

## Chapter14

### True/False

*Indicate whether the statement is true or false.*

- 1. Blackout units are a solution to extreme changes in voltage, and can provide several minutes to several hours of backup battery power.
- 2. In recent years, identity theft has been more prevalent as part of phishing.
- 3. Computer “infections” are so named because they act on programs and data in a fashion similar to the way viruses act on living tissue.
- 4. Intentional damage to software occurs because of poor training, lack of adherence to simple backup procedures, or simple human error.
- 5. Bots are implemented not only for access but also to implement policies and ensure that nonsensical data is not entered into corporate databases.
- 6. Controls translate business policies into system features.
- 7. IS managers encourage users to change their user IDs frequently.
- 8. Several manufacturers of computer equipment offer individual keyboard-embedded and mouse-embedded fingerprint devices.
- 9. Atomic transactions ensure encrypting of all appropriate files.
- 10. The best defense against unauthorized access to systems over the Internet is a firewall, which is hardware and software that blocks access to computing resources.
- 11. With encryption, the original message is called plaintext.
- 12. Symmetric encryption is also called “public-key” encryption.
- 13. A protocol called Transport Layer Security (TLS) is used for transactions on the Web.
- 14. A digital certificate contains its holder’s name, a serial number, expiration dates, and a copy of the certificate holder’s public key (used to encrypt messages and digital signatures).
- 15. The recipient of an encrypted message uses the certificate authority’s private key to decode the digital certificate attached to the message.
- 16. Encryption slows down communication because the software must encrypt and decrypt every message.
- 17. Companies that choose not to fully develop their own recovery plan can outsource it to companies that specialize in either disaster recovery planning or provision of alternative sites.

- \_\_\_ 18. Copies of applications are usually kept in a safe place to replace those that get damaged.
- \_\_\_ 19. Redundancies increase expected downtime.
- \_\_\_ 20. The greater the number of interdependent systems, the greater the expected downtime.

### Multiple Choice

*Identify the choice that best completes the statement or answers the question.*

- \_\_\_ 21. In \_\_\_\_, the voltage of the power decreases, or there are very short interruptions in the flow of power.
- |              |                      |
|--------------|----------------------|
| a. brownouts | c. keystroke logging |
| b. blackouts | d. UPSs              |
- \_\_\_ 22. \_\_\_\_ software records individual keystrokes.
- |                      |                  |
|----------------------|------------------|
| a. Clickstream       | c. Virus         |
| b. Keystroke logging | d. Remote access |
- \_\_\_ 23. Con artists use tricks known as \_\_\_\_.
- |                     |                       |
|---------------------|-----------------------|
| a. social pathology | c. social engineering |
| b. knowledge theft  | d. data mining        |
- \_\_\_ 24. A \_\_\_\_ is a bogus record in a networked database that neither employees nor business partners would ever access for legitimate purposes.
- |             |               |
|-------------|---------------|
| a. honeypot | c. flame      |
| b. phish    | d. honeytoken |
- \_\_\_ 25. A \_\_\_\_ is a server that contains a mirrored copy of a production database (a database that is used for business operations), or one with invalid records.
- |               |                 |
|---------------|-----------------|
| a. honeytoken | c. bogus server |
| b. phish      | d. honeypot     |
- \_\_\_ 26. One way to protect against viruses is to use \_\_\_\_, which is readily available on the market from companies that specialize in developing this kind of software, such as Symantec and McAfee.
- |                       |                       |
|-----------------------|-----------------------|
| a. antiphish software | c. antivirus software |
| b. security worms     | d. secure viruses     |
- \_\_\_ 27. \_\_\_\_ are usually planted by insiders, that is, employees of the victimized organization.
- |                |            |
|----------------|------------|
| a. Spams       | c. Phishes |
| b. Logic bombs | d. Flames  |
- \_\_\_ 28. \_\_\_\_ occurs when a Web site receives an overwhelming number of information requests, such as merely logging on to a site.
- |                                    |                                  |
|------------------------------------|----------------------------------|
| a. Denial-of-service (DoS)         | c. Global attack                 |
| b. Global denial-of-service (GDoS) | d. Full denial-of-service (FDoS) |
- \_\_\_ 29. \_\_\_\_ a computer means using some or all of the resources of a computer linked to a public network without the consent of its owner.
- |              |                 |
|--------------|-----------------|
| a. Hijacking | c. Phishing     |
| b. Attacking | d. Sequestering |
- \_\_\_ 30. Hijacking is carried out by surreptitiously installing a small program called a \_\_\_\_ on a computer.
- |         |         |
|---------|---------|
| a. mine | c. spot |
|---------|---------|



- a. SSL
  - b. SDLC
  - c. DoS
  - d. SSO
- \_\_\_ 44. The \_\_\_\_, as it is popularly known, gives law enforcement agencies surveillance and wiretapping rights they did not have before 2001.
- a. PATRIOT Act
  - b. 9/11 Decree
  - c. 9/11 Act
  - d. PATRIOT Manifesto
- \_\_\_ 45. When tapping communications, law enforcement agencies need the cooperation of a third party, such as a telephone company or a(n) \_\_\_\_.
- a. ISP
  - b. SSP
  - c. Web site
  - d. systems developer
- \_\_\_ 46. \_\_\_\_, those without which the business cannot conduct its operations, are given the highest priority by the disaster recovery coordinator.
- a. Backup applications
  - b. Up applications
  - c. Mission-critical applications
  - d. Recovery applications
- \_\_\_ 47. CIOs often find the tasks of earmarking funds for \_\_\_\_ difficult because they cannot show the return on investment (ROI) of such planning.
- a. backup programs
  - b. disaster recovery programs
  - c. archival programs
  - d. database security programs
- \_\_\_ 48. Experts are usually employed to estimate the cost and \_\_\_\_ of damages, as well as the cost of security measures.
- a. impact
  - b. probabilities
  - c. effect
  - d. causes
- \_\_\_ 49. Managers should focus on the asset they must protect, which in most cases is \_\_\_\_, not applications.
- a. hardware
  - b. software
  - c. information
  - d. systems
- \_\_\_ 50. Experience in \_\_\_\_ certain systems, such as ERP and SCM systems, can teach the IT staff for how many minutes or seconds per year the system is likely to fail.
- a. operating
  - b. developing
  - c. maintaining
  - d. archiving

### Completion

Complete each statement.

51. \_\_\_\_\_, the time during which ISs or data are not available in the course of conducting business, has become a dreaded situation for almost every business worldwide.
52. \_\_\_\_\_ are total losses of electrical power.
53. To ensure against interruptions in power supply, organizations use \_\_\_\_\_ systems, which provide an alternative power supply for a short time, as soon as a power network fails.
54. Once criminals have a person's identifying details, such as a Social Security number, driver's license number, or credit-card number, they can pretend to be this person, which is a crime called \_\_\_\_\_.

55. Some viruses are called \_\_\_\_\_, analogous to the destructive gift given to the ancient Trojans.
56. A(n) \_\_\_\_\_ is software that is programmed to cause damage at a specified time to specific applications and data files.
57. \_\_\_\_\_ occurs when a Web site receives an overwhelming number of information requests, such as merely logging on to a site.
58. \_\_\_\_\_ are constraints and other restrictions imposed on a user or a system, and they can be used to secure systems against risks or to reduce damage caused to systems, applications, and data.
59. Probably the easiest way to protect against loss of data is to automatically duplicate all data periodically, a process referred to as data \_\_\_\_\_.
60. A(n) \_\_\_\_\_ characteristic is a unique physical, measurable characteristic of a human being that is used to identify a person.
61. One popular tracking tool is the \_\_\_\_\_: a series of documented facts that help detect who recorded which transactions, at what time, and under whose approval.
62. The audit trail is the most important tool of the \_\_\_\_\_, the professional whose job it is to find erroneous or fraudulent cases and investigate them.
63. \_\_\_\_\_ is the process of ensuring that the person who sends a message to or receives a message from you is indeed that person.
64. When both the sender and recipient use the same secret key, the technique is called \_\_\_\_\_.
65. A(n) \_\_\_\_\_ is a way to authenticate online messages, analogous to a physical signature on a piece of paper, but implemented with public-key cryptography.
66. \_\_\_\_\_ are computer files that serve as the equivalent of ID cards by associating one's identity with one's public key.
67. To prepare for mishaps, either natural or malicious, many organizations have well-planned programs in place, called \_\_\_\_\_.
68. \_\_\_\_\_ provide backup and operation facilities to which a client's employees can move and continue operations in case of a disaster.
69. The cost of damage is the aggregate of all the potential damages multiplied by their respective \_\_\_\_\_.
70. There might be no point in spending much money to increase the " \_\_\_\_\_" of uptime for every system.