**Solutions for Review Questions**

Chapter 1

1. Ian recently earned his security certification and has been offered a promotion to a position that requires him to analyze and design security solutions as well as identifying users’ needs. Which of these generally recognized security positions has Ian been offered?
2. **Security administrator**
3. Security technician
4. Security officer
5. Security manager
6. Alyona has been asked by her supervisor to give a presentation regarding reasons why security attacks continue to be successful. She has decided to focus on the issue of widespread vulnerabilities. Which of the following would Alyona NOT include in her presentation?
7. Large number of vulnerabilities
8. End-of-life systems
9. Lack of vendor support
10. **Misconfigurations**
11. Tatyana is discussing with her supervisor potential reasons why a recent attack was successful against one of their systems. Which of the following configuration issues would NOT covered?
12. Default configurations
13. Weak configurations
14. **Vulnerable business processes**
15. Misconfigurations
16. What is a race condition?
17. When a vulnerability is discovered and there is a raceto see if it can be patched before it is exploited by attackers.
18. **When two concurrent threads of execution access a shared resource simultaneously, resulting in unintended consequences.**
19. When an attack finishes its operation before antivirus can complete its work.
20. When a software update is distributed prior to a vulnerability being discovered.
21. Which the following is NOT a reason why it is difficult to defend against today’s attackers?
22. Delays in security updating
23. **Greater sophistication of defense tools**
24. Increased speed of attacks
25. Simplicity of attack tools
26. Which of the following is NOT true regarding security?
27. Security is a goal.
28. Security includes the necessary steps to protect from harm.
29. Security is a process.
30. **Security is a war that must be won at all costs.**
31. Adone is attempting to explain to his friend the relationship between security and convenience. Which of the following statements would he use?
32. “Security and convenience are not related.”
33. “Convenience always outweighs security.”
34. **“Security and convenience are inversely proportional.”**
35. “Whenever security and convenience intersect, security always wins.”
36. Which of the following ensures that only authorized parties can view protected information?
37. Authorization
38. **Confidentiality**
39. Availability
40. Integrity
41. Which of the following is NOT a successive layer in which information security is achieved?
42. Products
43. People
44. Procedures
45. **Purposes**
46. Complete this definition of information security: *That which protects the integrity, confidentiality, and availability of information* \_\_\_\_\_.
47. *on electronic digital devices and limited analog devices that can connect via the Internet or through a local area network.*
48. *through a long-term process that results in ultimate security.*
49. *using both open-sourced as well as supplier-sourced hardware and software that interacts appropriately with limited resources.*
50. ***through products, people, and procedures on the devices that store, manipulate, and transmit the information.***
51. Which of the following is an enterprise critical asset?
52. System software
53. **Information**
54. Outsourced computing services
55. Servers, routers, and power supplies
56. Gunnar is creating a document that explains risk response techniques. Which of the following would he NOT list and explain in his document?
57. **Extinguish risk**
58. Transfer risk
59. Mitigate risk
60. Avoid risk
61. Which act requires banks and financial institutions to alert their customers of their policies in disclosing customer information?
62. Sarbanes-Oxley Act (Sarbox)
63. Financial and Personal Services Disclosure Act
64. Health Insurance Portability and Accountability Act (HIPAA)
65. **Gramm-Leach-Bliley Act (GLBA)**
66. Why do cyberterrorists target power plants, air traffic control centers, and water systems?
67. These targets are government-regulated and any successful attack would be considered a major victory.
68. These targets have notoriously weak security and are easy to penetrate.
69. **They can cause significant disruption by destroying only a few targets.**
70. The targets are privately owned and cannot afford high levels of security.
71. Which tool is most commonly associated with nation state threat actors?
72. Closed-Source Resistant and Recurrent Malware (CSRRM)
73. **Advanced Persistent Threat** **(APT)**
74. Unlimited Harvest and Secure Attack (UHSA)
75. Network Spider and Worm Threat (NSAWT)
76. An organization that practices purchasing products from different vendors is demonstrating which security principle?
77. Obscurity
78. **Diversity**
79. Limiting
80. Layering
81. What is an objective of state-sponsored attackers?
82. To right a perceived wrong
83. To amass fortune over of fame
84. **To spy on citizens**
85. To sell vulnerabilities to the highest bidder
86. Signe wants to improve the security of the small business where she serves as a security manager. She determines that the business needs to do a better job of not revealing the type of computer, operating system, software, and network connections they use. What security principle does Signe want to use?
87. **Obscurity**
88. Layering
89. Diversity
90. Limiting
91. What are industry-standard frameworks and reference architectures that are required by external agencies known as?
92. Compulsory
93. Mandatory
94. Required
95. **Regulatory**
96. What is the category of threat actors that sell their knowledge of vulnerabilities to other attackers or governments?
97. Cyberterrorists
98. Competitors
99. **Brokers**
100. Resource managers