monitor industrial processes. Stuxnet is notable for its ability to infect programmable logic controllers (PLCs) by subverting the Step-7 software application used to reprogram these devices. The

© 2026 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.



Management of Cybersecurity 7th edition Whitman Solutions Manual

worm's primary focus was on compromising Iranian nuclear facilities, particularly their uranium enrichment infrastructure. More than 60 percent of the computers infected worldwide were located in Iran, indicating a specific focus on this nation's nuclear program.

The creation of Stuxnet is widely attributed to a joint effort by the United States and Israeli governments, under a covert operation known as Operation Olympic Games. This operation was part of an extensive cyberwarfare campaign to hinder Iran's nuclear program capabilities. The worm's design allowed it to spread via USB flash drives, crossing air gaps intended to isolate sensitive systems from network attacks. Despite its targeted nature, Stuxnet also inadvertently spread beyond its intended targets, causing unintended global proliferation.

Stuxnet represents a significant milestone in cyberwarfare, being the first discovered malware to spy on and subvert industrial systems, and it highlighted the potential for cyberattacks to cause physical damage to critical infrastructure. The worm's discovery has led to increased awareness and concern about the security of industrial control systems and the potential implications of cyberwarfare on national and global security.

For detailed information, you may refer to the comprehensive analyses provided by Wikipedia, Britannica, and Avast.

3. Search the web for "The Official Phreaker's Manual." What information in this manual might help a security administrator protect a communications system?

**Solution Guidance:** "The Official Phreaker's Manual" and related information on phreaking provide valuable insights for security administrators aiming to protect communication systems. The manual and historical accounts of phreaking reveal several techniques that could be exploited to bypass security measures in telecommunications systems. Understanding these techniques can help administrators fortify their defenses against similar vulnerabilities.

Knowledge of system vulnerabilities—The manual details various technical aspects and vulnerabilities of telecommunications systems, such as the use of specific frequencies to manipulate phone systems. By understanding these vulnerabilities, administrators can better secure systems against unauthorized access or manipulation.

Insight into hacker mindset and techniques—Phreaking history shows how enthusiasts experimented with and exploited telecommunications systems, including the use of tone generators and social engineering. This insight helps administrators anticipate potential security threats and implement more effective countermeasures.

Specific attack methods—The manual outlines specific methods such as blue boxing, which involves generating tones to make free long-distance calls, and switch hooking, a method to place calls from locked telephones. By understanding these methods, security professionals can develop targeted strategies to detect and prevent such attacks.

Evolution of telecommunication security—The transition from in-band signaling to more secure systems like SS7 demonstrates how telecommunications security has evolved in response to phreaking activities. Security administrators can use this historical perspective to appreciate the importance of ongoing security updates and vigilance.

© 2026 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Management of Cybersecurity 7th edition Whitman Solutions Manual

Security enhancements—The manual's discussion of technologies and methodologies, including how calls are routed and managed within telecommunications networks, offers practical knowledge for enhancing security protocols and infrastructure design.

Security administrators should focus on continuously updating their knowledge base with information on both historical and emerging threats. Regular security audits, investing in modern security technologies, and fostering a culture of security awareness within organizations are crucial steps in protecting communications systems against potential breaches.

4. The chapter discussed many threats and vulnerabilities to cybersecurity. Using the web, find at least two other sources of information about threats and vulnerabilities. Begin with *www.securityfocus.com* and use a keyword search on "threats."

   **Solution Guidance:** Reliable sources for information about cybersecurity threats and vulnerabilities include:

   CVE Details (www.cvedetails.com): This website provides a database of publicly disclosed cybersecurity vulnerabilities. It allows users to search for vulnerabilities based on different criteria, including software, vendor, or the specific type of vulnerability. This resource is invaluable for understanding specific vulnerabilities that could impact systems and the potential threats exploiting these vulnerabilities.

   National Vulnerability Database (NVD; www.nist.gov/nvd): Managed by the National Institute of Standards and Technology (NIST), the NVD is the U.S. government repository of standards-based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

   For security administrators looking to protect communication systems, understanding the nature of threats and vulnerabilities is critical. By staying informed through the sources described above and other reputable sources, security professionals can better anticipate potential security issues and implement effective defenses.

5. Using the categories of threats mentioned in this chapter and the various attacks described, review several current media sources and identify examples of each threat.

   **Solution Guidance:** This will be a unique response for each student.

© 2026 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.



Management of Cybersecurity 7th edition Whitman Solutions Manual

# Instructor Manual

Michael E. Whitman and Herbert J. Mattord, Management of Cybersecurity 2026, 9798214011738; Chapter 1: Introduction to the Management of Cybersecurity

## TABLE OF CONTENTS

**Purpose and Perspective of the Chapter** ..... **2**
**Chapter Objectives** ..... **2**
**Chapter Outline** ..... **2**
**Note About Live Virtual Machine Labs** ..... **6**
**Additional Discussion Questions** ..... **7**
**Additional Activities and Assignments** ..... **7**
**Additional Resources** ..... **8**
External Video Resources ..... 8
Internet Resources ..... 8
External Audio Resources ..... 8
**Appendix** ..... **9**
Generic Rubrics ..... 9
Standard Writing Rubric ..... 9
Standard Discussion Rubric ..... 10

© 2026 Cengage Learning, Inc. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.



Management of Cybersecurity 7th edition Whitman Solutions Manual

## Purpose and Perspective of the Chapter

Introduction to the Management of Cybersecurity serves as an introduction to cybersecurity and project management. Students will learn about basic security concepts and organizational roles in relation to information protection. Different aspects of project management and their relationship with cybersecurity are discussed.

## Chapter Objectives

The following objectives are addressed in this chapter:

1. Summarize the key characteristics of cybersecurity.
2. Outline the 12 dominant categories of threats to cybersecurity.
3. Discuss the key characteristics of leadership and management.
4. Differentiate types of management and their role in securing information assets.

## Chapter Outline

1. Introduction to Cybersecurity
    a. In today's global markets, technology enables business operations. IT enables storing and transporting information—often a company's most valuable resource—from one business unit to another. The focus of cybersecurity is protecting information assets. Organizations know that cybersecurity involves more than information managers, the members of the cybersecurity team, or the IT managers. It must involve the entire organization, as represented by three communities of interest: those in cybersecurity, those in IT, and those from the rest of the organization.

        i. The dominant areas of security include:
            1. Cybersecurity–The 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; this area overlaps with all other security areas.
            2. Computer security–The protection of computerized information processing systems and the data they contain and process.
            3. Communications security–The protection of all communications media, technology, and content.
            4. Network security–A subset of communications security, the protection of voice and data networking components, connections, and content.

© 2026 Cengage Learning, Inc. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.



Management of Cybersecurity 7th edition Whitman Solutions Manual

5. Operations security–The protection of the details of an organization's operations and activities.
6. Physical security–The protection of physical items, objects, or areas from unauthorized access and misuse, known in the industry as corporate security.

b. The Value of Information and the C.I.A. Triad
   i. To better understand the management of cybersecurity, you must become familiar with the key characteristics of information that make it valuable to an organization, as expressed in the C.I.A. triad, the industry standard for computer-based security based on three characteristics that describe the utility of information: confidentiality, integrity, and availability.
      1. Confidentiality, an attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems, means limiting access to information only to those who need it and preventing access by those who do not.
      2. Integrity is an attribute of information describing how data is whole, complete, and uncorrupted and how it is threatened when exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being entered, stored, or transmitted.
      3. Availability, the information attribute that describes how data is accessible and correctly formatted for use without interference or obstruction, means that users, either people or other systems, have access to it in a usable format.

2. Key Concepts of Cybersecurity: Threats and Attacks
   a. To protect your organization’s information, you must: (1) know yourself—that is, be familiar with the information assets to be protected, their inherent flaws and vulnerabilities, and the systems, mechanisms, and methods used to store, transport, process, and protect them—and (2) know the threats you face as well as their attack methods, characteristics, and potential outcomes. To make sound decisions about cybersecurity, management must be informed about the various threats to an organization’s people, applications, data, and information systems.
   b. The Twelve Categories of Threats
      i. Deviations in services—utility service problems (Internet, phone, power, water, etc.).
      ii. Espionage or trespass—unauthorized access and/or data disclosure.
      iii. Forces of nature—fire, floods, earthquakes, lightning, etc.
      iv. Human error or failure—social engineering, accidents, or employee mistakes.
      v. Information extortion—blackmail, threatening information denial, or disclosure.

© 2026 Cengage Learning, Inc. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Management of Cybersecurity 7th edition Whitman Solutions Manual

vi. Intellectual property compromises -piracy, copyright infringement, research and development (R&D) disclosure.
vii. Sabotage or vandalism—unauthorized modification or destruction of systems or information.
viii. Software attacks—malware, website spoofing, or denial of service.
ix. Technical hardware failures or errors—equipment failure.
x. Technical software failures or errors—bugs or code problems.
xi. Technological obsolescence—antiquated or outdated technologies.
xii. Theft—illegal confiscation of equipment or information.

3. Management and Leadership
    a. To understand what management of cybersecurity is, you must first understand what management is and how it can be used effectively. In its most basic form, management is the process of getting a job done and achieving other objectives by appropriately applying a given set of resources. A manager is a member of the organization assigned to request, organize, and administer resources, coordinate the completion of tasks, and handle the many roles necessary to complete the desired objectives.
    b. Behavioral Types of Leaders
        i. Among leaders, there are three basic behavioral types: autocratic, democratic, and laissez-faire. Autocratic leaders reserve all decision-making responsibility for themselves and are “do as I say” types. Such leaders typically issue an order to accomplish a task and do not usually seek or accept alternative viewpoints. Democratic leaders work in the opposite way, typically seeking input from all interested parties, requesting ideas and suggestions, and then formulating positions that can be supported by a majority. The laissez-faire leader is also known as the “laid-back” leader. While both autocratic and democratic leaders tend to be action-oriented, the laissez-faire leader often sits back and allows the process to develop as it goes, only making minimal decisions to avoid bringing the process to a complete halt.
    c. Management Characteristics
        i. The management of tasks requires certain basic skills. These skills are variously referred to as management functions or management principles. The two basic approaches to management are:
            1. Traditional management theory: This approach uses the core principles of planning, organizing, staffing, directing, and controlling (POSDC).
            2. Popular management theory: This approach uses the core principles of planning, organizing, leading, and controlling (POLC).

© 2026 Cengage Learning, Inc. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Management of Cybersecurity 7th edition Whitman Solutions Manual

d. Governance
    i. The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly. Cybersecurity governance emphasizes escalating the importance of cybersecurity to the uppermost levels of the organization and providing it with an appropriate level of recognition and oversight.
e. Solving Problems
    i. All managers encounter problems during the organization's day-to-day operation. Whether a problem has a low or high profile, the same basic process can be used to solve it. However, time pressures often constrain decision-making when problems arise. Gathering and evaluating the necessary facts may be beyond available capabilities. Nevertheless, the methodology described in the following steps can be used as a basic blueprint for resolving many operational problems.
        1. Step 1: Recognize and Define the Problem
        2. Step 2: Gather Facts and Make Assumptions
        3. Step 3: Develop Possible Solutions
        4. Step 4: Analyze and Compare Possible Solution
        5. Step 5: Select, Implement, and Evaluate

4. Principles of Cybersecurity Management
    a. As part of the management team, the cybersecurity management team operates like all other management units by using the common characteristics of leadership and management discussed earlier in this chapter. However, the cybersecurity management team's goals and objectives differ from those of the IT and general management communities in that the cybersecurity management team is focused on the secure operation of the organization. In fact, some of the cybersecurity management team's goals and objectives may be contrary to or require resolution with the goals of the IT management team.
        i. Planning
            1. Planning in cybersecurity management extends the basic planning model. The cybersecurity planning model includes activities necessary to support the design, creation, and implementation of cybersecurity strategies within the planning environments of all organizational units, including IT.
        ii. Policy
            1. In cybersecurity, there are three general categories of policy and managerial guidance that dictate certain behaviors within the organization.
                a. Program policy
                b. Issue-specific policies
                c. System-specific policies

© 2026 Cengage Learning, Inc. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Management of Cybersecurity 7th edition Whitman Solutions Manual

iii. Programs
    1. Cybersecurity operations that are specifically managed as separate entities are called programs. An example would be a security education, training, and awareness (SETA) program, a risk management program, or contingency programs such as incident response, disaster recovery, or business continuity.
iv. Protection
    1. The protection function is executed via a set of risk management activities as well as protection mechanisms, technologies, and tools.
v. People
    1. People are the most critical link in the cybersecurity program. This area encompasses security personnel (the professional cybersecurity employees), the security of personnel (the protection of employees and their information), and aspects of the SETA program.
vi. Project Management
    1. Whether a cybersecurity manager is asked to roll out a new security training program or select and implement a new firewall, it is important that the process be managed as a project. The final element for thorough cybersecurity management is the application of a project management discipline to all elements of the cybersecurity program.

5. Closing Case
    a. This is a great opportunity for students to dissect the knowledge learned in this chapter, allowing students a further in-depth examination of the concepts presented.
        i. Case Discussion Questions
        ii. Case Ethical Decision Making

[return to top]

## Note About Live Virtual Machine Labs

The live virtual machine labs provide hands-on practice that will help students learn the material covered in each module. Throughout the labs, students will encounter gradable assessments in the form of multiple-choice questions and requests to use lab functionality and record screenshots of their live virtual machine lab desktop, noting their progress in the lab.
The introduction in the content pane in each live virtual machine lab provides a list of learning outcomes that students should be able to do after they complete the module. Each lab also covers a list of exam objectives. The main focus of the live

© 2026 Cengage Learning, Inc. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Management of Cybersecurity 7th edition Whitman Solutions Manual

virtual machine labs is to cover the practical, hands-on aspects of the exam objectives. The labs do not map directly back to the topics covered in each module of the book or MindTap course. It is recommended that students refer to course materials to research theoretical topics in more detail.
[return to top]

## Additional Discussion Questions

The following are discussion questions that do not appear in the text, PPTs, or courseware (if courseware exists)—they are for you to use as you wish. 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.

1. Start a class discussion about which leadership role students believe would be most effective in assisting with project completion and require that students justify their opinions.

2. Give students time to discuss what types of security should be considered when dealing with cybersecurity as a whole. Which areas of security might be more critical than others?

3. Have students research at least three (3) of the leading anti-malware programs available today. Students should compare features offered by each of the 3 programs and write a recommendation on which anti-malware program they feel an organization should use to protect information technology resources.

4. Task students with researching the different types of management approaches. Students should write down the defining features of several different types of management and then share them with the class.

[return to top]

## Additional Activities and Assignments

The following are activities and assignments developed by Cengage but not included in the text, PPTs, or courseware (if courseware exists)—they are for you to use if you wish.

1. Use the Internet to research the following concepts and prepare a brief report on each topic explaining how it works and why it is used. Also, discuss the different types.
    a. Threat
    b. Attack
    c. Threat event

© 2026 Cengage Learning, Inc. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.



Management of Cybersecurity 7th edition Whitman Solutions Manual

d. Threat agent
e. Exploit
f. Vulnerability
g. Information asset

[return to top]

## Additional Resources

### External Video Resources

- What Is Cyber Security | How It Works?
- Principles of Information Security: Confidentiality, Integrity, & Availability

### Internet Resources

- Board preparedness: 7 steps to combat cybersecurity threats
- 12 common types of malware attacks and how to prevent them
- The McCumber Cube Model Framework: Enhancing Information Security
- The McCumber Cube and CIA Triad (Interactive)
- CIA triad (confidentiality, integrity, and availability)
- The Best Malware Removal and Protection Software for 2024
- 5 Tips to Improve Your Defenses Against Social Engineering

### External Audio Resources

- Security From the Start With Sabin Thomas

[return to top]

© 2026 Cengage Learning, Inc. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.



Management of Cybersecurity 7th edition Whitman Solutions Manual

# APPENDIX

## GENERIC RUBRICS

Providing students with rubrics helps them understand the expectations and components of assignments. Rubrics help students become more aware of their learning process and progress, and they improve students' work through timely and detailed feedback.

Customize these rubric templates as you wish. The writing rubric indicates 40 points, and the discussion rubric indicates 30 points.

## STANDARD WRITING RUBRIC

| Criteria | Meets Requirements | Needs Improvement | Incomplete |
|---|---|---|---|
| Content | The assignment clearly and comprehensively addresses all questions in the assignment.<br>15 points | The assignment partially addresses some or all questions in the assignment.<br>8 points | The assignment does not address the questions in the assignment.<br>0 points |
| Organization and Clarity | The assignment presents ideas in a clear manner and with strong organizational structure. The assignment includes an appropriate introduction, content, and conclusion. Coverage of facts, arguments, and conclusions are logically related and consistent.<br>10 points | The assignment presents ideas in a mostly clear manner and with a mostly strong organizational structure. The assignment includes an appropriate introduction, content, and conclusion. Coverage of facts, arguments, and conclusions are mostly logically related and consistent.<br>7 points | The assignment does not present ideas in a clear manner and with strong organizational structure. The assignment includes an introduction, content, and conclusion, but coverage of facts, arguments, and conclusions are not logically related and consistent.<br>0 points |
| Research | The assignment is based upon appropriate and adequate academic literature, including peer reviewed journals and other scholarly work.<br>5 points | The assignment is based upon adequate academic literature but does not include peer reviewed journals and other scholarly work.<br>3 points | The assignment is not based upon appropriate and adequate academic literature and does not include peer reviewed journals and other scholarly work.<br>0 points |
| Research | The assignment follows the required citation guidelines.<br>5 points | The assignment follows some of the required citation guidelines.<br>3 points | The assignment does not follow the required citation guidelines.<br>0 points |
| Grammar and Spelling | The assignment has two or fewer grammatical and spelling errors.<br>5 points | The assignment has three to five grammatical and spelling errors.<br>3 points | The assignment is incomplete or unintelligible.<br>0 points |

[return to top]

© 2026 Cengage Learning, Inc. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.



Management of Cybersecurity 7th edition Whitman Solutions Manual

## STANDARD DISCUSSION RUBRIC

| Criteria | Meets Requirements | Needs Improvement | Incomplete |
|---|---|---|---|
| Participation | Submits or participates in discussion by the posted deadlines. Follows all assignment instructions for initial post and responses.<br>5 points | Does not participate or submit discussion by the posted deadlines. Does not follow instructions for initial post and responses.<br>3 points | Does not participate in discussion.<br>0 points |
| Contribution Quality | Comments stay on task. Comments add value to discussion topic. Comments motivate other students to respond.<br>20 points | Comments may not stay on task. Comments may not add value to discussion topic. Comments may not motivate other students to respond.<br>10 points | Does not participate in discussion.<br>0 points |
| Etiquette | Maintains appropriate language. Offers criticism in a constructive manner. Provides both positive and negative feedback.<br>5 points | Does not always maintain appropriate language. Offers criticism in an offensive manner. Provides only negative feedback.<br>3 points | Does not participate in discussion.<br>0 points |

[return to top]

© 2026 Cengage Learning, Inc. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.



Management of Cybersecurity 7th edition Whitman Solutions Manual