***Experiencing MIS, 9e* (Kroenke)**
Chapter Extension 14 Data Breaches

1) A student at the MSA University hacked into the university's official Web site and stole some confidential information about the scholarship program. This incident is an example of _____.
A) a data breach
B) asynchronous communication
C) key escrow
D) a sequence flow
Answer: A
AACSB: Reflective Thinking
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-1: What Is a Data Breach?
Classification: Application

2) Which of the following is a direct cost of handling a data breach?
A) loss of reputation
B) abnormal customer turnover
C) legal fees and consultation
D) increased customer acquisition activities
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-1: What Is a Data Breach?
Classification: Concept

3) Sam is a hacker who makes money by stealing and selling credit cards. He has targeted the employees of a local firm and is looking for details such as names, addresses, dates of birth, social security numbers, credit card numbers, or health records. In this case, Sam is looking for _____.
A) firewall security measures
B) business continuity plans
C) malware definitions
D) personally identifiable information
Answer: D
AACSB: Reflective Thinking
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-1: What Is a Data Breach?
Classification: Application

4) _____ refers to the process of placing a small charge on a credit card to ensure it is working.
A) Hoarding
B) Carding
C) Phishing
D) Credit card hijacking
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-1: What Is a Data Breach?
Classification: Concept

5) Direct costs of handling a data breach do not include paying for detection of the breach.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-1: What Is a Data Breach?
Classification: Concept

6) According to the Ponemon's *Institute*, there is a 28 percent chance of experiencing a data breach over any given 24-month period.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-1: What Is a Data Breach?
Classification: Concept

7) Personally identifiable information (PII) includes a person's bank account numbers, personal identification numbers, email address, and social security numbers.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-1: What Is a Data Breach?
Classification: Concept

8) Stolen credit cards are validated through a process called carding.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-1: What Is a Data Breach?
Classification: Concept

9) Explain how hackers use information stolen from data breaches for credit card forgery.
Answer: Over 67 percent of data breaches come from hackers trying to make money. Hackers are primarily looking for personally identifiable information (PII), or data that can be used to identify a person. This includes names, addresses, dates of birth, social security numbers, credit card numbers, health records, bank account numbers, personal identification numbers, and email addresses. Stolen information is commonly used for credit card fraud. Stolen credit card information is validated through a process called carding, where a small charge is placed on the card to ensure it is working. Valid cards are then bundled and sold on the black market. The price of stolen credit cards can run from $9 to $26 per card, depending on the type of account. Stolen data is commonly used for identity theft, extortion, and industrial espionage.
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-1: What Is a Data Breach?
Classification: Concept

10) The first step in protecting oneself from data breaches is _____.
A) securing credit and debit card details
B) understanding how they happen
C) learning the technologies used for these activities
D) installing necessary software to protect from possible breaches
Answer: B
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-2: How Do Data Breaches Happen?
Classification: Concept

11) Bob, a hacker, encountered a vulnerability in a bank's firewall when he was trying to hack into its Web site. Which of the following can Bob use to take advantage of this vulnerability?
A) exploit
B) attack vector
C) carding
D) wardriver
Answer: A
AACSB: Reflective Thinking
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-2: How Do Data Breaches Happen?
Classification: Application

12) A group of hackers use a targeted phishing attack to breach a company's firewalls and hack into its security system. Which of the following techniques have the hackers used?
A) pretexting
B) IP spoofing
C) spear phishing
D) phone phishing
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-2: How Do Data Breaches Happen?
Classification: Concept

13) A group of hackers decide to steal credit card details of the users of Swift Shopping Inc., a leading e-commerce company. They infect the security system of the company's third-party vendor and gain access into its internal network. They compromise an internal Windows server of the company and use a malware to extract customer data. Which of the following is illustrated in this scenario?
A) hardening
B) carding
C) pretexting
D) data breaching
Answer: D
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-2: How Do Data Breaches Happen?
Classification: Application

14) Each type of data breach is different because hackers are continually developing new tools and techniques that enable them to steal more data.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-2: How Do Data Breaches Happen?
Classification: Concept

15) Attack vectors are synonymous with attack tactics.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-2: How Do Data Breaches Happen?
Classification: Concept

16) An exploit is a type of attack vector used by hackers.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-2: How Do Data Breaches Happen?
Classification: Concept

17) Spear phishing is used by organizations to monitor traffic passing through their internal network.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-2: How Do Data Breaches Happen?
Classification: Concept

18) Explain how data breach occurs with an example.
Answer: Hackers are continually developing new tools and techniques that enable them to steal more data. They experiment with new attack vectors, or ways of attacking a target. In the data breach that occurred at Target Corporation in late 2013, attackers first purchased malware designed specifically for the attacks they planned to carry out. They then used spear phishing, or a targeted phishing attack, to infect a Target third party vendor's system and gather keystrokes, login credentials, and screenshots from the vendor's users. The attackers used this information to gain access into Target's internal network. Once inside Target's network, the attackers compromised an internal Windows file server. From this server, the attackers used malware named Trojan.POSRAM to extract customer data from point-of-sale (POS) terminals. Customer data was continuously sent from the POS terminals to an extraction server within Target's network. It was then funneled out of Target's network to drop servers in Russia, Brazil, and Miami. From there, the data was collected and sold on the black market.
AACSB: Information Technology
Difficulty: 3: Challenging
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-2: How Do Data Breaches Happen?
Classification: Concept

19) Stuart works for a financial brokerage. His job involves handling sensitive client information such as financial details. Stuart illegally transfers details of some clients from his office computer to his personal email ID, to misuse later. With reference to this situation, Stuart is guilty of _____.
A) exfiltrating
B) carding
C) hardening
D) pretexting
Answer: A
AACSB: Reflective Thinking
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Application

20) Which of the following is TRUE of the measures to be taken by an organization in the event of a data breach?
A) The organization must delay informing its users so that the occurrence of data breach remains private.
B) The organization must not involve additional technical or law enforcement professionals, as it may lead to further damage to its data.
C) The organization must destroy the evidence of the breach to avoid future security problems.
D) The organization must respond quickly to mitigate the amount of damage hackers can do with the stolen data.
Answer: D
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Concept

21) Executives, managers, and all systems personnel of an organization discuss the actions to be taken by each employee in case a data breach occurs. They identify areas that would need immediate attention and assign specific responsibilities to each employee. The employees of the organization are performing a(n) _____.
A) exfiltration
B) documentation
C) walkthrough
D) case study
Answer: C
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Application

22) The purpose of a business continuity planning session in an organization is to _____.
A) discuss how to return the organization to normal operations as quickly as possible after a data breach
B) build plans to increase the market presence of the organization and increase its user base
C) identify new markets that will accelerate the growth of the organization
D) understand the type of information stored by the organization and implement relevant security measures as required by regulatory laws
Answer: A
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Concept

23) Which of the following should be done by employees to protect against data breaches?
A) They should develop new exploits.
B) They should remove existing honeypots.
C) They should design methods for data extrusion.
D) They should conduct a walkthrough.
Answer: D
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Concept

24) Jobs Dot Com, an online recruitment site, was hacked into, and personal information of a number of users was stolen. What information should Jobs Dot Com include in its data breach notification to its users?
A) the costs incurred due to the breach
B) a sincere apology and an acceptance of responsibility for the incident
C) details of how the breach occurred and the reasons for the breach
D) a report on the current security measures
Answer: B
AACSB: Reflective Thinking
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Application

25) Data extrusion helps organizations secure their data from possible data breaches.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Concept

26) Despite data breach, organizations should refrain from informing their users immediately as it will lead to mass user defection.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Concept

27) Decisions on how to respond to a data breach are most effective if they are made when the breach is happening.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Concept

28) Performing a walkthrough should be done as part of a business continuity planning session.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Concept

29) Data breach notifications should state that the existing security policies and procedures are inadequate and that changes are being made to prevent similar breaches in the future.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Concept

30) Why should organizations respond quickly to data breaches?
Answer: Organizations need to respond to data breaches quickly for several reasons. First, by responding quickly an organization can stop hackers from doing more damage. Hackers can be prevented from accessing other internal systems, and affected systems can be patched and cleaned. Additionally, if organizations respond quickly enough, hackers may be prevented from exfiltrating, or illegally transferring, data out of the organization. Second, responding quickly may mitigate the amount of damage hackers can do with the stolen data. If the affected users are notified immediately they can change their passwords, cancel their credit cards, and possibly activate credit monitoring services. Third, the longer organizations delay in notifying users, the more upset users become. Based on past data breaches, users are reasonably forgiving of organizations that quickly notify them about what happened and what steps that are being taken to make things right.
AACSB: Information Technology
Difficulty: 3: Challenging
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Concept

31) What are the steps involved in an organization's plan for a data breach?
Answer: Data breaches aren't guaranteed to happen, but they are likely to happen. As a result, organizations need to plan for data breaches. They need to rehearse what they will do when a breach happens. Executives, managers, and systems personnel must perform a walkthrough and discuss the specific steps each person will take after a breach occurs. This should be done as part of a broader business continuity planning session that discusses how to return the organization to normal operations as quickly as possible. As part of the planning process, organizations should form a computer security incident response team (CSIRT) consisting of staff from the legal and public relations departments, as well as executives and systems administrators. Coordinated pre-planning for an incident helps organizations avoid missteps like accidentally destroying evidence and issuing poorly worded data breach notices to users. Decisions must be made before the incident, not while it's happening.
Finally, as part of the planning process, organizations need to identify additional technical and law enforcement professionals that may need to be brought in to help handle the data breach. Evidence of the breach must be preserved, and the extent of the damage needs to be accurately measured.
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Concept

32) The _____ is a regulatory law that requires security precautions for government agencies.
A) Federal Information Security Management Act (FISMA)
B) Gramm-Leach-Bliley Act (GLBA)
C) Payment Card Industry Data Security Standard (PCI DSS)
D) Family Educational Rights and Privacy Act (FERPA)
Answer: A
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-4: What Are the Legal Consequences of a Data Breach?
Classification: Concept

33) Which of the following regulatory laws requires data protection for financial institutions?
A) the Family Educational Rights and Privacy Act (FERPA)
B) the Federal Information Security Management Act (FISMA)
C) the Gramm-Leach-Bliley Act (GLBA)
D) the Health Information Portability and Accountability Act (HIPAA)
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-4: What Are the Legal Consequences of a Data Breach?
Classification: Concept

34) Adam owns and manages a large insurance company. In order to protect his organization from data breach, Adam has to ensure that he has incorporated the security measures required by the _____.
A) Family Educational Rights and Privacy Act (FERPA)
B) Federal Information Security Management Act (FISMA)
C) Payment Card Industry Data Security Standard (PCI DSS)
D) Gramm-Leach-Bliley Act (GLBA)
Answer: D
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-4: What Are the Legal Consequences of a Data Breach?
Classification: Application

35) Venclave Hospital is a privately-owned organization that specializes in treating neurological diseases. Which of the following regulatory laws governs the data security measures to be taken by this hospital for protecting against data breach?
A) the Health Maintenance Organization Act of 1973
B) the Health Information Portability and Accountability Act (HIPAA)
C) the Gramm-Leach-Bliley Act (GLBA)
D) the Federal Information Security Management Act (FISMA)
Answer: B
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-4: What Are the Legal Consequences of a Data Breach?
Classification: Application

36) Which of the following regulatory laws requires data protection for health care institutions?
A) the Gramm-Leach-Bliley Act (GLBA)
B) the Federal Information Security Management Act (FISMA)
C) the Health Information Portability and Accountability Act (HIPAA)
D) the Health Maintenance Organization Act of 1973
Answer: C
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-4: What Are the Legal Consequences of a Data Breach?
Classification: Concept

37) The _____ is a regulatory law that provides protection for student education records.
A) Family Educational Rights and Privacy Act (FERPA)
B) Equal Educational Opportunities Act of 1974
C) Smith-Lever Act of 1914
D) Federal Information Security Management Act (FISMA)
Answer: A
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-4: What Are the Legal Consequences of a Data Breach?
Classification: Concept

38) Organizations need to understand the body of regulatory law relative to the type of information they store because they will be held accountable for implementing those standards.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-4: What Are the Legal Consequences of a Data Breach?
Classification: Concept

39) The Federal Information Security Management Act (FISMA) details the procedures to be followed by a federal agency in case an organization fails to ensure the minimum security requirements for its data and systems.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-4: What Are the Legal Consequences of a Data Breach?
Classification: Concept

40) The Gramm-Leach-Bliley Act (GLBA) is a universal regulatory law that applies to all types of industries.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-4: What Are the Legal Consequences of a Data Breach?
Classification: Concept

41) List some of the regulatory laws that govern the secure storage of data in certain industries.
Answer: Organizations need to understand the body of regulatory law relative to the type of information they store because they will be held accountable for implementing those standards. A few prominent regulatory laws that govern the secure storage of data in certain industries are listed below.
1. The Federal Information Security Management Act (FISMA) requires security precautions for government agencies.
2. The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act, requires data protection for financial institutions.
3. The Health Information Portability and Accountability Act (HIPAA) requires data protection for health care institutions.
4. The Payment Card Industry Data Security Standard (PCI DSS) governs the secure storage of cardholder data.
5. The Family Educational Rights and Privacy Act (FERPA) provides protection for student education records.
AACSB: Information Technology
Difficulty: 3: Challenging
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-4: What Are the Legal Consequences of a Data Breach?
Classification: Concept

42) _____ are software or procedures used to prevent an information security attack.
A) Malware definitions
B) Countermeasures
C) Exploits
D) Attack vectors
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-5: How Can Data Breaches Be Prevented?
Classification: Concept

43) Talgedco Inc., a software company, has taken several steps to secure its systems and data. The company has also installed a network intrusion detection system and data loss prevention system. Employees of this company have also been trained on the procedures to be followed to reduce the probability of a data breach. These steps taken by Talgedco are an example of _____.
A) attack vectors
B) countermeasures
C) malware
D) exfiltration
Answer: B
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-5: How Can Data Breaches Be Prevented?
Classification: Application

44) A(n) _____ is used to examine traffic passing through an organization's internal network.
A) honeypot
B) attack vector
C) security protocols open repository
D) network intrusion detection system
Answer: D
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-5: How Can Data Breaches Be Prevented?
Classification: Concept

45) _____ are countermeasures designed to prevent sensitive data from being released to unauthorized persons.
A) Malware definitions
B) Attack vectors
C) Data loss prevention systems
D) Data extrusion prevention systems
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-5: How Can Data Breaches Be Prevented?
Classification: Concept

46) Organizations can implement countermeasures that make data breaches impossible to occur.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-5: How Can Data Breaches Be Prevented?
Classification: Concept

47) It is easy for organizations to prepare a list of countermeasures against many different types of attacks and take appropriate measures accordingly.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-5: How Can Data Breaches Be Prevented?
Classification: Concept

48) An organization can easily stop a simple SQL injection attack on its online store by additional user training, stronger vendor authentication, or an internal network intrusion detection system.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-5: How Can Data Breaches Be Prevented?
Classification: Concept

49) What are countermeasures? Why is it important for organizations to implement countermeasures?
Answer: Countermeasures are software or procedures used to prevent an attack. They make data breaches improbable, or unlikely to occur. Phishing detection software, user authentication systems, network intrusion detection systems, and data loss prevention systems are examples of countermeasures that can be taken by organizations. A network intrusion detection system (NIDS) used to examine traffic passing through an organization's internal network can identify possible attacks. Finally, data loss prevention systems (DLP), which are designed to prevent sensitive data from being released to unauthorized persons, can be used to stop the data from leaving the internal network. Such countermeasures help to detect and stop hacker activity at each step of data breaching.
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-5: How Can Data Breaches Be Prevented?
Classification: Concept

50) Explain the basic countermeasures to be taken by organizations to protect themselves against data breaches.
Answer: There is no list of countermeasures for each type of data breach. Each attack is unique and requires its own set of countermeasures. As a starting point, however, organizations should appoint a chief information security officer (CISO) to ensure sufficient executive support and resources are given to the process of data protection. Organizations then need to implement security safeguards and appropriate data protections based on internal policies. In addition, special consideration should be given to regulatory requirements if the organization is storing certain types of sensitive data. Finally, organizations should form a computer security incidence report team, have a business continuity plan in place, and rehearse their incident response plan.
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-5: How Can Data Breaches Be Prevented?
Classification: Concept

51) Stolen information is commonly used to pay bills.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-1: What Is a Data Breach?
Classification: Concept

52) Which of the following is NOT a way for criminals to make money from data breaches?
A) selling a stolen purse
B) identify theft
C) extortion
D) industrial espionage
Answer: A
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-1: What Is a Data Breach?
Classification: Concept

53) Internal employees can steal data more easily than external hackers.
Answer: TRUE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-1: What Is a Data Breach?
Classification: Concept

54) Hackers experiment with new _____ or ways of attacking a target.
A) exploit
B) attack vector
C) carding
D) wardriver
Answer: B
AACSB: Reflective Thinking
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-2: How Do Data Breaches Happen?
Classification: Application

55) Which company waited four years before information their customers about a data breach?
A) Target
B) Macy's
C) the IRS
D) LinkedIn
Answer: D
AACSB: Reflective Thinking
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-2: How Do Data Breaches Happen?
Classification: Application

56) What was one major change that happen in business because of the Target breach?
A) a shift from magnetic swipe cards to EMV-compliant smart cards
B) the government requiring all companies to hire a CISO
C) people choosing to use cash instead of credit cards
D) companies granting all of their customers credit monitoring services
Answer: A
AACSB: Reflective Thinking
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-2: How Do Data Breaches Happen?
Classification: Application

57) Which of the following are NOT ways a company should handle a data breach?
A) Respond quickly.
B) Be honest about the breach.
C) Only send notification to a small number of users.
D) Notify users as soon as possible.
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Application

58) When planning for a data breach which of the following should be part of the process?
A) a walkthrough
B) being honest with customers
C) exfiltrating
D) perform a forensic investigation
Answer: A
AACSB: Reflective Thinking
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Application

59) Which of the following is a best practice for notifying users of a data breach?
A) Keep the information internal until the executive can decide how to deal with the breach.
B) Notify the clients there is no evidence their cards have been compromised.
C) Stay focused and concise.
D) Do not give out key details about the breach.
Answer: C
AACSB: Reflective Thinking
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Application

60) All of these are PCI DSS requirements EXCEPT _____.
A) build a secure network
B) test networks once every ten years
C) maintain an information policy
D) protect cardholder data
Answer: B
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-4: What Are the Legal Consequences of a Data Breach?
Classification: Concept

61) Regulatory fines imposed after a data breach can never be higher than the financial damage done during the data breach.
Answer: FALSE
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-4: What Are the Legal Consequences of a Data Breach?
Classification: Concept

62) All of the following these legal actions can occur as a consequence of a data breach EXCEPT _____.
A) lawsuits
B) fines for violating industry regulations
C) a massive reduction in consumer confidence
D) fines from payment card issuers
Answer: A
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-4: What Are the Legal Consequences of a Data Breach?
Classification: Concept

63) List suggestions for preventing data loss?
Answer: Don't collect more data than necessary. Permanently destroy old data. Limit the number of places data is stored. Limit employee access to data necessary to perform their job. Document access to critical data. Develop effective termination procedures to prevent data theft. Develop policies that govern offsite data storage and use. Encrypt data when possible. Provide training to users about data security stands.
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-5: How Can Data Breaches Be Prevented?
Classification: Concept

64) Companies can implement measures that make data breaches impossible.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-5: How Can Data Breaches Be Prevented?
Classification: Concept

65) If a company wants to prevent a SQL injection attack, all they have to do is train their users.
Answer: FALSE
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-5: How Can Data Breaches Be Prevented?
Classification: Concept

66) Which company had the largest data breach in history?
A) Target
B) Yahoo!
C) Google
D) Twitter
Answer: B
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-1: What Is a Data Breach?
Classification: Concept

67) _____ is among the most difficult parts of a data breach to manage.
A) Responding quickly to all parties
B) Working with law enforcement
C) The negative fallout
D) Resolving the problem
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-3: How Should Organizations Respond to Data Breaches?
Classification: Application

68) All of the following legal actions can occur as a consequence of a data breach EXCEPT _____.
A) lawsuits
B) fines for violating industry regulations
C) a massive reduction in consumer confidence
D) fines from payment card issuers
Answer: B
AACSB: Information Technology
Difficulty: 2: Moderate
Course LO: Discuss the ethical and social issues raised by the use of information systems.
Learning Obj: LO CE14-4: What Are the Legal Consequences of a Data Breach?
Classification: Concept

69) As a starting point, organizations should _____ to ensure sufficient executive support to prevent data breaches?
A) check all vendor credentials
B) develop countermeasures
C) hire a chief information security officer (CISO)
D) hire ex-hackers to examine the system
Answer: C
AACSB: Information Technology
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-5: How Can Data Breaches Be Prevented?
Classification: Concept

70) Which of the following password guidelines are the easiest to crack?
A) a six-letter password with upper and lower-case letters
B) a ten-digit password with only uppercase letters
C) a password with special characters
D) a twelve-digit password with letters only
Answer: B
AACSB: Reflective Thinking
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-6: What Is Your Role in IS Security?
Classification: Application

71) Every system ultimately depends on _____.
A) the dependability of the firewall
B) the behavior of its users
C) strong security protocols
D) an advanced authentication system
Answer: A
AACSB: Reflective Thinking
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-6: What Is Your Role in IS Security?
Classification: Application

72) What is the best way to create a longer, more complicated password that is easy to remember?
A) Write it on a piece of paper.
B) Base them on the first letter of the words in a phrase.
C) Tell a close co-worker.
D) Make the password hint the same as the password.
Answer: A
AACSB: Reflective Thinking
Difficulty: 1: Easy
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-6: What Is Your Role in IS Security?
Classification: Application

73) Briefly describe password etiquette.
Answer: Once you have created a strong password, you need to protect it with proper behavior. Proper password etiquette is one of the marks of a business professional. Never write down your password, and do not share it with others. Never ask others for their passwords, and never give your password to someone else. If someone asks for your password, do not give it out. Instead, get up, go over to that person's machine, and enter your password yourself. Stay present while your password is in use, and ensure that your account is logged out at the end of the activity. No one should mind or be offended in any way when you do this. It is the mark of a professional.
AACSB: Reflective Thinking
Difficulty: 2: Moderate
Course LO: Describe different methods of managing IS security.
Learning Obj: LO CE14-6: What Is Your Role in IS Security?
Classification: Application