Security Awareness 5e 9781305500372

Review Question Answers

Chapter 1 Review Questions

1. Each of the following is a reason why it is difficult to defend against today’s attackers except \_\_\_\_\_\_\_.
2. faster detection of vulnerabilities
3. **complexity of attack tools**
4. user confusion
5. greater sophistication of attacks
6. In a general sense “security” is \_\_\_\_\_\_\_.
7. only available on specialized computers
8. protection from only direct actions
9. **the steps necessary to protect a person or property from harm**
10. something that can relatively easy to achieve
11. \_\_\_\_\_ ensures that only authorized parties can view the information.
12. Integrity
13. **Confidentiality**
14. Availability
15. Authorization
16. Why can brokers command such a high price for what they sell?
17. Brokers are licensed professionals.
18. The attack targets are always wealthy corporations.
19. **The vulnerability they uncover was previously unknown and is unlikely to be patched quickly.**
20. Brokers work in teams and all the members must be compensated.
21. Each of the following is a successive layer in which information security is achieved except \_\_\_\_\_\_\_.
22. policies and procedures
23. people
24. products
25. **purposes**
26. What is a person or element that has the power to carry out a threat?
27. exploiter
28. **threat agent**
29. hazard element
30. risk agent
31. In information security terminology a(n) \_\_\_\_\_ is a flaw or weakness that allows an attacker to bypass security protections.
32. access
33. **vulnerability**
34. worm hole
35. access control
36. \_\_\_\_\_ ensures that individuals are who they claim to be.
37. Demonstration
38. **Authentication**
39. Accounting
40. Certification
41. The \_\_\_\_\_ requires that enterprises must guard protected health information and implement policies and procedures to safeguard it.
42. Hospital Protection and Insurance Association Agreement (HPIAA)
43. Sarbanes-Oxley Act (Sarbox)
44. Gramm-Leach-Bliley Act (GLBA)
45. **Health Insurance Portability and Accountability Act (HIPAA)**
46. The motivation of \_\_\_\_\_ is attacking for the sake of their principles or beliefs.
47. **cyberterrorists**
48. insiders
49. script kiddies
50. computer spies
51. What is the difference between a hactivist and a cyberterrorist?
52. A hactivist is motivated by ideology while a cyberterrorist is not.
53. Cyberterrorists always work in groups while hactivists work alone.
54. **The aim of a hactivist is not to incite panic like cyberterrorists.**
55. Cyberterrorists are better funded than hactivists.
56. Keeping backup copies of important data stored in a safe place is an example of
57. **minimizing losses**
58. sending secure information
59. blocking attacks
60. layering
61. Each of the following can be classified as an “insider” except \_\_\_\_\_\_\_.
62. business partners
63. contractors
64. **cybercriminals**
65. employees
66. What is an objective of state-sponsored attackers?
67. to right a perceived wrong
68. **to spy on citizens**
69. to sell vulnerabilities to the highest bidder
70. fortune over fame
71. Each of the following is a characteristic of cybercriminals except \_\_\_\_\_\_\_.
72. **low motivation**
73. better funded
74. less risk averse
75. more tenacious
76. Each of the following is a characteristic of cybercrime except\_\_\_\_\_\_.
77. unauthorized attempts to access to information
78. targeted attacks against financial networks
79. **exclusive use of worms and viruses**
80. theft of personal information
81. An example of a(n) \_\_\_\_\_ is a software defect in an operating system that allows an unauthorized user to gain access to a computer without a password.
82. asset exploit (AE)
83. threat agent
84. **vulnerability**
85. threat
86. \_\_\_\_\_ requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information and to protect all electronic and paper containing personally identifiable financial information.
87. California Savings and Loan Security Act (CS&LSA)
88. Sarbanes-Oxley Act (Sarbox)
89. **Gramm-Leach-Bliley Act (GLBA)**
90. USA Patriot Act
91. \_\_\_\_\_ ensures that the information is correct and no unauthorized person or malicious software has altered that data.
92. **integrity**
93. obscurity
94. layering
95. confidentiality
96. Protecting information is accomplished by
97. **protecting the devices on which the information is found**
98. securing only local servers
99. hiring an Information Security Officer (CISO)
100. reducing risk factors