1. data	**2.** information assets
3. information	**4.** media
5. database security	**6.** data security
7. databases	**8.** attack
9. exploits	**10.** vulnerabilities

2. The focus of information security; information that has value to the organization, and the systems that store, process, and transmit the information.	**1.** Items of fact collected by an organization. Data includes raw numbers, facts, and words. Student quiz scores are a simple example of data.
4. As a subset of information assets, the systems and networks that store, process, and transmit information.	**3.** Data that has been organized, structured, and presented to provide additional insight into its context, worth, and usefulness. For example, a student's class average can be presented in the context of its value, as in "90=A".
6. Commonly used as a surrogate for information security, data security is the focus of protecting data or information in its various states—at rest (in storage), in processing, and in transmission (over networks).	**5.** A subset of information security that focuses on the assessment and protection of information stored in data repositories like database management systems and storage media.
8. An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it. Attacks can be active or passive and direct or indirect.	**7.** A collection of related data stored in a structured form and usually managed by a database management system.
10. A potential weakness in an asset or its defensive control system(s).	**9.** A technique used to compromise a system.

11. intellectual property (IP)	**12.** software piracy
13. availability disruption	**14.** service level agreement (SLA)
15. downtime	**16.** uptime
17. spike	**18.** surge
19. fault	**20.** sag

12. The unauthorized duplication, installation, or distribution of copyrighted computer software, which is a violation of intellectual property.	**11.** The creation, ownership, and control of original ideas as well as the representation of those ideas.
14. A document or part of a document that specifies the expected level of service from a service provider. An SLA usually contains provisions for minimum acceptable availability and penalties or remediation procedures for downtime.	**13.** An interruption in service, usually from a service provider, which causes an adverse event within an organization.
16. The percentage of time a particular service is available; the opposite of downtime.	**15.** The percentage of time a particular service is not available; the opposite of uptime.
18. A long-term increase in electrical power availability.	**17.** A short-term increase in electrical power availability, also known as a swell.
20. A short-term decrease in electrical power availability.	**19.** A short-term interruption in electrical power availability.

21. competitive intelligence	**22.** brownout
23. noise	**24.** blackout
25. shoulder surfing	**26.** trespass
27. industrial espionage	**28.** hacker
29. expert hacker	**30.** professional hacker

22. A long-term decrease in electrical power availability.	**21.** The collection and analysis of information about an organization's business competitors through legal and ethical means to gain business intelligence and competitive advantage.
24. A long-term interruption (outage) in electrical power availability.	**23.** The presence of additional and disruptive signals in network communications or electrical power delivery. Also, noise can be alarm events that are accurate and noteworthy but do not pose significant threats to information security. Unsuccessful attacks are the most common source of IDPS noise, although some noise
26. Unauthorized entry into the real or virtual property of another party.	**25.** The direct, covert observation of individual information or system use.
28. A person who accesses systems and information without authorization and often illegally.	**27.** The collection and analysis of information about an organization's business competitors, often through illegal or unethical means, to gain an unfair competitive advantage. Also known as corporate spying, which is distinguished from espionage for national security reasons.
30. A hacker who conducts attacks for personal financial benefit or for a crime organization or foreign government. Not to be confused with a penetration tester.	**29.** A hacker who uses extensive knowledge of the inner workings of computer hardware and software to gain unauthorized access to systems and information. Also known as elite hackers, expert hackers often create automated exploits, scripts, and tools used by other hackers.

31. novice hacker	**32.** penetration tester
33. script kiddies	**34.** packet monkeys
35. privilege escalation	**36.** jailbreaking
37. rooting	**38.** cracker
39. Phreakers	**40.** cracking

32. An information security professional with authorization to attempt to gain system access in an effort to identify and recommend resolutions for vulnerabilities in those systems.	**31.** A relatively unskilled hacker who uses the work of expert hackers to perform attacks. Also known as a neophyte, n00b, or newbie. This category of hackers includes script kiddies and packet monkeys.
34. A script kiddie who uses automated exploits to engage in denial-of-service attacks.	**33.** A hacker of limited skill who uses expertly written software to attack a system. Also known as skids, skiddies, or script bunnies.
36. Escalating privileges to gain administrator-level or root access control over a smartphone operating system (typically associated with Apple iOS smartphones). See also *rooting*.	**35.** The unauthorized modification of an authorized or unauthorized system user account to gain advanced access and control over system resources.
38. A hacker who intentionally removes or bypasses software copyright protection designed to prevent unauthorized duplication or use.	**37.** Escalating privileges to gain administrator-level control over a computer system (including smartphones). Typically associated with Android OS smartphones. See also *jailbreaking*.
40. Attempting to reverse-engineer, remove, or bypass a password or other access control protection, such as the copyright protection on software. See *cracker*.	**39.** A hacker who manipulates the public telephone system to make free calls or disrupt services.

41. dictionary password attack	**42.** 10.4 password rule
43. brute force password attack	**44.** rainbow table
45. social engineering	**46.** advance-fee fraud (AFF)
47. Pretexting	**48.** phishing
49. spear phishing	**50.** hacktivist

42.
An industry recommendation for password structure and strength that specifies passwords should be at least 10 characters long and contain at least one uppercase letter, one lowercase letter, one number, and one special character.

41.
A variation of the brute force password attack that attempts to narrow the range of possible passwords guessed by using a list of common passwords and possibly including attempts based on the target's personal information.

44.
A table of hash values and their corresponding plaintext values that can be used to look up password values if an attacker is able to steal a system's encrypted password file.

43.
An attempt to guess a password by attempting every possible combination of characters and numbers in it.

46.
A form of social engineering, typically conducted via e-mail, in which an organization or some third party indicates that the recipient is due an exorbitant amount of money and needs only a small advance fee or personal banking information to facilitate the transfer.

45.
The process of using social skills to convince people to reveal access credentials or other valuable information to an attacker.

48.
A form of social engineering in which the attacker provides what appears to be a legitimate communication (usually e-mail), but it contains hidden or embedded code that redirects the reply to a third-party site in an effort to extract personal or confidential information.

47.
A form of social engineering in which the attacker pretends to be an authority figure who needs information to confirm the target's identity, but the real object is to trick the target into revealing confidential information. Pretexting is commonly performed by telephone.

50.
A hacker who seeks to interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency.

49.
Any highly targeted phishing attack.

51. Information extortion	**52.** ransomware
53. cyberwarfare	**54.** cyberterrorism
55. cyberactivist	**56.** Malware
57. malicious code	**58.** zero-day attack
59. malicious software	**60.** Spyware

52. Computer software specifically designed to identify and encrypt valuable information in a victim's system in order to extort payment for the key needed to unlock the encryption.	**51.** The act of an attacker or trusted insider who steals or interrupts access to information from a computer system and demands compensation for its return or for an agreement not to disclose the information.
54. A hacker who attacks systems to conduct terrorist activities via networks or Internet pathways.	**53.** Formally sanctioned offensive operations conducted by a government or state against information or systems of another government or state. Sometimes called information warfare.
56. Computer software specifically designed to perform malicious or unwanted actions.	**55.** See *hacktivist*.
58. An attack that makes use of malware that is not yet known by the anti-malware software companies.	**57.** See *malware*.
60. Any technology that aids in gathering information about people or organizations without their knowledge.	**59.** See *malware*.

61. adware	**62.** macro virus
63. virus	**64.** boot virus
65. non-memory-resident viruses	**66.** memory-resident viruses
67. Trojan horses	**68.** worms
69. virus hoaxes	**70.** polymorphic threat

62. A type of virus written in a specific macro language to target applications that use the language. The virus is activated when the application's product is opened. A macro virus typically affects documents, slideshows, e-mails, or spreadsheets created by office suite applications.	**61.** Malware intended to provide undesired marketing and advertising, including pop-ups and banners on a user's screens.
64. Also known as a boot sector virus, a type of virus that targets the boot sector or Master Boot Record (MBR) of a computer system's hard drive or removable storage media.	**63.** A type of malware that is attached to other executable programs. When activated, it replicates and propagates itself to multiple systems, spreading by multiple communications vectors. For example, a virus might send copies of itself to all users in the infected system's e-mail program.
66. A virus that is capable of installing itself in a computer's operating system, starting when the computer is activated, and residing in the system's memory even after the host application is terminated. Also known as a resident virus.	**65.** A virus that terminates after it has been activated, infected its host system, and replicated itself. NMR viruses do not reside in an operating system or memory after executing. Also known as a non-resident virus.
68. A type of malware that is capable of activation and replication without being attached to an existing program.	**67.** A malware program that hides its true nature and reveals its designed behavior only when activated.
70. Malware (a virus or worm) that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures.	**69.** A message that reports the presence of a nonexistent virus or worm and wastes valuable time as employees share the message.

71. back door	**72.** maintenance hook
73. trap door	**74.** bots
75. distributed denial-of-service (DDoS) attack	**76.** denial-of-service (DoS) attack
77. zombies	**78.** packet sniffer
79. mail bomb	**80.** Spam

72. See *back door*.	**71.** A malware payload that provides access to a system by bypassing normal access controls. A back door may also be an intentional access control bypass left by a system designer to facilitate development.
74. An abbreviation of *robot*, an automated software program that executes certain commands when it receives a specific input. See also *zombie*.	**73.** See *back door*.
76. An attack that attempts to overwhelm a computer target's ability to handle incoming communications, prohibiting legitimate users from accessing those systems.	**75.** A form of DoS attack in which a coordinated stream of requests is launched against a target from many locations at the same time using bots or zombies.
78. A software program or hardware appliance that can intercept, copy, and interpret network traffic.	**77.** See *bot*.
80. Undesired e-mail, typically commercial advertising transmitted in bulk.	**79.** An attack designed to overwhelm the receiver with excessive quantities of e-mail.

81. sniffer	**82.** spoofing
83. Pharming	**84.** Domain Name System (DNS) cache poisoning
85. man-in-the-middle	**86.** TCP hijacking
87. session hijacking	**88.** mean time between failure (MTBF)
89. mean time to failure (MTTF)	**90.** MTTD

82.
A technique for gaining unauthorized access to computers using a forged or modified source IP address to give the perception that messages are coming from a trusted host.

81.
See *packet sniffer*.

84.
The intentional hacking and modification of a DNS database to redirect legitimate traffic to illegitimate Internet locations. Also known as DNS spoofing.

83.
The redirection of legitimate user Web traffic to illegitimate Web sites with the intent to collect personal information.

86.
A form of man-in-the-middle attack whereby the attacker inserts himself into TCP/IP-based communications. TCP/IP is short for Transmission Control Protocol/Internet Protocol.

85.
A group of attacks whereby a person intercepts a communications stream and inserts himself in the conversation to convince each of the legitimate parties that he is the other communications partner. Some man-in-the-middle attacks involve encryption functions.

88.
The average amount of time between hardware failures, calculated as the total amount of operation time for a specified number of units divided by the total number of failures.

87.
See *TCP hijacking*.

90.
The average amount of time a computer repair technician needs to determine the cause of a failure.

89.
The average amount of time until the next hardware failure.

91. buffer overrun (or buffer overflow)	**92.** command injection
93. MTTR	**94.** Cross-site scripting (XSS)
95. integer bug	**96.** theft

92. An application error that occurs when user input is passed directly to a compiler or interpreter without screening for content that may disrupt or compromise the intended function.	**91.** An application error that occurs when more data is sent to a program buffer than it is designed to handle.
94. A Web application fault that occurs when an application running on a Web server inserts commands into a user's browser session and causes information to be sent to a hostile server.	**93.** The average amount of time a computer repair technician needs to resolve the cause of a failure through replacement or repair of a faulty unit.
96. The illegal taking of another's property, which can be physical, electronic, or intellectual.	**95.** A class of computational error caused by methods that computers use to store and manipulate integer numbers; this bug can be exploited by attackers.