# CHAPTER 2: INFORMATION SECURITY PRINCIPLES OF SUCCESS

**Multiple Choice:**

**1.** Given enough time, tools, inclination, and _____, a hacker can break through any security measure.

A. talent

B. skills

C. intelligence

D. assets

**Answer:** B **Reference:** Principle 1: There Is No Such Thing **Difficulty:** moderate

**2.** In 2003 the Whitworth Gallery's layered security system included all of the following except:

A. Closed-circuit television

B. Alarm systems

C. Electronic motion sensors

D. Rolling patrols.

**Answer:** C **Reference:** Principle 1: There Is No Such Thing **Difficulty:** moderate

**3.** Which of the following is not a common class of ratings for safes?

A. B-rate

B. C-rate

C. ULTL-30

D. ULTL-40

**Answer:** D **Reference:** Principle 1: There Is No Such Thing **Difficulty:** moderate

**4.** The goals of information security measures include:

A. Protecting confidentiality of data

B. Preserving the integrity of data

C. Promoting the availability of data for authorized use

D. All of the above are goals

**Answer:** D **Reference:** Principle 2: The Three Security Goals **Difficulty:** moderate

**5.** IS professionals who create a plan to protect a computer system consider all of the following in the planning process except:

A. Defining the structural composition of data

B. Protecting the confidentiality of data

C. Preserving the integrity of data

D. Promoting the availability of data for authorized use

**Answer:** A **Reference:** Principle 2: The Three Security Goals **Difficulty:** moderate

**6.** Synonyms for confidentiality include all of the following except:

A. privacy

B. secrecy

C. integrity

D. discretion

**Answer:** C **Reference:** FYI: Confidentiality by Another Name **Difficulty:** moderate

**7.** Which of the following is NOT a goal of an integrity model security system?

A. Preventing unauthorized users from modifying data or programs

B. Verifying data consistency for internal and external programs

C. Preventing authorized users form making unauthorized modifications

D. Maintaining internal and external consistency of data and programs

**Answer:** B **Reference:** Integrity Models **Difficulty:** moderate

**8.** Common availability challenges do NOT include which of the following?

A. Equipment failure

B. Denial of service

C. Rapid spread of viruses

D. Loss of information system due to natural disaster or human action.

**Answer:** C **Reference:** Availability Models **Difficulty:** moderate

**9.** Which of the following is NOT an activity designed to preserve information system availability?

A. Grant access to authorized personnel

B. Apply encryption to information sent over the Internet

C. Develop a disaster recovery plan

D. All of the above preserve system availability.

**Answer:** D **Reference:** Availability Models **Difficulty:** moderate

**10.** Layered security is also referred to as:

A. Denial of service

B. Defense in depth

C. Multi-system security

D. None of the above.

**Answer:** B **Reference:** Principle 3: Defense in Depth **Difficulty:** moderate

**11.** Overlapping layers provide all of the following elements necessary to secure assets except:

A. Direction

B. Response

C. Detection

D. Prevention

**Answer:** A **Reference:** Principle 3: Defense in Depth **Difficulty:** moderate

**12.** Defense in depth means that security devices are layered in a series that _____, detects, and responds to attacks on systems.

A. deflects

B. denies

C. defends

D. prevents

**Answer:** D **Reference:** Principle 3: Defense in Depth **Difficulty:** moderate

**13.** Which of the following statements about Principle 4 is false?

A. In exchange for worthless goods, people tend to give up credentials.

B. The organizers of Infosecurity Europe 2003 found that 75% of survey respondents revealed information immediately.

C. Today's virus writers are not very sophisticated.

D. It is easy to fool people into spreading viruses.

**Answer:** C Re**ference:** Principle 4: When Left on Their Own **Difficulty:** moderate

**14.** Avoid phishing, ID theft, and monetary loss by taking all of the following steps except:

A. Recognize the signs of fraud

B. Ignore links embedded in e-mail messages

C. Follow advice of financial services provider

D. Keep virus software current.

**Answer:** D **Reference:** In Practice: Phishing for Dollars **Difficulty:** moderate

**15.** IS principle five states that security depends on these requirements:

A. Functional and assurance

B. Verification and validation

C. Availability and integrity

D. Usability and interface.

**Answer:** A **Reference:** Principle 5: Computer Security Depends on Requirements **Difficulty:** moderate

**16.** Which of the following questions is NOT answered by the functional and assurance requirements as specified by Principle 5?

A. Does the system do the right things?

B. Does the system do the right things in the right way?

C. Both of the above are answered

D. Neither of the above are answered.

**Answer:** C **Reference:** Principle 5: Computer Security Depends on Requirements **Difficulty:** moderate

**17.** Software developers often lack the _____ and _____ needed to test and break their software.

A. Wherewithal, motivation

B. Money, time

C. Expertise, resources

D. Qualifications, experience.

**Answer:** A **Reference:** Principle 5: Computer Security Depends on Requirements **Difficulty:** moderate

**18.** Which of the following is true for Principle six?

A. There is no such thing as absolute security.

B. Risk management provides security.

C. Security through obscurity is not an answer.

D. Security has no finite limit.

**Answer:** C **Reference:** Principle 6: Security Through Obscurity **Difficulty:** moderate

**19.** One school of thought says that if _____ do not know how software is secured, security is better.

A. hackers

B. crackers

C. users

D. developers

**Answer:** A **Reference:** Principle 6: Security Through Obscurity **Difficulty:** moderate

**20.** What does security through obscurity mean?

A. Security details are not published.

B. Little known security techniques are used.

C. Hiding details secures the system.

D. Security details are encrypted.

**Answer:** C **Reference:** Principle 6: Security Through Obscurity **Difficulty:** moderate

**21.** To gain confidence in software products both _____ and _____ answers are needed.

A. risk, process

B. integrity, availability

C. functional, assurance

D. verification, validation.

**Answer:** D **Reference:** Principle 5: Computer Security Depends **Difficulty:** moderate

**22.** More dangerous than not addressing security is obscuring security because it leads to a:

A. False sense of security

B. Higher level of security

C. Reduced level of security

D. Complete breakdown of security.

**Answer:** A **Reference:** Principle 6: Security Through Obscurity **Difficulty:** moderate

**23.** Central themes to securing information systems are:

A. Risk consequences and risk assessment

B. Risk acceptance and risk mitigation

C. Risk analysis and risk management

D. None of the above.

**Answer:** C **Reference:** Principle 7: Security = Risk Management **Difficulty:** moderate

**24.** Which of the following is NOT an outcome of risk analysis?

A. Risks are countered

B. Insurance against loss is acquired

C. Risk is accepted and consequences are managed

D. Risk is not accepted and consequences do not exist.

**Answer:** D **Reference:** Principle 7: Security = Risk Management **Difficulty:** moderate

**25.** The factors used to determine degree of risk include:

A. Determining the consequence of loss

B. Determining the likelihood that loss will occur

C. Both of the above

D. None of the above.

**Answer:** C **Reference:** Principle 7: Security = Risk Management **Difficulty:** moderate

**26.** Which of the following actions may be required after a high risk rating is determined?

A. Immediate action required

B. Senior management attention needed

C. Manage by routine procedures

D. Management responsibility must be specified

**Answer:** B **Reference:** Principle 7: Security = Risk Management **Difficulty:** moderate

**27.** The unique security issues and considerations of every system make it crucial to understand all of the following except:

A. Adherence to security standards

B. The security skills of the development teams

C. What hardware and software is used to deploy the system

D. The specific nature of data the system maintains.

**Answer:** A **Reference:** Principle 7: Security = Risk Management **Difficulty:** moderate

**28.** Which of the following is NOT considered a pillar of security?

A. People

B. Process

C. Disclosure

D. Technology

**Answer:** C **Reference:** Principle 11 People, Process, and Technology **Difficulty:** moderate

**Fill in the Blank:**

**29.** The first principle of information security says that a hacker can break any security system given enough time, inclination, tools, and _____.

**Answer:** skills **Reference:** Principle 1: There Is No Such Thing **Difficulty:** moderate

**30.** The Whitworth Gallery in Manchester England used a _____ security system in 2003.

**Answer:** layered **Reference:** Principle 1: There Is No Such Thing **Difficulty:** moderate

**31.** One goal of information security is to promote the _____ of data for authorized use.

**Answer:** availability **Reference:** Principle 2: The Three Security Goals **Difficulty:** moderate

**32.** Confidentiality, integrity, and availability or the _____ form the basis of all security programs.

**Answer:** CIA triad **Reference:** Principle 2: The Three Security Goals **Difficulty:** moderate

**33.** Confidentiality controls are user IDs and _____.

**Answer:** passwords **Reference:** Caution: Confidentiality Models **Difficulty:** moderate

**34.** Keeping data pure and trustworthy by protecting system data is the hallmark of the _____ model.

**Answer:** integrity **Reference:** Integrity Model **Difficulty:** moderate

**35.** During emergencies or disasters _____ models keep data and resources available.

**Answer:** availability **Reference:** Availability Models **Difficulty:** moderate

**36.** Periodically test the security of an operating system to uncover any new _____.

**Answer:** vulnerabilities **Reference:** Availability Models **Difficulty:** moderate

**37.** With a layered security system, each mechanism is thoroughly tested before _____ to ensure that the system is suitable for operation.

**Answer:** deployment **Reference:** Principle 3: Defense in Depth **Difficulty:** moderate

**38.** An Internet-attached _____ designed with security in mind includes routers, firewalls, and IDS to protect from intruders.

**Answer:** network **Reference:** Principle 3: Defense in Depth **Difficulty:** moderate

**39.** As a general rule, people give up the _____ that technologies use to secure systems.

**Answer:** secrets **Reference:** Principle 4: When Left on Their Own **Difficulty:** moderate

**40.** An example of how easily people are duped into breaching security is _____.

**Answer:** phishing **Reference:** In Practice: Phishing for Dollars **Difficulty:** moderate

**41.** Principle 5 states that the _____answer the questions: Does the system do the right things? Does the system do the right things in the right way?

**Answer:** requirements **Reference:** Principle 5: Computer Security Depends On **Difficulty:** moderate

**42.** While software needs both verification and validation answers, most commercial off-the-shelf software and systems stop at _____.

**Answer:** verification **Reference:** Principle 5: Computer Security Depends On **Difficulty:** moderate

**43.** Spending more on securing on asset than the intrinsic value of the asset is a waste of _____.

**Answer:** resources **Reference:** Principle 7: Security = Risk Management **Difficulty:** moderate

**44.** The Security Control types include preventative, _____, and responsive.

**Answer:** detective **Reference:** Principle 8: The Three Types of Security Controls **Difficulty:** moderate

**45.** Security requests are rarely _____ if spending resources are justified with solid business rationale.

**Answer:** denied **Reference:** Principle 10: Fear, Uncertainty, and Doubt **Difficulty:** moderate

**46.** The three pillars of security are: _____, process, and technology.

**Answer:** people **Reference:** Principle 11: People, Process, and Technology **Difficulty:** moderate

**47.** In order for administrators to defend systems they must have specific _____ of any security vulnerability.

**Answer:** knowledge **Reference:** In Practice: To Disclose or Not to Disclose **Difficulty:** moderate

**48.** People, _____, and technology must work together to secure systems.

**Answer:** process **Reference:** In Practice: How People, Process, and Technology **Difficulty:** moderate

**Matching:**

**49.** Match the following terms to their meanings:

| | |
|---|---|
| I. Principle 1 | A. Defense in depth |
| II. Principle 2 | B. Functional and assurance |
| III. Principle 3 | C. confidentiality, integrity, availability |
| IV. Principle 4 | D. No absolute security |
| V. Principle 5 | E. Unsupervised people make bad decisions |

**Answer:** D C A E B **Reference:** Information Security Principles **Difficulty:** moderate

**50.** Match the following terms to their meanings:

| | | |
|---|---|---|
| I. | Principle 6 | A. Risk Management |
| II. | Principle 7 | B. No fear, uncertainty, or doubt |
| III. | Principle 8 | C. Complexity is the enemy |
| IV. | Principle 9 | D. Obscurity not an answer |
| V. | Principle 10 | E. Preventative, detective, responsive |

**Answer:** D A E C B **Reference:** Information Security Principles **Difficulty:** moderate

**51.** Match the following terms to their meanings:

| | | |
|---|---|---|
| I. | Dual control | A. Load too much information into the input area |
| II. | Separation of duties | B. One person acts as a countermeasure to another |
| III. | Buffer overflow | C. Cookbook on how to take advantage of vulnerability |
| IV. | Exploit | D. Has characteristics of skill and will |
| V. | Attacker | E. No one person has the ability to control a security activity |

**Answer:** B E A C D **Reference:** Principle: 7 Security = Risk Management (and Principle 11) **Difficulty:** moderate