Answers to Practice Exam 1

Answers at a Glance

1. A
2. B
3. C
4. D
5. C
6. C
7. A
8. C
9. C
10. C
11. D
12. C
13. D
14. D and F
15. B
16. B
17. C and F
18. A and F
19. A and E
20. C
21. C
22. C and E
23. A
24. C
25. B
26. C and D
27. B
28. A
29. C
30. D
31. D
32. C
33. B
34. C
35. A and D
36. B
37. A
38. C
39. A and D
40. B
41. A
42. B
43. C
44. D
45. D
46. B
47. D
48. B
49. D
50. C and E
51. D
52. B
53. C
54. C
55. D and F
56. C and E
57. D
58. D
59. C
60. D
61. A
62. C
63. B
64. D
65. C and D
66. B
67. A
68. C
69. A and C
70. C
71. A
72. D
73. C
74. D
75. A and D
76. A
77. B, D, and F
78. B
79. D
80. C

Answers with Explanations

1. Answer: A. Establishing baseline reporting

   Explanation: The key words of the question are "security posture." One of the best methods of monitoring the security posture of your systems is establishing baseline reporting. Baselining is the process of measuring changes in networking, hardware, software, and so on. Creating a baseline consists of selecting something to measure and measuring it consistently for a period of time. It is this baselining (and automated reporting with baselining tools such as Performance Monitor or Wireshark) that allows you to be vigilant and watch over your network carefully in real time.

   See the section "Monitoring Methodologies" in Chapter 13, "Monitoring and Auditing," for more information.

   Incorrect answers: Disabling unnecessary services is an important security concept, but this refers to *hardening* the system, and reducing the attack surface. Training staff on security policies is *educating the user* and is extremely important when attempting to reduce the consequences of successful social engineering attacks. Installing anti-malware applications also hardens the system, and secures it in general against viruses, worms, Trojans, and other forms of malware.

2. Answer: B. The AAA server and port 1812

   Explanation: AAA in computer security is an acronym that refers to authentication, authorization, and accounting. RADIUS (Remote Authentication Dial-In User Service) is an example of an AAA server, and would be the server that takes care of authentication for the wireless access point (WAP) in this scenario. By default, the RADIUS server uses port 1812 for authentication. Also by default, it does this over a UDP transport mechanism (though it can use TCP as well).

   See the section "Authentication Models and Components" in Chapter 10, "Physical Security and Authentication Models," for more information.

   Incorrect answers: The DHCP server (which uses ports 67 and 68) takes care of assigning IP addresses to computers on the network that require dynamic assignment. The Lightweight Directory Access Protocol (LDAP) server is used to maintain directory information, for example, in a Microsoft domain controller or an e-mail server. It uses port 389. It is based on the X.500 specification, and allows either unencrypted authentication or encrypted authentication via Transport Layer Security (TLS). An e-mail server that uses port 143 has the Internet Message Access Protocol (IMAP) e-mail protocol running. Though this server may be involved in the authentication of e-mail logins, it does not authenticate for connections made to a WAP.

3. Answer: C. Pharming

   Explanation: Pharming (a portmanteau of farming and phishing) is an attack that redirects traffic from a legitimate site to a different illegitimate and possibly malicious site. It can occur because of an exploited DNS server (which would affect many users), or can occur by modifying the hosts file of one or more computers (which would affect those computers only). If a hosts file is modified, it can be easily fixed by deleting the file, and either re-creating the file or letting the operating system re-create it. Individual computers can also be protected by configuring anti-phishing in the web browser or adding on third-party anti-phishing software, and using updated antivirus software. DNS servers can be protected through careful monitoring of DNS configurations and log files.

   See the section "Malicious Attacks" in Chapter 7, "Networking Protocols and Threats," for more information.

   Incorrect answers: Phishing is an attempt at obtaining private information from someone. It is usually done by e-mail. Whereas pharming attacks are often designed to "phish" for

information, phishing can be accomplished in a variety of ways in addition to pharming. Whaling is a subset of phishing and refers to when an attacker targets senior executives, which is an example of spear phishing. Spim is the abuse of messaging systems other than e-mail.

4. Answer: D. SCP

Explanation: SCP (Secure Copy) is a protocol/application used to transfer files securely between computers. It relies on Secure Shell (SSH) and uses port 22, and it is an application, and therefore resides on the application layer (layer 7), the highest layer of the OSI model, as does SSH. Because the OSI model is normally represented with a top-down approach, the application layer is at the top, and is considered "highest."

See the section "Ports and Protocols" in Chapter 7, "Networking Protocols and Threats," for more information.

Incorrect answers: IPsec is a protocol used to secure IP communications, for example, within Layer 2 Tunneling Protocol (L2TP) VPN connections. It is a network layer (layer 3) protocol. TCP resides on the transport layer (layer 4). ICMP (Internet Control Message Protocol) resides on the network layer (layer 3), and is instrumental in testing networking connections; for example, with the `ping` command.

5. Answer: C. The security controls on the USB drive can be bypassed.

Explanation: If access mechanisms such as permissions and policies are not implemented correctly on a USB hard drive (or any hard drive for that matter), then those security controls for that drive can be bypassed by an attacker.

See the section "Securing Computer Hardware and Peripherals" in Chapter 3, "Computer Systems Security Part II," for more information.

Incorrect answers: The possibility of data corruption usually happens because a hard drive physically fails or becomes too fragmented, not because of security controls being bypassed. Data on the USB drive should not be vulnerable to log analysis because the logs are normally stored in the system partition of the operating system. That drive is internal to the computer, whereas a USB hard drive will be external to the computer. The same holds true for user accounts. Those accounts are stored within the OS, and again on the main drive, not on a USB hard drive.

6. Answer: C. Identification

Explanation: The *first* response within the incident response that should be taken in this scenario is identification. The malware needs to be identified, the computers affected need to be identified, and so on. Identification is usually the first step of an organization's incident response process.

See the section "Incident Response Procedures" in Chapter 18, "Policies and Procedures," for more information.

Incorrect answers: An example of the main phases of incident response (as listed in CompTIA Security+ exam objective 5.4) is as follows: 1. Preparation; 2. Identification; 3. Containment; 4. Eradication; 5. Recovery, and finally; 6. Lessons learned. (This list can vary from one organization to the next and from one standardization body to the next.) A pre-step to this list is preparation—being ready with tools, knowledge, and training before an incident occurs. Validation can occur during steps 5 through 7, depending on the type of validation. Follow-up can be considered part of the documenting and monitoring step.

7. Answer: A. Transport encryption

Explanation: When securing data that passes between two points on an IP network, you need some kind of transport layer communications encryption protocol. Examples include Transport Layer Security (TLS) and Secure Sockets Layer (SSL). Protocols such as these operate on layer 4 of the OSI model; they encrypt the transmissions between IP-based

computers, protecting the session data from eavesdroppers, and are thus known as transport layer encryption protocols. They make use of X.509 certificates and a public key infrastructure (PKI). These protocols can utilize block ciphers (for instance, Advanced Encryption Standard [AES]) or stream ciphers (for example, RC4), but more commonly use the former. By the way, *APT* stands for advanced persistent threat, a group of continuous hacking processes often performed by multiple attackers. APTs are carried out by knowledgeable groups of people using very sophisticated attacks; often they reside in another country.

See the section "Security Protocols" in Chapter 15, "PKI and Encryption Protocols," for more information.

Incorrect answers: Key escrow is when decryption keys are held in escrow (placed in the custody of a third party), in the case that they are needed to gain access to data. They are common in PKI systems. This is a concept of where keys are stored, but not a method of encrypting data transmissions between two hosts. The answers "block ciphers" and "stream ciphers" are not specific enough. You can use either as part of an overall solution to secure data passing between two points on an IP network, but more often than not you will encounter SSL certificates that make use of RSA (for the key exchange) and AES (the actual cipher used for the transfer of session data).

8. Answer: C. Incident time offsets were not accounted for.

Explanation: In this scenario, the copyright infringement alert was triggered at 02: 30: 01 GMT. This means that it happened at 2:30 AM (during the first second) and that the incident, and the logs, are based on GMT (Greenwich Mean Time), the global time standard. Note the third log shows that a movie file was accessed at 03: 30: 01. There is exactly a one-hour difference between the copyright infringement alert and the log file that shows the file access that occurred (which is the infringement). This could be due to the fact that the server hosting the file has its time based on a different time zone. There are several other possibilities why the incident time offset occurred, but it did occur. When scanning for incident time offsets (because your log files will probably be large), look for incidents that happened during the same minute and second, but on a different hour. Ultimately, what you (and the incident response team) need to find out is who downloaded the movie and triggered the copyright infringement. It could be that Amy was the downloader, based on the time offset, but you would need to analyze the situation further to be sure.

See the section "Incident Response Procedures" in Chapter 18, "Policies and Procedures," for more information.

Incorrect answers: The logs are certainly not corrupt, and they are definitely available, because the incident response team was able to access them and send them (or a copy of them) to you to review. You don't know if the chain of custody was properly maintained. It is beyond your understanding because the incident response team has the log files. You only received a copy of some of the log file information.

9. Answer: C. Zero day

Explanation: A zero day attack (such as a zero day virus) is one that up until the point of time when the attack occurs was previously unknown to antivirus software companies and IDS companies. So, for the attack in question there was no AV or IDS signature available to detect it—it is an unknown and undocumented exploit. The admin found it by utilizing a heuristic system, which is a more advanced type of IDS. In a similar scenario, if a malicious exploit is found in an application and you inquire with the software vendor about remediation steps, and then find that no patches are available, you have most likely found a zero day attack. In these situations, you will have to *improvise*.

See the section "Secure Programming" in Chapter 5, "Application Security," for more information.

Incorrect answers: The rest of the answers are known attacks. Directory traversal is a method of accessing unauthorized parent directories on web servers. XML injection is a type of code injection used on website forms. Baiting is a type of social engineering attack where a USB flash drive or other type of removable media (often containing malware) is left out in the open for an unsuspecting person to pick up and (hopefully) insert into a computer.

10. Answer: C. Hardware address filtering has been implemented.

Explanation: The security administrator denied one MAC address at the SOHO router: 01:23:6D:A9:55:EC. This is most likely the MAC address of the mobile device that cannot connect to the network. Individual octets of a MAC address are often separated by colons when working in a router. However, in an operating system such as Windows they are often separated by hyphens. Be able to identify both. Note that the admin also permitted (or allowed) a particular MAC address to connect to the network. Access control lists (ACLs), or rules, such as these are created on the router to allow or disallow access.

See the section "Firewalls and Network Security" in Chapter 8, "Network Perimeter Security," for more information.

Incorrect answers: Port filtering could mean physical ports or logical TCP/IP ports such as port 80 HTTP. IP address filtering means that entire IP addresses (such as 10.254.254.101) have been filtered out. Both of these answers are incorrect because this scenario clearly deals with MAC addresses. WPA2-PSK is a method of connecting, but the "PSK" portion implies that it does not require a supplicant the way a technology such as 802.1X does. PSK means pre-shared key, a key that the admin selects and inputs into the router, which the user must know in order to connect to a wireless network.

11. Answer: D. WAF

Explanation: A WAF (web application firewall) can be implemented as hardware or software. Among other things it can protect from XSS (cross-site scripting) and SQL injection attacks. The WAF can be an appliance, server software, or plug-in, and applies a set of rules to HTTP sessions to protect from various attacks. WebKnight and ModSecurity are examples of open source WAFs. Unlike other devices such as network intrusion detection systems (NIDSs), routers, and some firewalls, the WAF operates at layer 7 of the OSI model (application layer).

See the section "Firewalls and Network Security" in Chapter 8, "Network Perimeter Security," for more information.

Incorrect answers: A flood guard is a separate feature of firewalls that can protect against SYN flood attacks. *IDS* stands for intrusion detection system—a device or software that monitors network activities and *alerts* an administrator to various types of malicious activities. A URL content filter is a software filter that monitors for specific URLs (domain names and website names) that are undesirable and disallows access to them.

12. Answer: C. Information security awareness

Explanation: Information security awareness means training users on how to screen calls and e-mails; not to give out personally identifiable information (PII); not to share confidential organizational data; and in general, to protect data and PII. This will be the best method for reducing the chances of another data leak due to social engineering attacks. By the way, if the social engineering attacks were conducted by phone, the attack type is known as *vishing*, a form of phishing.

See the section "User Education" in Chapter 17, "Social Engineering, User Education, and Facilities Security," for more information.

Incorrect answers: The use of social media and the option to bring your own device (BYOD) often lead to increased social engineering (in the form of spim, phishing, and possibly pharming), and additional security is required to meet that threat. When it comes to BYOD,

the main security concern is that there is a lack of controls in place to ensure that the devices have the latest system patches and signature files. Mobile device management (MDM) systems can alleviate that situation. Acceptable use is usually stated in policy form, and basically describes what people are allowed to do with company-owned computers and data. Though adherence to this policy can potentially help to reduce data leaks, it is not the best or most effective solution.

Note This is an example of a question for which two answers could arguably be correct. When taking the CompTIA Security+ exam, be sure to analyze the question carefully and select the best answer for most situations.

Data handling and disposal is also important, but training in them won't reduce the type of social engineering attack in the question that was perpetrated on the organization; that attack was vishing. However, data handling policies can help with shoulder surfing, dumpster diving, and a variety of other attacks.

13. Answer: D. Generate a new private key based on RSA

Explanation: When a person is required to submit a CSR (certificate signing request) to a CA (certificate authority), the first step—before generating the CSR—is to create a private key. This will be an asymmetric key such as RSA, commonly a 2048-bit key. (In fact, since the end of 2013 it is mandated that the key be 2048-bit or larger.) The next steps are to generate the CSR, submit the CSR for signing (the crucial part of the process), and finally install the signed certificate. It is important to keep the original RSA private key safe and secure. No one, including the CA, should know the RSA key. The CA should only know the CSR generated, which is based on the private RSA key.

See the section "Public Key Infrastructure" in Chapter 15, "PKI and Encryption Protocols," for more information.

Incorrect answers: Symmetric keys such as AES are not used for this process; asymmetric keys such as RSA are the standard. The security administrator must use and keep safe a private key that only he or she knows. Later, when people connect to the organization's website or network, they will make use of the public key portion.

14. Answers: D and F. Bob's public key or the CA's public key

Explanation: The key word here is *verify*. If Alice is to verify the validity of Bob's certificate, she will need either Bob's public key or the CA's public key. Table 1 sums up the keys required for encrypting/decrypting data, signatures, and certificates. This table is based on RSA, but usually these rules of thumb hold true for any scenario where a public/private key pair are used.

Table 1 Summary of RSA Public and Private Key Usage

Task	Which Person's Key to Use	Type of Key
Send an encrypted message	Receiver's	Public key
Decrypt an encrypted message	Receiver's	Private key
Send an encrypted signature	Sender's	Private key
Decrypt an encrypted signature *or verify a certificate*	Sender's	Public key

As you can see from the last row of the table, to decrypt an encrypted signature or verify a certificate, you would need the sender's public key; in this case, Bob's public key (or the CA's public key).

See the section "Cryptography Concepts" in Chapter 14, "Encryption and Hashing Concepts," for more information.

Incorrect answers: Alice cannot use her own key to verify the certificate, and cannot use anyone else's private keys. She would have to use the public key of the sender, be it Bob's or the CA's. Table 1 shows that there are a variety of possibilities depending on the scenario, and depending on who is sending what. For example, if Bob sent an encrypted *message* to Alice, he would need to use her public key to encrypt the message, and Alice would need to use her private key to decrypt the message.

15. Answer: B. To utilize single sign-on capabilities

Explanation: Both LDAP and Kerberos can be used for single sign-on (SSO). This eases the burden on users of having to remember different usernames and passwords and allows a single login to multiple systems.

See the section "Authentication Models and Components" in Chapter 10, "Physical Security and Authentication Models," for more information.

Incorrect answers: A CA is used to sign certificates, including wildcard certificates. Queries on a directory service can be made with LDAP, but not with Kerberos. SSO is a derivative of federated identity management (FIM), but FIM will be its own system altogether separate of LDAP and Kerberos.

16. Answer: B. RFID

Explanation: RFID (radio-frequency identification) tags could be attached to mobile items such as network testers, laptops, and so on. These tags can be extremely small and hard for an intruder to notice. Any proximity point that the item is not supposed to go past can be configured to automatically set off an alert or alarm when the RFID tag passes it.

See the section "Physical Security" in Chapter 10, "Physical Security and Authentication Models," for more information.

Incorrect answers: None of the other answers allow for automatic notification of item removal. Environmental monitoring is the real-time analysis of controls and programs that concern heating, ventilation, and air conditioning (HVAC) and supervisory control and data acquisition (SCADA). Electromagnetic interference (EMI) shielding is used to reduce or eliminate crosstalk and data emanation. CCTV (closed-circuit television) is used to monitor and record things that transpire within the work area, but again cannot (without the help of other software/technology) alert an administrator automatically.

17. Answers: C and F. Create a VLAN for the servers, and create an ACL to access the server.

Explanation: If the servers and the BYOD users are on the same network, then the BYOD users could easily access the servers, regardless of whether a computer is connected in a wired fashion or wireless fashion by default. So to protect the servers from the users' mobile devices, you could first create a virtual LAN (VLAN) for the servers. This VLAN would separate the servers and you could then control who is allowed access to the servers via access control lists (ACLs) within the firewall portion of the SOHO all-in-one wireless router. If the SOHO router supported it, you could also place the web servers in a DMZ.

See the section "Network Design" in Chapter 6, "Network Design Elements," and "Rights, Permissions, and Policies" in Chapter 11, "Access Control Methods and Models," for more information.

Incorrect answers: The EAP-TLS authentication scheme should not be necessary for this scenario; it is used, for example, to authenticate wireless clients to a wireless network, which was not specified in the question. Changing the default HTTP port (which is normally 80) would cause your Internet guests some difficulty in finding the web servers, and is not necessary in this scenario either. Denying incoming connections to the outside router interface would also make it difficult for Internet users to access the web servers, and is therefore not

recommended. If a physical port is disabled, anything connected to that port will be effectively offline. This also compounds the issue instead of solving it.

18. Answers: A and F. Change the implicit rule to an implicit deny and add the following ACL at the bottom of the current ACL: `deny IP any any 53`

Explanation: First of all, a firewall should not be set with an implicit allow by default. That would allow just about any kind of traffic through the firewall. Plus, it would make the already configured ACL unnecessary. So, the firewall should be changed to an implicit *deny* for all connections. That is the default settings for firewalls and it disallows all traffic coming from the Internet through the inbound interface (unless otherwise stated with an ACL). Second, you would add the ACL `deny IP any any 53` at the bottom of the current ACL. This will deny any DNS traffic (because DNS uses port 53) including DNS requests and zone transfers. It does this for any type of IP connection (including TCP and UDP) and for all IP addresses on the local and remote ends.

See the section "Firewalls and Network Security" in Chapter 8, "Network Perimeter Security," for more information.

Incorrect answers: Removing the current ACL would do nothing because the firewall is currently configured with an implicit allow. However, if you changed that default rule to an implicit deny and removed the ACL, Internet users would no longer be able to connect to the web server (which uses ports 80 and 443). That doesn't solve your problem; in fact, it creates another one. It doesn't really matter where you place the new ACL to block DNS requests—top, bottom, doesn't make a difference because when you are finished, the firewall will have an implicit deny, and then two separate ACLs that pretty much work independently of each other. However, you would normally place the ACLs in order, and this would mean placing the new ACL below the first. The key with the other two possible ACLs in the answers is that they are not blocking enough traffic. One shows TCP, which is not enough; you need to block TCP and UDP—this is done by simply stating `IP`. ICMP is not correct, because that deals with layer 3 testing, such as the ping utility.

19. Answers: A and E. MD5 and HMAC.

Explanation: The key word in this question is *integrity*. When we are dealing with the integrity of files, we often employ hashing. The only two hashing options in the supplied answers are MD5 and HMAC. Those cryptographic hash values could be compared to last night's integrity scan to find out which files have been changed in the two hours that the employee was working today.

See the section "Hashing Basics" in Chapter 14, "Encryption and Hashing Concepts," for more information.

Incorrect answers: Elliptic curve cryptography (ECC), Advanced Encryption Standard (AES), Pretty Good Privacy (PGP), and Blowfish are all encryption protocols used to encrypt files. None of them are cryptographic hashing functions.

20. Answer: C. Rule-based access control

Explanation: You would want to write a rule that automatically gives Bob write access to the database when Alice is gone. This is an example of rule-based access control. In this type of access control model, the security administrator writes the rule and allows the computer to automate the action of the rule when necessary.

See the section "Access Control Models Defined" in Chapter 11, "Access Control Methods and Models," for more information.

Incorrect answers: Discretionary access control (DAC) is when the user has ownership of the resource in question and can create permissions as necessary. Mandatory access control (MAC) is similar to rule-based access control; in fact, rule-based access control is a subset of

MAC. However, MAC is controlled by the system and does not work at this type of depth concerning rules. Role-based access control (RBAC) concerns users and their roles in the organization, including which groups they are members of, and applies rights and permissions accordingly. Attribute-based access control (ABAC) is a context-aware model that utilizes dynamic authentication and bases its decisions on the results of IF-THEN statements.

21. Answer: C. The system was designed to fail-open for life safety.

Explanation: In this scenario, the system did what it was supposed to do. In the case of a failure, the security administrator designed the system to *fail-open*, meaning that the door would unlock, allowing people to leave the server room in the event of an emergency (thus the meaning of life safety). The attacker probably had knowledge of this design, and so planned the attack accordingly. To protect against the attacker's gaining access in this scenario, multifactor authentication could be implemented: for example, adding biometrics, a passcode, or other form of authentication.

See the section "NIDS Versus NIPS" in Chapter 8, "Network Perimeter Security," for more information.

Incorrect answers: The proximity reader was definitely installed properly. It's just that the system has vulnerabilities, one of which the attacker has exploited. These vulnerabilities are built into the design of the system for safety. We don't know whether or not the system uses magnetic locks; there is not enough information in the question to make that assumption. The system was not designed in a fail-close configuration. If it were, the door would have remained locked when the proximity reader was broken.

22. Answers: C and E. Bcrypt and PBKDF2

Explanation: Bcrypt and PBKDF2 are examples of key stretching software. This software takes a weaker password key and *stretches* the key length, in the end outputting an enhanced and more powerful key, usually to 128 bits in length. This makes brute-force attacks difficult if not impossible. Bcrypt also adds salting (additional data added to the password hash), which helps protect against dictionary attacks and rainbow table attacks.

See the section "Hashing Basics" in Chapter 14, "Encryption and Hashing Concepts," for more information.

Incorrect answers: MD5 and SHA2 are cryptographic hashing protocols, used to verify the integrity of files. AES is a common symmetric encryption protocol used to encrypt files and session data. CHAP is an authentication scheme, one that could be used by a RADIUS server or other authentication system.

23. Answer: A. The Remote Authentication Dial-In User Service certificate has expired.

Explanation: 802.1X secure network access can be used to connect to wireless networks. It can use EAP, CHAP, or PEAP authentication. It can also utilize centralized authentication such as RADIUS. Though the scenario does not say so specifically, you can assume an 802.1X/PEAP/RADIUS configuration. If the RADIUS certificate expires, none of the wireless users would be able to connect.

See the section "Authentication Models and Components" in Chapter 10, "Physical Security and Authentication Models," for more information.

Incorrect answers: The DNS server is a separate service altogether. If it was overwhelmed (perhaps by a DDoS attack), then DNS queries would fail, but those queries would be to items on the domain, or websites, and so on. It should not affect the wireless network. Too many incorrect authentication attempts could cause some users to be disabled, but most likely this will be a temporary loss of service. In the scenario, *all* employees report no service to the wireless network. The scenario also states the technician verified that there were *no outages*, so the IDS should not have disabled the wireless network.

24. Answer: C. TCP Wrapper

Explanation: TCP Wrapper is a host-based ACL program that provides protection against host name and host address spoofing in Linux and Unix environments. Most gaming consoles are Linux-based, and the video streaming servers they connect to are most likely Linux- or Unix-based as well. By using this program, rules can be configured to restrict access to TCP services. For example, attackers can easily determine when an unprotected Linux-based system is idle, and then attempt to access that system when it is unattended. The TCP Wrapper program acts as a pseudo-firewall in that it monitors incoming packets for authorization, thereby blocking the potential attacker. Programs used for streaming can be compiled with TCP Wrapper, and these can also be encrypted to further foil the would-be attacker. (Often this program is also referred to as TCP Wrappers.) By the way, credit card numbers should usually be stored in a transactional database that encrypts down to the database field level, not only the file level.

See the section "Firewalls and Network Security" in Chapter 8, "Network Perimeter Security," for more information.

Incorrect answers: Firmware updates are important for any system, but will not stop the problem being described. Some kind of software such as TCP Wrapper (an application layer program) is needed. A web application firewall (WAF) isn't the correct type of firewalling required by video streaming servers and the gaming consoles that connect to them. Plus, WAF along with IDS are solutions that are installed at the server side. This scenario calls for secure coding of the program that transmits data between the gaming consoles and the video streaming servers.

25. Answer: B. It should be performed on the server side.

Explanation: The best answer is that it should be performed on the server side. Given the choice between server-side and client-side input validation, server-side wins out. However, both should be incorporated as secure coding methods.

See the section "Secure Programming" in Chapter 5, "Application Security," for more information.

Incorrect answers: Using the client side only can actually create additional vulnerabilities at the server. As a programmer, you don't really care about the user's knowledge level; you have to assume that smart users or attackers will come along at some point and try to hack your forms, web pages, or other applications, and design the client and server sides of the application appropriately. Even SSL-protected pages can be hacked into if they weren't properly validated. In fact, SSL doesn't really have too much effect on the matter, especially when it comes to web forms built in PHP or other similar web programming languages.

26. Answers: C and D. SSH and PGP

Explanation: SSH (Secure Shell) can secure connections to remote machines and is instrumental in encrypting data in motion over the network. PGP (Pretty Good Privacy) encrypts data that is meant for transit via e-mail or for data that is meant to be *at rest*, or simply stored somewhere for an indeterminate amount of time. These are the only answers listed that will encrypt data and/or data sessions (and are not outdated).

See the section "Ports and Protocols" in Chapter 7, "Networking Protocols and Threats," and "Encryption Algorithms" in Chapter 14, "Encryption and Hashing Concepts," for more information.

Incorrect answers: TFTP is used to send small and basic files in an unsecure manner between two hosts on a LAN. It does not encrypt data. The Temporal Key Integrity Protocol (TKIP) is used as a security protocol in wireless networks but is outdated and should be replaced by either Counter Mode CBC-MAC Protocol (CCMP) or Advanced Encryption Standard (AES). TKIP is insecure because it makes use of RC4, which is considered outdated. The Simple Network Management Protocol (SNMP) concerns the

monitoring of networks and network devices and hosts. NTLM (NT LAN Manager hash) is a cryptographic hashing protocol used with Windows passwords. This is also outdated and should be replaced with NTLMv2.

27. Answer: B. DLP

Explanation: DLP (data loss prevention) methods are often implemented in scenarios where USB mass storage devices are utilized (such as USB flash drives and external hard drives). A storage-based DLP system monitors data at rest, and performs content inspection in order to prevent unauthorized use of the data.

See the section "Implementing Security Applications" in Chapter 3, "Computer Systems Security Part II," for more information.

Incorrect answers: An IDS (intrusion detection system) is used to detect attacks and anomalies on the network. Content filtering is performed by proxy servers and Internet content filters—usually relating to Internet content. Auditing is when files and other resources are investigated in real time to see who accessed what and when.

28. Answer: A. Alice's private key

Explanation: Alice should use her own private key to sign the file. Refer to Table 14-4 in the book. It shows that to send an encrypted signature, Alice (the sender) would need her own private key. To decrypt the signature, Bob (the recipient) would need Alice's (the sender's) public key.

See the section "Cryptography Concepts" in Chapter 14, "Encryption and Hashing Concepts," for more information.

Incorrect answers: In this scenario, Bob's keys don't even come into play because he is the receiver. However, in a scenario where Alice had sent Bob an encrypted *message*, Bob's public and private keys would be utilized for the encrypting and decrypting of the message, respectively.

29. Answer: C. Incorporating diversity into redundant design

Explanation: The key word in the question is *availability*. One of the best ways to encourage availability is to have redundancy. The more diverse the redundancy, the more fault tolerant the system.

See the section "Redundancy Planning" in Chapter 16, "Redundancy and Disaster Recovery," and "Facilities Security" in Chapter 17, "Social Engineering, User Education, and Facilities Security," for more information.

Incorrect answers: Some industrial control systems do not have the option to run AV software, but even if they did, AV software does not promote availability directly. It helps to secure from viruses and other malware, but it is not a method of fault tolerance. Multiple firewalls, for example, a back-to-back perimeter configuration, will help to block network-based attacks, but also do not increase availability. Application whitelists, if not configured properly, could actually reduce availability. They are meant to restrict users to specific allowed applications.

30. Answer: D. Fingerprint readers

Explanation: The best answer is to use a biometric solution such as fingerprint readers. This is a different factor of authentication, and works well with smart cards and passwords. Biometric authentication falls into the factor category of something you *are*.

See the section "Physical Security" in Chapter 10, "Physical Security and Authentication Models," for more information.

Incorrect answers: The rest of the answers are within the categories of factors already mentioned in the question. Badge readers would be used with smart cards (or proximity cards) as would hard tokens; they are within the category of something you *have*. Passphrases are essentially the same as passwords; they are within the category of something you *know*.

31. Answer: D. 22 and TCP

Explanation: SFTP (Secure FTP) uses port 22 and rides on SSH to make connections. It uses TCP as the transport mechanism. Most secure connections of this sort require guaranteed, connection-oriented transmission of data—thus TCP.

See the section "Ports and Protocols" in Chapter 7, "Networking Protocols and Threats," for more information.

Incorrect answers: Port 21 is used by plain FTP, with no security. FTP also uses TCP as the transport mechanism. The answers listed might have appeared tricky at first, but if you know your protocols and associated port numbers and transport mechanisms used, you will prevail. Be sure to memorize Table 7-2 in the book!

32. Answer: C. Scarcity

Explanation: Scarcity refers to a limited supply, something in short supply, thus "exclusive access" in the question. Some users, especially the ones at the top of the marketing pyramid—the innovators—don't want to be left out of the latest, newest, exclusive smartphone offers. It is these people who are targeted by social engineers with the method of scarcity. Most likely, the link is bogus, and leads to another website altogether unexpected by the user.

See the section "Social Engineering" in Chapter 17, "Social Engineering, User Education, and Facilities Security," for more information.

Incorrect answers: It is possible that the e-mail could use the other methods mentioned in the incorrect answers, but they are not described in the scenario. An example of trust would be a money-back guarantee, or using some kind of knowledge of the user. An example of intimidation could be the use of hoax ransomware, or perhaps the e-mail says you are required to appear in court, and so on. An example of familiarity would be if a social engineer shows sympathy or empathy for a user, usually with previously learned information about the user.

33. Answer: B. $5000

Explanation: If the server had a 10% loss of functionality, then that would be $500, or 1/10 of the server value. If this happened 10 times per year, then you would multiply that individual loss of $500 × 10, resulting in a $5000 loss for the year. Remember that the ALE is the total loss in dollars per year for a specific incident. The entire quantitative risk assessment equation is

SLE × ARO = ALE

In this case, the single loss expectancy (SLE) is 10%, which equals $500. The annualized rate of occurrence (ARO) is the number of times per year that the incident occurred—in this case, 10. So:

$500 × 10 = $5000. The ALE = $5000, which just happens to be the value of the server. Hmmm, time for a replacement? At the very least, some investigative work needs to be done to find out why the server is going down so often.

See the section "Conducting Risk Assessments" in Chapter 12, "Vulnerability and Risk Assessment," for more information.

Incorrect answers: The other answers of $500, $10,000, and $50,000 are not correct because they do not fit the equation of SLE × ARO = ALE. Math doesn't lie.

34. Answer: C. Hardening

Explanation: It appears that an external IP address (208.159.67.23) is attempting to connect remotely to the local computer (10.248.248.67), possibly using the Remote Desktop Connection program. The connections were unsuccessful, but hardening is required at the local system and at the firewall to ensure that this IP address cannot connect through to the

local computer. Services should be analyzed and, if necessary, shut down at the local computer. Ports should be scanned and, if necessary, closed at the firewall.

See the section "Hardening Operating Systems" in Chapter 4, "OS Hardening and Virtualization," for more information.

Incorrect answers: System log monitoring is incorrect because the logs are present, and they have been monitored and analyzed, resulting in the answer that additional hardening is necessary. An IDS (intrusion detection system) looks for attacks and will notify an administrator (and possibly shut down a firewall if necessary), but it is not working correctly at this point. To truly mitigate the problem, the IDS should be reconfigured and hardened, or an IPS (intrusion prevention system) should be implemented. Reporting, along with the logs, seems to be working properly.

35. Answers: A and D. Validate input on the client and the server side, and restrict the use of special characters in form fields

Explanation: Input validation is extremely important when it comes to website attacks such as XSRF (cross-site request forgery) and cross-site scripting (XSS) attacks. Forms and other documents should be validated on the client side and the server side (if at all possible). Special characters should be restricted and sanitized within form fields and URLs. This is all part of secure coding.

See the section "Secure Programming" in Chapter 5, "Application Security," for more information.

Incorrect answers: Using angle brackets for HTML code (for example < and >) is just good programming. Without angle brackets, the HTML statement won't work, but it has nothing to do with *input* validation. The more redirection that occurs, the more the chance of vulnerabilities being exploited. URL redirection should be limited if not eliminated. Web proxies make for more efficient web connections in a variety of ways but do nothing for input validation.

36. Answer: B. Install a digital certificate on the authentication server

Explanation: If you are running a WPA2-Enterprise wireless network, then the wireless access point (WAP) will need to access a RADIUS server for the authentication portion of the wireless connection. This scenario calls for a digital certificate to be loaded on the RADIUS server.

See the section "Authentication Models and Components" in Chapter 10, "Physical Security and Authentication Models," for more information.

Incorrect answers: A DHCP server might be utilized at the WAP (or other all-in-one network device), or there could be a separate DHCP server, but this is a different task altogether that the RADIUS server is not normally responsible for. The RADIUS server needs a digital certificate; the encryption key for WPA2 would be stored on the WAP. A token is not necessary, but is often used with swipeable smart cards for physical authentication.

37. Answer: A. OCSP

Explanation: OCSP (Online Certificate Status Protocol) is used as a lightweight (albeit less secure) alternative to the CRL. It validates certificates by returning responses such as "good," "unknown," and "revoked."

See the section "Public Key Infrastructure" in Chapter 15, "PKI and Encryption Protocols," for more information.

Incorrect answers: *PKI* stands for public key infrastructure, which OCSP is a part of. The PKI is the entire set of software, hardware, users, computers, certificates, and so on—it is an entire infrastructure. CRL stands for certificate revocation list, which is a list of certificates that are no longer valid. The RA is the registration authority, which is used to verify requests for certificates; it forwards the response to the CA.

38. Answer: C. Deploy a NIPS at the edge of the SCADA network

Explanation: The only answer that does not require modifications to the actual SCADA (supervisory control and data acquisition) system and network is to deploy a NIPS (network intrusion prevention system) at the *edge* of the SCADA network. This will monitor for (and protect against) attacks on the SCADA system, but does not require that the SCADA system be modified.

See the section "Facilities Security" in Chapter 17, "Social Engineering, User Education, and Facilities Security," for more information.

Incorrect answers: Installing a firewall, updating AV definitions, and enabling auditing all require modifications to the SCADA system and network. While you wait for testing to be completed and obtain vendor approval, these avenues should be explored, but not implemented.

39. Answers: A and D. ECDHE and Diffie-Hellman

Explanation: Standard Diffie-Hellman and ECDHE (Elliptic Curve Diffie-Hellman in ephemeral mode) were designed to securely negotiate encryption keys over an unencrypted channel.

See the section "Encryption Algorithms" in Chapter 14, "Encryption and Hashing Concepts," for more information.

Incorrect answers: PBKDF2 is a program used for key lengthening; it is often used to make weak keys stronger. Steganography is the art of hiding messages, for example, within pictures or photographs. Symmetric encryption is not used in this scenario. Both answers (and other solutions) will be asymmetric methods.

40. Answer: B. Open system authentication

Explanation: The best answer listed is to use open system authentication. In a public hotspot wireless network, this means that anyone can connect as long as she knows the password or passphrase. You could also utilize a captive portal, which forces the wireless client to authenticate via a special web page and possibly supply an e-mail address as part of the authentication process.

See the section "Securing Wireless Networks" in Chapter 9, "Securing Network Media and Devices," for more information.

Incorrect answers: Disabling the SSID would make it difficult for a computer to find the wireless network, and therefore difficult (if not impossible) for patrons to use the Internet. A MAC filter would be very inefficient as the proprietor of the establishment would need to find out the MAC address of each person coming through the door. Reducing the WAP power level is a good way to reduce the chances of war-driving, but isn't necessary in this scenario, though it is a good practice.

41. Answer: A. Create a virtualized sandbox and utilize snapshots

Explanation: You should create a virtualized sandbox—a place where you can work with many virtualized images and test them frequently. By utilizing snapshots, you are taking limited images of the systems at a specific point, most likely before and after the patch installation. The snapshot is a set of information at a particular point in time, and not necessarily an entire image.

See the section "Secure Programming" in Chapter 5, "Application Security," for more information.

Incorrect answers: Creating a single image of a patched PC is not enough. Good patch management requires that the security administrator do thorough testing; in the scenario you are

required to test the patch a dozen times. Incremental backups are used as a part of an efficient backup plan that usually includes incremental and full backups. But this—and the fact that the PC is unpatched—does not help a security administrator to test the patching process quickly and often. A full disk image after each patch installation could be very time consuming. Instead, snapshots are the better option.

42. Answer: B. MoUs are generally loose agreements that do not have strict guidelines governing the transmission of sensitive data.

Explanation: An MoU is generally a loose agreement. It differs from a service level agreement (SLA) and an interconnection security agreement (ISA) in that those are very specific regarding legal issues and security concerns.

See the section "Legislative and Organizational Policies" in Chapter 18, "Policies and Procedures," for more information.

Incorrect answers: It could be said that an MoU between two parties cannot be held to the same legal standards as an SLA. However, that is a legal risk and not a security risk. Because the MoU may not have budgetary considerations written carefully, an entity may be left to absorb unexpected cost, but this is a financial risk, not a security risk. MoUs do not generally have strict policies concerning services performed between entities. The name implies a lot: memorandum of understanding. It is an understanding that has been met, not an *agreement*.

43. Answer: C. LDAP

Explanation: DC=ServerName and DC=COM imply the use of a Microsoft Windows domain controller (thus the DC parameter). Lightweight Directory Access Protocol (LDAP) is a directory access and authentication service used by Windows domain controllers, among other technologies.

See the section "Authentication Models and Components" in Chapter 10, "Physical Security and Authentication Models," for more information.

Incorrect answers: SAML (Security Assertion Markup Language) is used to address single sign-on (SSO) solutions between two providers; it is based on XML. RADIUS and TACACS+ are other types of authentication servers and are not necessarily Microsoft domain–based. (In fact, TACACS+ is Cisco-based.) Also, they are more often used for remote authentication, whereas the scenario implies a local authentication technology.

44. Answer: D. Rogue access point

Explanation: It appears from the information given that there is a rogue access point (ABC-WAP4). This could be a WAP that was forgotten about, or one that was purposely and maliciously placed inside the network. Note that the question stated there are *three* wireless networks, and that the first three WAPs utilize nonoverlapping channels (1, 6, and 11). However, the fourth WAP uses channel 4 (which would overlap with the ABC-WAP1), and has a lower power level reading, meaning that it is probably somewhere near the physical perimeter of your building. To mitigate the issue, this WAP should be physically located and taken offline.

See the section "Securing Wireless Networks" in Chapter 9, "Securing Network Media and Devices," for more information.

Incorrect answers: Wireless jamming would cause one or more of the WAPs to fail, and would ultimately cause connectivity issues for wireless users; this is not mentioned in the scenario. Packet sniffing is the capturing of data that crosses the network. This could possibly be happening if an attacker is monitoring the fourth WAP, but you do not know this. Near field communication (NFC) is a standard used by smartphones to establish radio communications easily over short distances (often by touching the two devices together or bringing them very close to each other).

45. Answer: D. MAC filtering

Explanation: When MAC filtering is enabled on a WAP, it actually broadcasts information wirelessly. This makes it vulnerable to spoofing. Because MAC filtering and a disabled SSID can be easily circumvented using a network sniffer, it is very important to also use strong encryption, and possibly consider other types of network access control (such as 802.1X) and external authentication methods (such as RADIUS).

See the section "Malicious Attacks" in Chapter 7, "Networking Protocols and Threats," for more information.

Incorrect answers: WPA-LEAP and WPA-PEAP are authentication protocols designed specifically to counter spoofing and other attacks. If the SSID is enabled, there is no need to do any spoofing because the SSID can be easily scanned for by war-drivers and other attackers.

46. Answer: B. ISA

Explanation: An ISA is an interconnection security agreement. It is an agreement that is established between two (or more) organizations that own and operate connected IT systems and data sets. Its purpose is to specifically document the technical and security requirements of the interconnection between the organizations. This is the type of agreement you need in this scenario because the data is sensitive and the CIO requires that there is a clear understanding of security controls to be implemented and agreed upon.

See the section "Legislative and Organizational Policies" in Chapter 18, "Policies and Procedures," for more information.

Incorrect answers: An SLA (service level agreement) is a contract between a service provider and a customer that specifies the nature of the service to be provided and the level of service that the provider will offer to the customer. It can be a very basic agreement, or it could also state the technical and performance parameters, but it will probably not include any specific security controls. An MoU is not an agreement at all, but a memorandum of understanding between two organizations or government agencies. It does not specify any security controls either. A BPA (business partners agreement) is a type of contract that can establish the profits each partner will get, what responsibilities each partner will have, and exit strategies for partners. Note that you might see the acronym *BPA* used for other things as well in the business and IT worlds.

47. Answer: D. Armored virus

Explanation: The armored virus protects itself from AV programs by tricking the program into thinking that it is located in a different place than where it actually resides. It thwarts attempts at analysis of its code. This makes it difficult to reverse engineer, and therefore makes building a defense against it difficult.

See the section "Malicious Software Types" in Chapter 2, "Computer Systems Security Part I," for more information.

Incorrect answers: A logic bomb is code that is inserted into software that "detonates" one of many types of malware when specific criteria are met. So, the logic bomb is more of a method of delivery for malware than the malware itself. The same holds true for backdoors; they are coded entrances to a system that either were designed for testing and forgotten about or are openings that were never found during a secure code review. A worm is similar to a virus except that it self-replicates. However, worms are fairly easy to detect and locate, making reverse engineering at least feasible.

48. Answer: B. To reduce the burden of certificate management

Explanation: A wildcard certificate (usually associated with SSL certificates) secures a website URL and an unlimited number of its subdomains. For example, it could secure www.davidlprowse.com, as well as the fictitious subdomains sy0-501.davidlprowse.com, blog.davidlprowse.com, and so on. Instead of having multiple SSL certificates, you could

use a single wildcard SSL certificate. This can make the management of certificates easier, and can possibly save time and money.

See the section "Public Key Infrastructure" in Chapter 15, "PKI and Encryption Protocols," for more information.

Incorrect answers: Extending the renewal date of a certificate is incorrect because, generally, a renewal of a certificate simply means that a new certificate is purchased; a CSR is generated (with a new RSA private key) and submitted for approval. The same goes for increasing a certificate's encryption key length. Normally, this is not done, and a new certificate is purchased. Due to a mandate with a deadline of December 31, 2013, companies began renewing any certificates that were based on RSA encryption lower than 2048-bit. So, any older 1024-bit certificates were also added to the organization's certificate revocation list (CRL). Securing the certificate's private key is incorrect because the wildcard functionality has nothing to do with this. The certificate is based on the RSA private key, but this key should not be known by anyone accept the person who generated it. Again, this key should be 2048-bit.

49. Answer: D. BIND server

Explanation: *BIND* stands for Berkeley Internet Name Domain. It is the most widely used DNS server on the Internet and was originally designed at the University of California at Berkeley. It normally runs on Unix systems. This would have to be booted first in order to establish DNS services; in fact, it is the only server listed that will establish DNS services in this scenario.

See the section "Cloud Security and Server Defense" in Chapter 6, "Network Design Elements," for more information.

Incorrect answers: Apache is a type of web server. Exchange is a type of e-mail server. RADIUS is an authentication server. None of these establish DNS services, unless DNS has also been loaded on those computers separately.

50. Answer: C and E. Password complexity and password length

Explanation: The two best ways to increase security of passwords are to have longer passwords (for example, 10 to 15 characters in length) and to make the passwords more complex (for example, adding uppercase letters, numerals, and special characters). It is these two methods that will make a password difficult to crack. Finally, the best way to enforce the creation of complex passwords is to configure a policy within the computer system.

See the section "Rights, Permissions, and Policies" in Chapter 11, "Access Control Methods and Models," for more information.

Incorrect answers: It is also important to have a maximum password age before expiration, and disallow the use of passwords that were previously used in history. However, these are minor methods compared to password complexity and password length.

51. Answer: D. Matrix of job titles with required privileges

Explanation: The information gathering stage of a task such as this requires a matrix of job titles and required privileges, preferably something in spreadsheet format that can easily be entered into the system quickly. Each employee in the matrix would fall into a specific role in the RBAC model.

See the section "Access Control Models Defined" in Chapter 11, "Access Control Methods and Models," for more information.

Incorrect answers: The important information here for the RBAC model is the names of employees, job titles, and their required privileges. The clearance levels are also important, but they should be translated into required privileges before they are sent to the security administrator planning the RBAC model. Rules under which certain systems can be accessed aren't required here; besides, that would be an example of *rule*-based access control, not

role-based access control. Any group-based privileges already in place will most likely be wiped clean once the new RBAC system is up and running, so they probably aren't necessary either.

52. Answer: B. 802.1X and VLANs

Explanation: In this question the RJ45 wired jacks are the key. You don't want just anyone connecting to the wired jacks and having access to internal resources. So, implementing 802.1X and VLANs is an excellent solution. This will authenticate computers; only systems with the proper 802.1X adapter will be authenticated to internal resources. Other computers that connect will only be able to connect to the Internet. The virtual LAN can be port-based, with a VLAN per conference room, or perhaps protocol-based, defining which computers are allowed to internal resources and which are allowed to the Internet only.

See the section "Authentication Models and Components" in Chapter 10, "Physical Security and Authentication Models," for more information.

Incorrect answers: A virtual private network (VPN) is used so that remote users can gain access to the network. The scenario speaks only to localized conference rooms and resources, so a VPN (and the supporting IPsec used in L2TP connections) is not necessary. The organization will most likely have at least one switch and firewall already. However, the switch can be used as the *authenticator* of the 802.1X system. NAT (network address translation) is used in IPv4 networks to mask internal IP addresses when they access the Internet. This will most likely already be implemented by default, so any guests accessing the Internet will enjoy the security benefits of NAT. However, a demilitarized zone (DMZ) has little to do with the scenario; this is when servers (such as WWW and FTP) are placed in an area outside the LAN but still within the organization's network, making it easier for people on the Internet to access them.

53. Answer: C. LEAP

Explanation: LEAP (Lightweight Extensible Authentication Protocol) is Cisco's version of EAP. It allows for dynamic Wired Equivalent Privacy (WEP) keys and mutual authentication with a RADIUS server.

See the section "Authentication Models and Components" in Chapter 10, "Physical Security and Authentication Models," for more information.

Incorrect answers: The other answers do not use a RADIUS server; they all rely on the pre-shared key (PSK). Counter Mode CBC-MAC Protocol (CCMP) is a secure alternative to Temporal Key Integrity Protocol (TKIP), both of which are used with a protocol such as WPA or WPA2. Both WEP-PSK and WPA2-PSK use pre-shared keys (PSK) that the administrator enters locally at the WAP. However, WEP should not be used in this manner, as it is deprecated. It can, however, be used in conjunction with a RADIUS server. In that scenario, it is possible to use WEP in a secure fashion.

54. Answer: C. Packet sniffing

Explanation: The network switch is probably intercepting cables to and from the CEO's office, and is probably replaying information to an attacker somewhere (perhaps a malicious insider), where packets are being analyzed by a packet sniffer such as Wireshark.

See the section "Assessing Vulnerability with Security Tools" in Chapter 12, "Vulnerability and Risk Assessment," for more information.

Incorrect answers: Impersonation is when a person attempts to gain access to a building by posing as someone else; it is a form of social engineering. Spear phishing, another type of social engineering, is when one or more individuals are targeted specifically. It is a derivative of phishing. The highly specific version of that—whaling—could possibly be happening here; you don't know without further analysis. MAC flooding is when a switch's content addressable memory (CAM) table is flooded with numerous packets, causing the switch to switch to fail-open mode and broadcast information instead of functioning as a proper switch.

55. Answers: D and F. Safety and integrity

Explanation: The fencing and additional lighting are for employee safety, especially at night. Digitally signing software, or anything else, speaks to keeping the integrity of the software intact. Hashing is another concept that could be implemented.

See the section "Conducting Audits" in Chapter 13, "Monitoring and Auditing," and "Physical Security" in Chapter 10, "Physical Security and Authentication Models," for more information.

Incorrect answers: Encryption would infer confidentiality. If the security consultant were to say that data is not secure in transit or at rest, then encryption would be a viable option. Fault tolerance infers availability. If the security consultant were to say that there are too many single points of failure, then fault-tolerant methods such as a redundant array of inexpensive [or independent] disks (RAID) array would be worth considering.

56. Answers: C and E. Screen locks and full device encryption

Explanation: Screen locks (especially the password and passcode variety) can make it difficult for an attacker to get to the data stored on the device. Better yet, full device encryption will make it virtually impossible to read the data. These are the best options, but not the only options. For example, a security administrator might opt to install a remote wipe program. Once it is known the mobile device has been stolen, the admin can trigger the wipe from a central location. However, there is a time delay concerning this method, so it should be used with the previous techniques.

See the section "Securing Mobile Devices" in Chapter 3, "Computer Systems Security Part II," for more information.

Incorrect answers: From a security standpoint, a global positioning system (GPS) is usually more of a hindrance than a security control. It might help in recovering the device, but by that point the damage has probably already been done. Inventory control and the tracking of assets are important (and are sometimes done with the aid of GPS), but remember that an unprotected mobile device can have its data downloaded by an attacker in a matter of minutes. So these things are great from a management standpoint, but not from a security standpoint.

57. Answer: D. Salting

Explanation: Salting is additional random data that is added to a one-way cryptographic hash. It can be used by itself or with key stretching if the hash has a weak key.

See the section "Hashing Basics" in Chapter 14, "Encryption and Hashing Concepts," for more information.

Incorrect answers: Rainbow tables are used to reverse cryptographic password hashes. Salting can help to deter this attack. Symmetric cryptography deals with the encryption of data using symmetric protocols such as the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES). NTLMv2 is a newer Microsoft password hash used by Windows.

58. Answer: D. 69 and UDP

Explanation: TFTP, the Trivial File Transfer Protocol, uses port 69 by default, and utilizes the UDP (User Datagram Protocol) connectionless transport mechanism. This makes for a simple, lightweight protocol used to automate the transfer of basic files such as boot files in a localized environment. For example, if a PXE-compliant client computer boots off of the network, it might make use of an embedded TFTP program within the network card to transfer the appropriate boot files from a server located somewhere on the local area network. TFTP is inherently insecure, so it is not recommended for use on the Internet.

See the section "Ports and Protocols" in Chapter 7, "Network Perimeter Security," for more information.

Incorrect answers: Port 68 is used by the Dynamic Host Configuration Protocol (DHCP) (client side) and the client side of the Bootstrap Protocol (BOOTP). TCP is the Transmission Control Protocol, which offers a guaranteed, connection-oriented transport mechanism, in contrast to UDP. TCP is not used by TFTP via port 69 or DHCP via port 68 (or port 67 for that matter).

59. Answer: C. Cluster tip wiping

Explanation: A cluster tip is the last portion of a hard drive's cluster that is not used by a file. Often, files take up more than a single cluster. The cluster remainders don't get erased by default, but could possibly contain data remanence. So, some disk cleanup programs contain an option to wipe the cluster tips, thus better sanitizing the drive. This can even be performed while the computer is in use.

See the section "Legislative and Organizational Policies" in Chapter 18, "Policies and Procedures," for more information.

Incorrect answers: Encryption of any type does not sanitize the drive. Storage retention and data retention usually manifest themselves as policies. For example, an organization might have a storage retention policy that states a hard drive must be kept in storage for a minimum of three years before being fully sanitized and/or destroyed. This is common in high-security environments where data is extremely confidential, or where auditing and other logging information must be kept for a specific amount of time.

60. Answer: D. Verify that virtual machines have the updates and patches installed

Explanation: One of the most important security precautions you can take is to install the updates and patches. This concept applies to regular operating systems, applications, and virtual machines.

See the section "Virtualization Technology" in Chapter 4, "OS Hardening and Virtualization," for more information.

Incorrect answers: It is unnecessary for virtual machines to be multihomed because this will not increase their security. In fact, the more network connections a VM has, the less security it has. Penetration testing should be completed before the virtual machines have been implemented. Subnetting is not necessary for virtual machines, although it can increase security. Subnetting should be taken into account during the planning and implementation stage.

61. Answer: A. Role-based access control

Explanation: Role-based access control (RBAC) works with sets of permissions; each set of permissions constitutes a role. Users are assigned to roles to gain access to resources. Examples of user groups that are assigned to roles include remote users, extranet users, guests, and so on. In this question, the remote users are the group that has been assigned a role that enables them to access the network only during normal business hours.

See the section "Access Control Models Defined" in Chapter 11, "Access Control Methods and Models," for more information.

Role-based access control should not be confused with rule-based access control, which is a type of mandatory access control (MAC). MAC is an access control policy determined by a computer system and not by a user or owner. Discretionary access control (DAC) is generally determined by the owner of a resource.

62. Answer: C. Items not specifically given access are denied by default.

Explanation: If a user or group of users does not have permissions to gain access to a resource, many systems will deny access by default; this is known as implicit deny and is common in firewalls and Windows operating systems. Default access control lists, or ACLs, will be set up for implicit deny and remain that way unless they are changed.

See the section "Access Control Models Defined" in Chapter 11, "Access Control Methods and Models," for more information.

Incorrect answers: ACLs are not a secure way of moving traffic, but rather they are a secure way of permitting or denying traffic to pass through a firewall or permitting or denying a user or group of users access to resources. Implicit deny does not deny all traffic, only traffic that has not been previously allowed.

63. Answer: B. Firewall log

Explanation: The firewall log can help you find out whether files are being illegitimately copied to an external location. This is the only log listed that can give you any information about files being copied to an external or remote location.

See the section "Conducting Audits" in Chapter 13, "Monitoring and Auditing," for more information.

Incorrect answers: The DNS log can help you find out whether unauthorized zone transfers or DNS poisoning has occurred. The antivirus log shows what viruses have been detected and quarantined on a system. The System log is a log file within the Event Viewer that provides information about the operating system and device drivers.

64. Answer: D. Steganography

Explanation: Steganography is the science and art of writing hidden messages. It is a form of security through obscurity. The goal is that no one aside from the sender and receiver should even suspect that a hidden message exists. Although steganography can come in different forms, it is most commonly found in image files.

See the section "Cryptography Concepts" in Chapter 14, "Encryption and Hashing Concepts," for more information.

Confidentiality means preventing the disclosure of information to unauthorized persons. By definition, cryptography is the practice and study of hiding information. In computer science, cryptography uses encryption to hide information and make it secret, whereas steganography, if accomplished correctly, does not imply that a hidden message even exists. If a person were to see an encrypted cryptographic message, they would know it for what it is and may try to crack it. A digital signature authenticates a document or e-mail, letting the recipient know that the document was created and sent by the actual sender and not someone else.

65. Answers: C and D. Provide an appropriate ambient temperature, and maintain appropriate humidity levels

Explanation: The HVAC system's primary responsibilities are to provide an appropriate ambient temperature for the equipment and to maintain appropriate humidity levels. This keeps the equipment from overheating and prevents electrostatic discharge (ESD).

See the section "Facilities Security" in Chapter 17, "Social Engineering, User Education, and Facilities Security," for more information.

Incorrect answers: HVAC equipment cannot shield other equipment from EMI. However, some HVAC equipment needs to be shielded to reduce EMI after it is installed. Isolation can be provided by other methods such as the material used in the perimeter of the room (for example, physical firewalls). A separate ventilation system can be installed to vent fumes away from the server room; however, there shouldn't be any fumes. Products that contain fumes should be stored in a separate and specially secured area. And if a fire were to occur, the sprinkler system or special hazards system should end that threat, eliminating any fumes that were a result of the fire.

66. Answer: B. SLA.

Explanation: An SLA, service-level agreement, is the part of a service contract in which the level of service is formally defined. This might include traffic performance guarantees, restoration guarantees, and minimum downtime guarantees.

See the section "Legislative and Organizational Policies" in Chapter 18, "Policies and Procedures," for more information.

Incorrect answers: A chain of custody is the chronological documentation of evidence. *DRP* stands for disaster recovery plan, which includes contact information, determination of impact, a recovery plan, and so on. Incident response procedures are sets of procedures that an investigator will use when examining a computer security incident. They might include preparation, identification, containment, eradication, recovery, and lessons learned.

67. Answer: A. NAC

Explanation: NAC, or network access control, makes security checks of the users or the actual connections that are made before sessions are initiated. It can also remediate issues automatically if configured properly. 802.1X is an example of network access control.

See the section "Network Design" in Chapter 6, "Network Design Elements," for more information.

Incorrect answers: NAT (network address translation) converts one set of IP addresses to another. VLAN is a virtual local area network. Subnetting compartmentalizes IP networks by way of IP addresses and mathematics.

68. Answer: C. Remove the read permission from the Finance group for the Reports folder

Explanation: Removing the read permission from the Finance group for the Reports folder will ensure that members of the Finance group solely cannot access the folder. However, members with dual membership, such as users who are part of the Accounting group and the Finance group, will still be able to access the folder.

See the section "Rights, Permissions, and Policies" in Chapter 11, "Access Control Methods and Models," for more information.

Incorrect answers: Denying the read permission to the Finance group for the Reports folder is incorrect because if the Finance group is denied access, that will override any other permissions, including anyone who is a member of the Finance department and a member of another department (such as Accounting) that is normally allowed access. Bottom line: deny access overrides any other permissions. Denying the read permission individually for each member of the Finance group for the Reports folder is incorrect for the same reason, but this time each individual user of the Finance group is being denied, which again would include users with dual membership. It is never wise to delete a group because that would have serious implications for all the users involved.

69. Answers: A and C. Create security groups and assign access permissions based on organizational roles, and create an OU for each organizational role and link GPOs to each OU

Explanation: The first thing you should do as a network administrator is create organizational units (OUs) for each of the departments in your organization; this helps to categorize and classify where users will ultimately end up. Each OU will be considered a different role. Next on the list is creating Group Policy objects (GPOs), modifying the security policies, and applying those to each individual OU. Then, you should create the users and place them in their correct OUs according to the department that they will be working in and the role that they will play. Finally, you should create security groups, add users to the appropriate security group or groups, and apply access permissions to the groups, instead of the users, to save time and keep administrative overhead to a minimum.

See the section "Rights, Permissions, and Policies" in Chapter 11, "Access Control Methods and Models," for more information.

Incorrect answers: Placing the user's computer in an OU could cause issues when it comes time to move a user account to another OU; the computer account would need to be moved with it. Access permissions should not be assigned solely by the individual user account; this would increase administrative overhead by a great deal.

70. Answer: C. Back up data to removable media and store a copy offsite

Explanation: Backing up data to removable media and storing it offsite is the least expensive solution.

See the section "Disaster Recovery Planning and Procedures" in Chapter 16, "Redundancy and Disaster Recovery," for more information.

Incorrect answers: Hot sites and cold sites can cost the organization a lot of money, especially hot sites. Implementing a remote backup solution usually requires some sort of service with a monthly fee. You, as the network administrator, can back up data to removable media and store it offsite without incurring any other fees except for the cost of the removable media.

71. Answer: A. The hard drive should be sanitized.

Explanation: Before a hard drive is recycled, it should be sanitized. Also known as purging, sanitizing is the removal of data in such a way that it cannot be reconstructed by any known technique. At this point the drive can be recycled within the organization or recycled with the rest of the computer.

See the section "Legislative and Organizational Policies" in Chapter 18, "Policies and Procedures," for more information.

Incorrect answers: Reformatting the drive is not enough because reformatting leaves data remanence, or data residue. Destroying the drive can render it useless and therefore cannot be recycled. Storing the drive in a safe area is not recycling the drive.

72. Answer: D. Deploy a honeypot in the perimeter network

Explanation: A honeypot can be used to lure attackers in and trap them while you analyze their methods. The honeypot is usually placed within the perimeter network, which is the DMZ.

See the section "Firewalls and Network Security" in Chapter 8, "Network Perimeter Security," for more information.

Incorrect answers: Proxy servers are usually not placed in the perimeter network; they act as go-betweens, or mediators, for users on the LAN and servers on the Internet. A NIPS (network intrusion prevention system) can be placed in or out of a perimeter network, but it does not lure in attackers; instead, a NIPS attempts to prevent attacks from happening.

73. Answer: C. Systems should be restored within six hours with a minimum of two days' worth of data.

Explanation: *RTO* stands for recovery time objective, the acceptable amount of time to restore a function, service, or entire system. In the question the RTO is six hours, and so systems should be restored within six hours. *RPO* stands for recovery point objective, the acceptable latency of data, or the maximum tolerable time that data can remain inaccessible after a disaster. In the question the RPO is two days, and so there should be a maximum of two days' worth of data latency.

See the section "Disaster Recovery Planning and Procedures" in Chapter 16, "Redundancy and Disaster Recovery," for more information.

Incorrect answers: All of the other answers give incorrect descriptions of RTO and RPO. Know your acronyms!

74. Answer: D. DDoS

Explanation: A DDoS (distributed denial of service) attack is occurring. Most likely there is a botnet with computers on the Internet (such as 212.119.64.32) and computers on the LAN (such as 10.254.254.102) that are all zombies—and part of the botnet—concentrating an attack on the server at 10.254.254.201. It is known as a distributed attack because the entire attack is broken up among multiple computers. These attacks often happen on a large scale, where thousands of computers simultaneously attack a well-known server.

See the section "Malicious Attacks" in Chapter 7, "Networking Protocols and Threats," for more information.

Incorrect answers: The Xmas tree attack is one where special packets are sent that have specific flags set. It can ultimately act as a denial of service (DoS) attack if launched correctly. But it is not used for distributed DoS attacks. *XSS* stands for cross-site scripting, a type of code injection attack that exploits a computer programming flaw, often in web server forms. As mentioned, *DoS* stands for denial of service, an attack often performed by a single computer, not six or thousands in the way that a DDoS attack would occur.

75. Answers: A and D. Disk wiping and full disk encryption

Explanation: You don't want anyone else to get a hold of your SSL certificates, even if they are expired. The best solution in the scenario is to either destroy the drives yourself or store them in a secure location for a period of time. However, if you are sending them to a third party for destruction, the best option would be to fully wipe the drives; sanitize them with powerful software, and strong methods such as the Gutmann method. Barring that, you would want to consider full disk encryption (FDE) that utilizes AES or another powerful cipher. This way, the third party, and anyone else between you and the third party, will not be able to learn the RSA keys that the certificates are based on.

See the section "Legislative and Organizational Policies" in Chapter 18, "Policies and Procedures," for more information.

Incorrect answers: A data retention policy states how long data must be stored by an organization. If the drives are going to another company, then this policy is moot in this case. The server's hard drives that are referred to in the question are most likely internal drives, so removable media encryption (for things such as USB flash drives) has no bearing here. Disk hashing is not necessary. You are not interested in the data anymore, so there is no reason to hash it.

76. Answer: A. Key stretching

Explanation: Key stretching techniques will take a weak key, process it, and output an enhanced and more powerful key. This is often based on a password, and will include salting, making dictionary attacks and brute-forcing difficult to accomplish. The phrase "…slowing down the runtime of the hashing algorithm and increasing entropy by passing the input and salt back during each iteration" is the key. Salting usually happens in conjunction with key stretching, so that was the first hint. Next, "each iteration" is another hint meaning the original hash is re-hashed over and over. Warning: too many iterations can slow down the server where passwords are being checked.

See the section "Hashing Basics" in Chapter 14, "Encryption and Hashing Concepts," for more information.

Incorrect answers: When dealing with ciphers, *confusion* refers to making the relationship between a key and the ciphertext as complex as possible, and *diffusion* refers to the structure of the plaintext being dissipated into the ciphertext. In encryption, *substitution* is commonly used for confusion and *transposition* is commonly used for diffusion. The Root of Trust (RoT) is the set of functions in trusted computing that are always trusted by the operating system. A monoalphabetic cipher is one that uses fixed substitution, such as in the Caesar cipher or ROT13. *PRNG* stands for pseudorandom number generator, which is most likely being used in this scenario as part of the hashing process, but it is not what the engineer is referring to directly. *Pass the hash* is a hacking technique where an attacker obtains the password hash of one or more user accounts, and reapplies them to a server or other system in order to fool the system into thinking that the attacker is authentic—we use key stretching and hashing to make passwords more secure so that we can avoid attacks such as pass the hash.

77. Answers: B, D, F. Compartmentalize the network, apply technical controls to meet compliance regulation, and establish a list of devices that must meet regulations

Explanation: Of the listed options, the best ones for achieving compliance with PCI (Payment Card Industry) and SOX (Sarbanes-Oxley) regulations include the following:

1) Compartmentalize the network—divvy up the network with methods such as VLANs, subnetting, DMZs, whatever security boundary necessary to protect servers and clients that deal with sensitive data.

2) Apply technical controls to meet compliance regulations—for example, vulnerability management, monitoring, protecting data, and so on.

3) Establish a list of devices that must meet regulations: Any devices and computers that will have payment info, health info, or PII of any kind flowing through them should be analyzed, secured, and continually monitored.

PCI compliance requirements can be summed up as the following:

- Protect cardholder data
- Build and maintain a secure network
- Maintain an information security policy
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test systems and networks

See the section "Legislative and Organizational Policies" in Chapter 18, "Policies and Procedures," for more information.

Incorrect answers: Establish a company framework is somewhat vague but could refer to creating an IT security framework. This is a very good idea, but it is more of a high-level plan on how to execute actual procedures and policies, and not the procedures and policies themselves. Centralizing management of all devices might be a good idea from a management perspective, but for security, certain devices will no doubt need to be compartmentalized. Establishing a list of users who work with each regulation is a good idea, but not as important as the technical controls previously mentioned. Note: Remember to familiarize yourself with whatever policies and procedures your organization employs, whether they are related to PCI, SOX, ISO, or other compliance and regulatory methods.

78. Answer: B. The hash key summary of the hardware and the specialized program no longer match.

Explanation: Some software activations are based on a hardware key, or a hardware key and a software key that are compared. The key is normally a hash value (computed with either MD5 or SHA-256, for instance), and if the hash values don't match, then the specialized program won't be able to execute the online activation process, which is required because the image was restored to the new computer (with a new and different key). This, of course, is the most likely cause, but not the only possible reason for why the specialized program stopped functioning.

See the section "Hashing Basics" in Chapter 14, "Encryption and Hashing Concepts," for more information.

Incorrect answers: If the image file to be restored was encrypted with the wrong key, then you wouldn't be able to complete the restoration, and the computer would not function. In trusted computing, remote attestation is when a client computer authenticates its hardware and software configuration to a remote server with the goal being to determine the level of trust—often using a PKI. Remote attestation might indeed be failing, but it is less likely being caused by blocked ports. The software configuration of the affected computer should not have changed, even after the restoration. Plus, the scenario doesn't mention any network changes, so the configuration of ports, ACLs, and so on should be the same. The least likely answer is that the binary files of the specialized program have been modified by malware.

Malware can target binary files, but it is less common compared to other types of files such as executables. Many application developers will protect their binary files with transport layer security encryption, making them difficult (if not impossible) to modify.

79. Answer: D. Fingerprinting

Explanation: The technique being used here is fingerprinting, which is used to find out information about a system. It can be done passively by sniffing packets between hosts, or actively by sending special packets to a target and analyzing the responses. It can be done by scanning ports, or by using commands in a browser's URL bar as is the case in this scenario. By adding syntax to the end of a domain, you can "test" the web server and ascertain information about it based on the results. In this case, we see "ORA-000001: SQL command not properly ended" is the result. This tells us that the website is running an Oracle database (a relational SQL-oriented database). From there an attacker could limit attack techniques to that particular type of server, saving time. Now, if you were to run that actual syntax against my website, you would not see anything about Oracle, but you might get a 404 Not Found error. Underneath it would tell you that the server is running Apache web server software, OpenSSL, and more. Unless, that is, we improved upon our input validation and secure coding concepts, which is exactly why these tests are performed—to uncover these vulnerabilities.

See the section "Secure Programming" in Chapter 5, "Application Security," and "Conducting Risk Assessments" in Chapter 12, "Vulnerability and Risk Assessment," for more information.

Incorrect answers: Cross-site scripting (XSS) exploits the trust a user's browser has in a website through code injection, often in web forms, but not in the URL bar. SQL injection is a type of code injection when user input in database web forms is not filtered correctly and is executed improperly. Privilege escalation is the act of exploiting a bug or design flaw in a software or firmware application to gain access to resources that normally would've been protected from an application or user. Remote code execution (RCE) is when an attacker obtains control of a target computer through some sort of vulnerability. Finally, a zero day attack is one that is executed on a vulnerability in software before that vulnerability is known to the creator. Unfortunately, as a security administrator, you are expected to be able to predict the future to a certain extent, and protect against the unknown. Don't worry, though; the more experienced you get, the easier this becomes!

80. Answer: C. Place the remote desktop server(s) on a screened subnet, and implement two-factor authentication.

Explanation: The key phrase here is that the risk assessment suggests that Windows should be protected from ingress traffic. That mainly implies the Windows clients, but could include the Windows server as well. Either way, to that end, one of the best ways to secure the server is to compartmentalize the remote desktop server on a screened subnet. Remember that contractors will be using this server too, so you don't want it to be anywhere near other important servers in your network, and possibly it should be isolated from any and all servers. The two-factor authentication is the icing on the cake, and is an excellent solution for remote workers where theft/loss of laptops can occur. All in all, it's the best of the listed answers.

See the sections "Network Design" in Chapter 6, "Network Design Elements," and "Authentication Models and Components" in Chapter 10, "Physical Security and Authentication Models," for more information.

Incorrect answers:

"Change remote desktop to a non-standard port, and implement password complexity for the entire active directory domain."—Changing the remote desktop port is commonly implemented. For example, Microsoft remote desktop services uses 3389 inbound by default. Any

attacker with a little experience knows this. So, changing the port is a good idea, but from the answer you can assume that the server is not in a screened subnet, DMZ, or similar protected area. Implementing password complexity for the Active Directory domain implies that the remote desktop server is located in the domain. You probably don't want that, or at least need to compartmentalize it in some way. Also, password complexity should already have been enabled, especially if this is an enterprise-level corporate network.

"Distribute new IPsec VPN client software to applicable parties, and then virtualize the remote desktop services functionality."—It's kind of a given: you would have to distribute *some kind* of VPN client software in order for remote users to connect. However, IPsec implies an L2TP connection. There are better, more secure options such as a Cisco GRE tunnel, or an always-on SSL/TLS-based VPN. But that doesn't tackle the problem of server location. Also, "virtualize the remote desktop services functionality" is vague. Are we talking about the clients? Server? Both? Most likely clients, and virtualizing apps can have security benefits, but remote desktop client apps aren't commonly virtualized. And if this is a large enterprise network (implying lots of remote users), then a virtualized remote access server is probably not a good idea from a performance standpoint.

"Deploy a remote desktop server on your internal LAN, and require an active directory integrated SSL connection for access."—We definitely don't want the remote access server on the LAN. No, it should be located somewhere more secure such as a DMZ, subnet, on the cloud, etc. Active Directory with SSL (meaning LDAP over SSL, port 636) is a good idea, but it again implies that the remote desktop server is on the LAN. Using a subnet or DMZ and using multifactor authentication dismisses most of the security issues associated with this incorrect answer's solution.

Remember to carefully secure your remote desktop servers using a layered defense strategy, especially if that server requires communication with a domain controller or other server on the LAN.

That is the end of the practice exam answers and explanations. Next, be sure to visit the companion website (www.pearsonitcertification.com/title/9780789759122) for additional practice exams, real-world scenarios, videos, and simulations. And visit my personal website as well (www.davidlprowse.com) for articles and videos relating to computer security.