1. Antimalware solutions, such as antivirus scanners and real-time threat protection, have become a necessity in modern security solutions. What are the two main qualities of data that they protect? Choose the best answer.

A. Data backups and data restores.
B. Data integrity and data confidentiality.
C. Threat mitigation and data preservation.
D. Data compression and active threat protection.
E. None of the above.

Correct answer: B.

Explanation: Antivirus and antimalware scanners scan system files and other data to make sure that it hasn't been corrupted, thus protecting the data's integrity. Furthermore, by removing spyware, rootkits, and preventing hackers from accessing system data, they also protect it's confidentiality. All other answers are incorrect.

2. The security department of your firm requires a block cipher solution with a relatively small key-length to facilitate encryption. Which of the following should you implement? Select all that apply.

A. Rivest Cipher 2
B. Rivest Cipher 3
C. Rivest Cipher 4
D. AES-256
E. AES-2048
F. Blowfish
G. None of the above.

Correct answer: F.

Explanation: While there is such thing as RC2, there is no such thing as RC3. At any rate, the Rivest Ciphers are not correct, and AES keys are much longer than other alternatives. In fact, AES most commonly comes in the 128-bit and 256-bit varieties. However, Blowfish offers dynamic key lengths anywhere from 32 to 448 bits in length, which provides the most flexibility.

3. Users need to be trained to blow whistles when they discover a violation of a firm's security policies. What topic relates to the actions (such as blowing a whistle) an employee should take if they notice a stranger strolling around a secured area without a visitor's pass, badge, escort, or proper clearance? Select all that apply.

A. Situational awareness
B. Threat response policy
C. Whistle blowing policy
D. Security on demand
E. None of the above

Correct answer: A.

Explanation: Within the context of I.T. security, Situational Awareness is defined as:

Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.

The other answers aren't even real terms or concepts.

4. Virtualization technologies have become ubiquitous in most modern I.T. service delivery models and corporate information infrastructures. Which of the following is true regarding virtualization technologies? Select all that apply.

A. Virtualization aggregates servers and services, making them more susceptible to attacks.
B. Virtualization technologies melds the roles of multiple servers into a single system, which doesn't isolate individual nodes.
C. Virtualization isolates individual nodes and separates the functions and operation of services.
D. Virtualization is simply a security technology that allows firewall resources and operations to be run on other devices, such as routers and network switches.
E. None of the above.
F. All of the above.

Correct answer: C.

Explanation: The only correct answer here is C, and it's mutually exclusive with some of the other answers. Though one hardware failure could affect multiple virtual machines, from a data corruption, system failure, and malware perspective, they are much more secure due to isolation of operating systems and services.

5. You work for a small-sized firm that is growing rapidly, and hiring new employees while also promoting from within. As such, users' roles within the firm are constantly changing, so you have been given the task of auditing user accounts, groups, and privileges. Which of the following need to be performed? Select the best two options.

A. Meet with security personnel and identify which systems, services, and resources should be audited.
B. Immediately suspend accounts that you suspect have too many privileges.
C. Activate auditing tools at the operating-system level.
D. Begin by auditing backups, since they likely contain a lot of sensitive information.
E. Only one of the above options is correct.

Correct answer: A, C.

Explanation: You simply must have some type of logging and auditing tool at the operating-system level, and you cannot possibly hope to implement the correct policies without first identifying who needs access to what.

6. The security department of a large firm is concerned about limiting access to their corporate network infrastructure, yet using wireless network technologies is a necessity, despite their security flaws. What can be done to limit the visibility and accessibility of wireless access points? Select all that apply.

A. Don't tell anyone the GUID of the wireless network.
B. Implement QoS technologies to rate-limit and throttle wireless connections from unknown hosts.
C. Scrap the wireless portion of the network infrastructure and run Ethernet cables to provide network access.
D. Configure WAPs to stop broadcasting their SSIDs.
E. None of the above.

Correct answer: D.

Explanation: One of the best ways to hide wireless networks is to stop them from broadcasting their SSIDs. Thus, in order for a user to connect to the network, they first need to know that it exists beforehand. This will prevent stray users and hackers from seeing the network populate in their list of wireless connections, and can help mitigate attacks such as war driving.

7. Super users and high-level officials, especially in an I.T. department, can gain too many network privileges and inadvertently represent a security threat to the network, especially through poor change management. What is the term that describes limiting the power of individual users and roles to mitigate risks?

A. Separation of powers.
B. Checks and balances.
C. Acceptable use policy.
D. Separation of duties.
E. None of the above.

Correct answer: D.

Explanation: Separation of powers, as well as check and balances, are both concepts that relate to dividing power in a government to prevent a single party from becoming too powerful. However, from a security perspective, a separation of duties will prevent one person from having too much access to the infrastructure.

8. You work for a medium-sized firm that uses LDAP to manage user authentication, though there have been recent attacks against the LDAP system. Which of the following accurately details LDAP injection attacks? Select the best answer.

A. Exploiting vulnerabilities in an LDAP system via queries designed to cause malfunctions in order to edit permissions or gain access to other systems.
B. Injecting and LDAP server with a malicious payload designed to disrupt other users' access to LDAP authentication.
C. Overwhelming and LDAP server from multiple nodes in order to deny access.
D. Physically breaking connections, such as Ethernet cables and connectors, to disable an LDAP system.
E. None of the above.

Correct answer: A.

Explanation: The whole point of LDAP is to manage authentication and login activities. If a hacker is able to successfully hack an LDAP system, they'll be able to manipulate user and group access permissions, and potentially escalate their own privileges.

9. Which of the following accurately describes the concept of an attack surface? Select all that apply.

A. An attack surface is the range of vulnerabilities and services that can be used to exploit a vulnerability.
B. An attack service describes a single point of entry, such as a network interface.
C. Attack surfaces are essentially matrix ciphers that can be used to execute malicious payloads.
D. Attack surfaces include flaws in physical-access security systems, such as a key-card entry system.
E. None of the above.

Correct answer: A.

Explanation: An attack surface is defined as the aggregate or sum of weaknesses and vulnerabilities that an attacker can target to potentially exploit a system.

10. You work for a medium-sized firm that has implemented visualization technologies to consolidate 6 separate systems onto one physical server. One of the virtual machines, which was running Windows Server, caught a virus that corrupted system files. The remaining 5 virtual machines run Linux server distributions, Windows Server, and virtualized network devices, such as a virtual switch. Which, if any, of the additional virtual machines are threatened by the virus on the Windows Server instance? Choose the best answer.

A. Only the virtual switch.
B. Only the Linux servers.
C. Only the additional Windows instances.
D. Both the Linux and Windows servers.
E. Both the virtual switch and Windows servers.
F. Both the Linux and virtual switch.
G. All additional virtual systems.
H. None of the above.

Correct answer: H.

Explanation: None of the above, because the vast majority of operating-system specific malware is not able to travel between virtual hosts on the same physical server. The virtual systems are isolated from one another, though a hardware failure could impact all of the virtual hosts on a single system.

11. You work for a medium-sized firm that is updating their users' workstations by purchasing new hardware, and your employer decided to destroy the old computers. What is the best course of action to ensure that sensitive and mission-critical data isn't left at risk? Select all that apply.

A. Encrypt the hard drives before sending them to a recycling service.
B. Send the old drives to the proper recycling service as-is.
C. Physically destroy the old drives.
D. Use a file-shredding utility on the hard drives to overwrite data with 1's, 0's, and random patterns to avoid file recovery.
E. None of the above.

Correct answer: C and D.

Explanation: The best way to go about ensuring that old data isn't recovered off of discarded hard drives is to use a file shredder *and* to physically destroy the drives. You see, when a user deletes a file from an operating system, the hard drive most typically just reallocates that space to be once again written over with new data. That is, the file still remains on the hard drive. In fact, there are special utilities that can detect minute variations in magnetism to discern the polarity of individual bits *even after* they have been overwritten. File shredding tools will flip the bits multiple times to prevent file recovery.

12. You are tasked with making a forensic copy of a hard drive and validating that the data contained within the image has its integrity intact. Which of the following, if any, can be used to verify the data's integrity? Choose all that apply.

A. The correct decryption key for the encrypted file image.
B. An image file hash.
C. File shredding software.
D. A bit by bit comparison of the last full backup with the image file.
E. None of the above.

Correct answer: B.

Explanation: Hashes are mathematical formulas that are frequently used to verify data integrity in a variety of different applications, especially with transmission protocols.

13. Which of the following terms accurately describes the process of permanently deleting files from hard drives by scrambling the magnetic polarity and resetting it to zero?

A. Wiping
B. Deleting
C. Degaussing
D. Shredding
E. None of the above

Correct answer: C.

Explanation: Degaussing is the term used to describe the act of wiping a hard drive clean at the bit-level.

14. You notice from numerous file captures that standard HTTP traffic is found on the same network interface as VoIP traffic. What should be done to increase security? Select all that apply.

A. Segment traffic into appropriate VLANs.
B. Create a firewall policy to block VoIP traffic on that particular network interface.
C. Nothing, it's perfectly acceptable as is.
D. Implement QoS procedures to prevent voice traffic from eating up too much bandwidth.
E. None of the above.

Correct answer: A.

Explanation: Traffic needs to be segmented into different VLANs to increase security. Otherwise, it would be possible for end users and attackers to capture, see, and interact with network services they have no business interacting with.

15. You notice from traffic logs that there is a massive spike in WAN bandwidth at 2:00 PM every day, and that the largest spike is due to FTPS traffic. What should you do to ensure that voice calls don't get crowded out by file transfers? Select all that apply.

A. Bar FTPS traffic during this time of the day with a firewall policy.
B. Implement QoS and traffic shaping to conserve WAN bandwidth.
C. Nothing; FTPS traffic always takes priority over voice traffic.
D. Switch to using FTP since it eats up less bandwidth.
E. None of the above.

Correct answer: B.

Explanation: Voice traffic is highly sensitive to latency, and needs to be protected with proper QoS controls.

16. What is the best way to go about storing masses of log files, such as firewall logs and SNMP alerts? Select all that apply.

A. Store the files locally on the devices that generated them for easy access.
B. Logs shouldn't be stored for more than 48 hours to avoid the risk of a paper trail.
C. They should be backed up with a cloud storage provider.
D. Keep them stored on a central storage volume that is kept offline for archiving purposes.
E. None of the above.

Correct answer: D.

Explanation: The best way to store log files is on a central and offline storage medium. That way, your log file archives can't be hacked into (since the device is offline), with exception to physical security breaches.

17. It is impossible to mitigate every risk that poses a threat to your network. So, the security department chooses to create a risk profile for different types of data and services, and to then prioritize security, heavily weighted on cost analysis. What is this concept referred to? Select the best answer.

A. Cost analysis security
B. SWOT analysis
C. Quantitative risk assessment
D. ROI threat analysis
E. None of the above.

Correct answer: C.

Explanation: A SWOT analysis is a business practice used to identify strengths, weaknesses, opportunities, and threats. The correct answer is a quantitative risk assessment. The rest are false and bogus answers.

18. Your firm is weighing the benefits of different security practices, and decides to make it publicly known (through banners on login pages and by posting on the company's website) that any attempt to hack into network services will result in prosecution. What is this concept referred to? Choose the best answer.

A. Proactive threat management
B. Risk deterrence
C. Criminal law
D. Data protection directive
E. None of the above

Correct answer: B.

Explanation: Making it publicly known that a firm will take legal action should they discover their infrastructure has been tampered with is a massive deterrent to would-be hackers and attackers.

19. Why is the NTFS file system superior to FAT32? Select all that apply.

A. It isn't; FAT32 is far superior since it is a newer technology.
B. NTFS encrypts files by default.
C. NTFS is a newer technology, and supports more data storage formats.
D. NTFS uses a hashing algorithm to check data integrity.
E. None of the above.

Correct answer: C.

Explanation: NTFS not only supports more file formats, but it can also partition volumes and disk space larger than FAT32 volumes.

20. What is the term that describes the act of limiting surfaces of vulnerabilities by shutting down unneeded and unused services, ports, and applications? Choose the best answer.

A. As-needed security
B. Active threat mitigation
C. Device hardening
D. Blackout security
E. None of the above

Correct answer: C.

Explanation: Device hardening is the process of shutting down unnecessary services, ports, and applications on a device to limit attack surfaces.