Name: _____ Class: _____ Date: _____

# Chapter 1 - Introduction to Security

## True / False

1. The Security Administrator reports directly to the CIO.

a. True
b. False

*ANSWER:* False
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Introduction to Security
*QUESTION TYPE:* True / False
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

2. The CompTIA Security+ certification is a vendor-neutral credential.

a. True
b. False

*ANSWER:* True
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Introduction to Security
*QUESTION TYPE:* True / False
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

3. Successful attacks are usually not from software that is poorly designed and has architecture/design weaknesses.

a. True
b. False

*ANSWER:* False
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Reasons for Successful Attacks
*QUESTION TYPE:* True / False
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

4. Smart phones give the owner of the device the ability to download security updates.

a. True

## Chapter 1 - Introduction to Security

b. False

*ANSWER:* False
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Difficulties in Defending Against Attacks
*QUESTION TYPE:* True / False
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

5. As security is increased, convenience is often increased.

a. True
b. False

*ANSWER:* False
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Understanding Security
*QUESTION TYPE:* True / False
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

6. A vulnerability is a flaw or weakness that allows a threat to bypass security.

a. True
b. False

*ANSWER:* True
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Information Security Terminology
*QUESTION TYPE:* True / False
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

7. To mitigate risk is the attempt to address risk by making the risk less serious.

a. True
b. False

*ANSWER:* True
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Information Security Terminology

## Chapter 1 - Introduction to Security

*QUESTION TYPE:* True / False
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

8. The Sarbanes-Oxley Act restricts electronic and paper data containing personally identifiable financial information.

a. True
b. False

*ANSWER:* False
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Understanding the Importance of Information Security
*QUESTION TYPE:* True / False
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

9. One of the challenges in combating cyberterrorism is that many of the prime targets are not owned and managed by the federal government.

a. True
b. False

*ANSWER:* True
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Understanding the Importance of Information Security
*QUESTION TYPE:* True / False
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

10. Brokers steal new product research or a list of current customers to gain a competitive advantage.

a. True
b. False

*ANSWER:* False
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Other Threat Actors
*QUESTION TYPE:* True / False
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM

Name: _____ Class: _____ Date: _____

# Chapter 1 - Introduction to Security

*DATE MODIFIED:* 8/28/2017 3:17 PM

**Multiple Choice**

11. What information security position reports to the CISO and supervises technicians, administrators, and security staff?

a. security manager
b. security engineer
c. security auditor
d. security administrator

*ANSWER:* a
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Introduction to Security
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

12. According to the U.S. Bureau of Labor Statistics, what percentage of growth for information security analysts is the available job outlook supposed to reach through 2024?

a. 10
b. 15
c. 18
d. 27

*ANSWER:* c
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Introduction to Security
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

13. Which position below is considered an entry-level position for a person who has the necessary technical skills?

a. security technician
b. security administrator
c. CISO
d. security manager

*ANSWER:* a

## Chapter 1 - Introduction to Security

*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Introduction to Security
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

14. What term refers to an action that provides an immediate solution to a problem by cutting through the complexity that surrounds it?

a. unicorn
b. approved action
c. secure solution
d. silver bullet

*ANSWER:* d
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Challenges of Securing Information
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

15. In what kind of attack can attackers make use of millions of computers under their control in an attack against a single server or network?

a. centered
b. local
c. remote
d. distributed

*ANSWER:* d
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Difficulties in Defending Against Attacks
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

16. Which term below is frequently used to describe the tasks of securing information that is in a digital format?

a. network security
b. information security

## Chapter 1 - Introduction to Security

c. physical security
d. logical security

*ANSWER:* b
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Defining Information Security
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

17. Which of the three protections ensures that only authorized parties can view information?

a. security
b. availability
c. integrity
d. confidentiality

*ANSWER:* d
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Defining Information Security
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

18. Select the information protection item that ensures that information is correct and that no unauthorized person or malicious software has altered that data.

a. availability
b. confidentiality
c. integrity
d. identity

*ANSWER:* c
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Defining Information Security
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

19. Which of the following ensures that data is accessible to authorized users?

## Chapter 1 - Introduction to Security

a. availability
b. confidentiality
c. integrity
d. identity

*ANSWER:* a
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Defining Information Security
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

20. In information security, what can constitute a loss?
    a. theft of information
    b. a delay in transmitting information that results in a financial penalty
    c. the loss of good will or a reputation
    d. all of the above

*ANSWER:* d
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Information Security Terminology
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

21. In information security, which of the following is an example of a threat actor?
    a. a force of nature such as a tornado that could destroy computer equipment
    b. a virus that attacks a computer network
    c. a person attempting to break into a secure computer network
    d. all of the above

*ANSWER:* d
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Information Security Terminology
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

## Chapter 1 - Introduction to Security

22. What type of theft involves stealing another person's personal information, such as a Social Security number, and then using the information to impersonate the victim, generally for financial gain?

a. cyberterrorism
b. identity theft
c. phishing
d. social scam

*ANSWER:* b
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Understanding the Importance of Information Security
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

23. Under which laws are health care enterprises required to guard protected health information and implement policies and procedures whether it be in paper or electronic format?

a. HIPAA
b. HLPDA
c. HCPA
d. USHIPA

*ANSWER:* a
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Understanding the Importance of Information Security
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

24. Those who wrongfully disclose individually identifiable health information can be fined up to what amount per calendar year?

a. $50,000
b. $250,000
c. $500,000
d. $1,500,000

*ANSWER:* d
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Understanding the Importance of Information Security
*QUESTION TYPE:* Multiple Choice

## Chapter 1 - Introduction to Security

*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

25. Which law requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information?

a. Gramm-Leach-Bliley
b. Sarbanes-Oxley
c. California Database Security Breach
d. USA Patriot

*ANSWER:* a
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Understanding the Importance of Information Security
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

26. To date, the single most expensive malicious attack occurred in 2000, which cost an estimated $8.7 billion. What was the name of this attack?

a. Nimda
b. Slammer
c. Love Bug
d. Code Red

*ANSWER:* c
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Understanding the Importance of Information Security
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

27. What term is used to describe a group that is strongly motivated by ideology, but is usually not considered to be well-defined and well-organized?

a. hactivists
b. hacker
c. script kiddies
d. cyberterrorist

*ANSWER:* a

## Chapter 1 - Introduction to Security

*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Hactivists
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

28. Which term is used to describe individuals who want to attack computers yet lack the knowledge of computers and networks needed to do so?

a. cybercriminal
b. hacker
c. script kiddies
d. cyberterrorist

*ANSWER:* c
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Script Kiddies
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

29. Select the term that best describes automated attack software?

a. open-source utility
b. insider software
c. open-source intelligence
d. intrusion application

*ANSWER:* c
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Script Kiddies
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

30. What class of attacks use innovative attack tools and once a system is infected it silently extracts data over an extended period?

a. Inside Attacks
b. Advanced Persistent Threat

## Chapter 1 - Introduction to Security

c. Embedded Attacks
d. Modified Threat

*ANSWER:* b
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Nation State Actors
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

31. What term is used to describe state-sponsored attackers that are used for launching computer attacks against their foes?

a. nation state threats
b. cyber military
c. nation state actors
d. state hackers

*ANSWER:* c
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Nation State Actors
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

32. What term describes a layered security approach that provides the comprehensive protection?

a. comprehensive-security
b. diverse-defense
c. limiting-defense
d. defense-in-depth

*ANSWER:* d
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Fundamental Security Principles
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

33. What process describes using technology as a basis for controlling the access and usage of sensitive data?

## Chapter 1 - Introduction to Security

a. technical controls
b. administrative controls
c. control diversity
d. vendor diversity

*ANSWER:* a
*POINTS:* 1
*DIFFICULTY:* Difficult
*REFERENCES:* Fundamental Security Principles
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

34. What type of diversity is being implemented if a company is using multiple security products from different manufacturers?

a. multiple-product security
b. manufacturer diversity
c. vendor diversity
d. vendor-control security

*ANSWER:* c
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Fundamental Security Principles
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

35. What level of security access should a computer user have to do their job?

a. password protected
b. least amount
c. limiting amount
d. authorized access

*ANSWER:* b
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Fundamental Security Principles
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM

# Chapter 1 - Introduction to Security

*DATE MODIFIED:* 8/28/2017 3:17 PM

36. What term best describes any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by subnational groups or clandestine agents?

a. cybercriminal
b. cracking
c. cyberterrorism
d. hacking

*ANSWER:* c
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Understanding the Importance of Information Security
*QUESTION TYPE:* Multiple Choice
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

**Multiple Response**

37. Which of the following is a valid fundamental security principle? (Choose all that apply.)

a. signature
b. diversity
c. simplicity
d. layering

*ANSWER:* b, c, d
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Fundamental Security Principles
*QUESTION TYPE:* Multiple Response
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

38. Which of the following describes various supporting structures for implementing security that provides a resource of how to create a secure IT environment? (Choose all that apply.)

a. regulatory frameworks
b. reference architectures
c. industry-standard frameworks
d. reference frameworks

*ANSWER:* b, c

## Chapter 1 - Introduction to Security

*POINTS:* 1
*DIFFICULTY:* Difficult
*REFERENCES:* Frameworks and Reference Architectures
*QUESTION TYPE:* Multiple Response
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

39. Which of the following is a common security framework? (Choose all that apply.)

a. ISO
b. COBIT
c. RFC
d. ASA

*ANSWER:* a, b, c
*POINTS:* 1
*DIFFICULTY:* Difficult
*REFERENCES:* Frameworks and Reference Architectures
*QUESTION TYPE:* Multiple Response
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

40. Which of the following are considered threat actors? (Choose all that apply.)

a. brokers
b. competitors
c. administrators
d. individuals

*ANSWER:* a, b
*POINTS:* 1
*DIFFICULTY:* Difficult
*REFERENCES:* Other Threat Actors
*QUESTION TYPE:* Multiple Response
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

### Subjective Short Answer

41. Why is the speed of malicious attacks making the challenge of keeping computers secure more difficult?

*ANSWER:* With modern tools at their disposal, attackers can quickly scan systems to find weaknesses and launch attacks with unprecedented speed. Many tools can even initiate new attacks without any human participation, thus increasing the speed at which systems are attacked.

## Chapter 1 - Introduction to Security

*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Difficulties in Defending Against Attacks
*QUESTION TYPE:* Subjective Short Answer
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

42. Why are there delays in updating products such as anti-virus software to resist attacks?
*ANSWER:* At the current rate of submissions of potential malware on a daily basis, updates for anti-virus software would need to be released every few seconds.
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Difficulties in Defending Against Attacks
*QUESTION TYPE:* Subjective Short Answer
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

43. List and describe three of the characteristics of information that must be protected by information security?
*ANSWER:* Three of the characteristics of information that must be protected by information security are: 1. Confidentiality-Confidentiality ensures that only authorized parties can view the information. 2. Integrity-Integrity ensures that the information is correct and no unauthorized person or malicious software has altered that data. 3. Availability-Availability ensures that data is accessible to authorized users.
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Defining Information Security
*QUESTION TYPE:* Subjective Short Answer
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

44. Information security is achieved through a combination of what three entities? Provide at least one example of each entity.
*ANSWER:* Products (physical security): The physical security around the data. May be as basic as door locks or as complicated as intrusion-detection systems and firewalls. People (personnel security): Those who implement and properly use security products to protect data. Procedures (organizational security): Plans and policies established by an organization to ensure that people correctly use the products.
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Defining Information Security
*QUESTION TYPE:* Subjective Short Answer

## Chapter 1 - Introduction to Security

*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

45. What are script kiddies?
*ANSWER:* Script kiddies are individuals who want to break into computers to create damage yet lack the advanced knowledge of computers and networks needed to do so. Instead, script kiddies do their work by downloading automated attack software (scripts) from Web sites and using it to perform malicious acts.
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Script Kiddies
*QUESTION TYPE:* Subjective Short Answer
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

46. What threat actors are generally believed to be the most dangerous threat actors? Explain your answer.
*ANSWER:* Many security researchers believe that nation state actors might be the deadliest of any threat actors. Nation state actors target very specific resources and the attackers keep working until they are successful. State sponsored attackers are highly skilled and have enough government resources to breach almost any security defense
*POINTS:* 1
*DIFFICULTY:* Easy
*REFERENCES:* Nation State Actors
*QUESTION TYPE:* Subjective Short Answer
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

47. What is the Payment Card Industry Data Security Standard (PCI DSS)?
*ANSWER:* The PCI DSS is a set of security standards that all companies that process, store, or transmit credit or debit card information must follow. PCI applies to any enterprise or merchant, regardless of its size or number of card transactions, that processes transactions either online or in person.
*POINTS:* 1
*DIFFICULTY:* Difficult
*REFERENCES:* Understanding the Importance of Information Security
*QUESTION TYPE:* Subjective Short Answer
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

48. What are the four different risk response techniques?

## Chapter 1 - Introduction to Security

*ANSWER:* Accept, transfer, avoid, and mitigate.
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Information Security Terminology
*QUESTION TYPE:* Subjective Short Answer
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

49. What is occurring when an attacker manipulates commonplace actions that are routinely performed in a business?

*ANSWER:* Vulnerable business processes, also called business process compromise (BPC), occurs when an attacker manipulates commonplace actions that are routinely performed within an organization.
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Reasons for Successful Attacks
*QUESTION TYPE:* Subjective Short Answer
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM

50. Describe the security principle of simplicity.

*ANSWER:* Because attacks can come from a variety of sources and in many ways, information security is by its very nature complex. The more complex something becomes, the more difficult it is to understand. In addition, complex systems allow many opportunities for something to go wrong. Complex security systems can be hard to understand, troubleshoot, and feel secure about. As much as possible, a secure system should be simple for those on the inside to understand and use. Complex security schemes are often compromised to make them easier for trusted users to work with, yet this can also make it easier for the attackers. In short, keeping a system simple from the inside but complex on the outside can sometimes be difficult but reaps a significant benefit.
*POINTS:* 1
*DIFFICULTY:* Moderate
*REFERENCES:* Fundamental Security Principles
*QUESTION TYPE:* Subjective Short Answer
*HAS VARIABLES:* False
*DATE CREATED:* 8/28/2017 3:17 PM
*DATE MODIFIED:* 8/28/2017 3:17 PM