APPENDIX B

Memory Tables Answer Key

Chapter 2

Table 2-1 Summary of Malware Threats

Malware Threat	Definition	Example
Virus	Code that runs on a computer without the user's knowledge; it infects the computer when the code is accessed and executed.	Love Bug virus Ex: *love-letter-for-you.txt.vbs*
Worm	Similar to viruses except that it self-replicates whereas a virus does not.	Nimda Propagated through network shares and mass e-mailing
Trojan horse	Appears to perform desired functions but are actually performing malicious functions behind the scenes.	Remote access Trojan Ex: SubSeven malware application
Spyware	Malicious software either downloaded unwittingly from a website or installed along with some other third-party software.	Internet Optimizer (aka DyFuCA)
Rootkit	Software designed to gain administrator-level control over a computer system without being detected.	Boot loader rootkits Ex: Evil Maid Attack
Spam	The abuse of electronic messaging systems such as e-mail, broadcast media, and instant messaging.	Phishing identity theft e-mails Lottery scam e-mails

Table 2-2 Summary of Malware Prevention Techniques

Malware Threat	Prevention Techniques
Virus	Run and update antivirus software. Scan the entire system periodically. Update the operating system. Use a firewall.
Worm	Run and update antivirus software. Scan the entire system periodically.
Trojan horse	Run and update antivirus software. Scan the entire system periodically. Run a Trojan scan periodically.
Spyware	Run and update antispyware software. Scan the entire system periodically. Adjust web browser settings. Consider technologies that discourage spyware.
Rootkit	Run and update antivirus software. Use rootkit detector programs.
Spam	Use a spam filter. Configure whitelists and blacklists. Close open mail relays. Train your users.

Chapter 3

Patch Management

- **Planning—**Before actually doing anything, a plan should be set into motion. The first thing that needs to be decided is whether the patch is necessary and if it will be compatible with other systems. Microsoft Baseline Security Analyzer (MBSA) is one example of a program that can identify security misconfigurations on the computers in your network, letting you know if patching is needed. If the patch is deemed necessary, the plan should consist of a way to test the patch in a "clean" network on clean systems, how and when the patch will be implemented, and how the patch will be checked after it is installed.
- **Testing—**Before automating the deployment of a patch among a thousand computers, it makes sense to test it on a single system or small group of systems first. These systems should be reserved for testing purposes only and should not be used by "civilians" or regular users on the network. I know, this is asking a lot, especially given the amount of resources some companies have. But the more you can push for at least a single testing system that is not a part of the main network, the less you will have to cover your tracks if a failure occurs!
- **Implementing—**If the test is successful, the patch should be deployed to all the necessary systems. In many cases this will be done in the evening or over the weekend for larger updates. Patches can be deployed automatically using software such as Microsoft's Systems Management Server (SMS).
- **Auditing—**When the implementation is complete, the systems (or at least a sample of systems) should be audited; first, to make sure the patch has taken hold properly, and second, to check for any changes or failures due to the patch. SMS, and other third-party tools can be used in this endeavor.

Keeping a Well-Maintained Computer

Step 1. **Use a surge protector or UPS—**Make sure the computer and other equipment connect to a surge protector, or better yet a UPS if you are concerned about power loss.

Step 2. **Update the BIOS—**Flashing the BIOS isn't always necessary; check the manufacturer's website for your motherboard to see if an update is needed.

Step 3. **Update Windows—**This includes the latest SPs and any Windows updates beyond that and setting Windows to alert if there are any new updates.

Step 4. **Update antimalware—**This includes making sure that there is a current license for the antimalware (antivirus and antispyware) and verifying that updates are turned on and the software is regularly scanning the system.

Step 5. **Update the firewall—**Be sure to have some kind of firewall installed and enabled; then update it. If it is the Windows Firewall, updates should happen automatically through Windows Update. However, if you have a SOHO router with a built-in firewall, or other firewall device, you need to update the device's ROM by downloading the latest image from the manufacturer's website.

Step 6. **Maintain the disks—**This means running a disk cleanup program regularly and checking to see if the hard disk needs to be defragmented from once a week to once a month depending on the amount of usage. It also means creating restore points, doing Complete PC Backups, or using third-party backup or drive imaging software.

Step 7. **(Optional) Create an image of the system**—After all your configurations and hardening of the OS are complete, you might consider creating an image of the system. Imaging the system is like taking a snapshot of the entire system partition. That information is saved as one large file or a set of compressed files that can be saved anywhere. It's kind of like system restore but at another level. The beauty of this is that you can reinstall the entire image if your system fails or is compromised, quickly and efficiently, with very little configuration necessary—only the latest security and AV updates since the image was created need to be applied. Of course, most imaging software has a price tag involved, but it can be well worth it if you are concerned about the time it would take to get your system back up and running in the event of a failure. This is the basis for standardized images in many organizations. By applying mandated security configurations, updates, and so on, and then taking an image of the system, you can create a snapshot in time that you can easily revert to if necessary, while being confident that a certain level of security is already embedded into the image.

Chapter 4

Table 4-1 Common Applications and Safeguards

Application Name	Safeguards
Outlook	Install the latest Office service pack. (This applies to all Office suite applications.) Keep Office up to date with Windows Update. (This also applies to all Office suite applications.) Increase the junk e-mail security level or use a whitelist. Read messages in plain text instead of HTML. Enable attachment blocking. Use a version that enables Object model guard functionality, or download it for older versions. Password protect any .PST files. Consider encrypting the authentication scheme, and possibly other traffic, including message traffic between Outlook clients and Exchange servers. Secure Password Authentication (SPA) can be used to secure the login and S/MIME, and PGP can be used to secure actual e-mail transmissions.
Word	Consider using passwords for opening or modifying documents. Use read-only or comments only (tracking changes) settings. Consider using a digital certificate to seal the document.
Excel	Use password protection on worksheets. Set macro security levels. Consider Excel encryption.

Table 4-2 Summary of Programming Vulnerabilities and Attacks

Vulnerability	Description
Backdoor	Placed by programmers, knowingly or inadvertently, to bypass normal authentication, and other security mechanisms in place
Buffer overflow	When a process stores data outside the memory that the developer intended
Cross-site scripting (XSS)	Exploits the trust a user's browser has in a website through code injection, often in web forms

continues

Table 4-2 Continued

Vulnerability	Description
Cross-site request forgery (XSRF)	Exploits the trust that a website has in a user's browser, which becomes compromised and transmits unauthorized commands to the website
SQL injection	User input in database web forms is not filtered correctly and is executed improperly
Directory traversal	A method of accessing unauthorized parent (or worse, root) directories

Chapter 5

Table 5-1 Private IP Ranges (as Assigned by the IANA)

IP Class	Assigned Range
Class A	10.0.0.0–10.255.255.255
Class B	172.16.0.0–172.31.255.255
Class C	192.168.0.0–192.168.255.255

Table 5-2 Types of IPv6 Addresses

IPv6 Type	Address Range	Purpose
Unicast	Global Unicast starts at 2000 Link-local ::1 and FE80::/10	Address assigned to one interface of one host.
Anycast	Structured like unicast addresses	Address assigned to a group of interfaces on multiple nodes. Packets are delivered to the "first" interface only.
Multicast	FF00::/8	Address assigned to a group of interfaces on multiple nodes. Packets are delivered to all interfaces.

Table 5-4 Port Ranges

Port Range	Category Type	Description
0–1023	Well-Known Ports	This range defines commonly used protocols, for example HTTP uses port 80. They are designated by the IANA (Internet Assigned Numbers Authority), which is operated by the ICANN (Internet Corporation for Assigned Names and Numbers).
1024–49,151	Registered Ports	Ports used by vendors for proprietary applications. These must be registered with the IANA For example, Microsoft registered 3,389 for use with the Remote Desktop Protocol (RDP), aka Microsoft Terminal Server.
49,152–65,535	Dynamic and Private Ports	These ports can be used by applications but cannot be registered by vendors.

Table 5-5 Ports and Their Associated Protocols

Port Number	Associated Protocol (or Keyword)	Full Name	Usage
7	Echo	Echo	Testing round trip times between hosts.
19	CHARGEN	Character Generator	Testing and debugging.
21	FTP	File Transfer Protocol	Transfers files from host to host.
22	SSH	Secure Shell	Remotely administers network devices and Unix/Linux systems. Also used by Secure copy (SCP) and Secure FTP (SFTP).
23	Telnet	TErminaL NETwork	Remotely administers network devices (deprecated).
25	SMTP	Simple Mail Transfer Protocol	Sends email.
49	TACACS	Terminal Access Controller Access-Control System	Remote authentication.
53	DNS	Domain Name System	Resolves IP addresses to host names.

continues

Table 5-5 Continued

Port Number	Associated Protocol (or Keyword)	Full Name	Usage
69	TFTP	Trivial File Transfer Protocol	Basic version of FTP.
80	HTTP	Hypertext Transfer Protocol	Transmits web page data.
88	Kerberos	Kerberos	Network authentication, uses tickets.
110	POP3	Post Office Protocol Version 3	Receives email.
119	NNTP	Network News Transfer Protocol	Transports Usenet articles.
135	RPC/epmap/ dcom-scm	Microsoft End Point Mapper/ DCE Endpoint Resolution	Used to locate DCOM ports. Also known as RPC (Remote Procedure Call).
137-139	NetBIOS	NetBIOS Name, Datagram, and Session Services, respectively	Name querying, sending data, NetBIOS connections.
143	IMAP	Internet Message Access Protocol	Retrieval of email with advantages over POP3.
161	SNMP	Simple Network Management Protocol	Remotely monitor network devices.
389	LDAP	Lightweight Directory Access Protocol	Maintains directories of users and other objects.
443	HTTPS	Hypertext Transfer Protocol Secure (uses TLS or SSL)	Secure transfer of hypertext through web pages. Used by FTPS.
445	SMB	Server Message Block	Provides shared access to files and other resources
636	LDAP over TLS/SSL	Lightweight Directory Access Protocol (over TLS/SSL)	Secure version of LDAP
1433	Ms-sql-s	Microsoft SQL Server	Opens queries to SQL server
1701	L2TP	Layer 2 Tunneling Protocol	VPN protocol with no inherent security. Often used with IPsec
1723	PPTP	Point-to-Point Tunneling Protocol	VPN protocol with built-in security
3389	RDP	Remote Desktop Protocol (Microsoft Terminal Server)	Remotely views and controls other systems

Chapter 6

Table 6-1 Summary of NIDS Versus NIPS

Type of System	Summary	Disadvantage/Advantage	Example
NIDS	Detects malicious network activities	Pro: Only a limited amount of NIDS are necessary on a network. Con: Only *detects* malicious activities.	Snort Bro-IDS
NIPS	Detects, removes, detains, and redirects traffic	Pro: Detects and mitigates malicious activity. Pro: Can act as a protocol analyzer. Con: Uses more resources. Con: Possibility of false positives and false negatives.	Dragon IPS McAfee IntruShield

Chapter 7

Table 7-1 Weak, Strong, and Stronger Passwords

Password	Strength of Password
Prowse	Weak
DavidProwse	Medium
|ocrian7	Strong
This1sV#ryS3cure	Very strong or “best”

Privilege Escalation

- **Vertical privilege escalation—**When a lower privileged user accesses functions reserved for higher privilege users, for example, if a standard user can access functions of an administrator. This is also known as privilege elevation and is the most common description. To protect against this, update the network device firmware. In the case of an operating system, it should again be updated, and usage of some type of access control system is also advisable, for example User Access Control (UAC).

- **Horizontal privilege escalation—**When a normal user accesses functions or content reserved for other normal users, for example, if one user reads another's e-mail. This can be done through hacking or by a person walking over to other people's computers and simply reading their e-mail! Always have your users lock their computer (or log off) when they are not physically at their desk!

Table 7-2 Wireless Protocols

Wireless Protocol	Description	Encryption Level (Key Size)
WEP	Wired Equivalent Privacy (Deprecated)	64-bit
WPA	Wi-Fi Protected Access	128-bit
WPA2	Wi-Fi Protected Access Version 2	256-bit
TKIP	Temporal Key Integrity Protocol (Deprecated) Encryption protocol used with WEP and WPA	128-bit
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol Encryption protocol used with WPA2 Addresses the vulnerabilities of TKIP Meets requirements of IEEE 802.11i	128-bit
AES	Advanced Encryption Standard Encryption protocol used with WPA/WPA2 Strongest encryption method in this table	128-bit, 192-bit, and 256-bit

Chapter 8

Table 8-1 VPN Tunneling Protocols

Tunneling Protocol	Description	Port Used
Point-to-Point Tunneling Protocol (PPTP)	This is the more commonly used tunneling protocol (although that is quickly changing) but the less secure solution of the two listed here. PPTP generally includes security mechanisms and no additional software or protocols need to be loaded. A VPN device or server must have inbound port 1723 open to enable incoming PPTP connections. PPTP works within the Point-to-Point Protocol (PPP) that is also used for dial-up connections, as we mentioned earlier.	Port 1723
Layer 2 Tunneling Protocol (L2TP)	This is quickly gaining popularity due to the inclusion of IPSec as its security protocol. Although this is a separate protocol and L2TP doesn't have any inherent security, L2TP will be considered the more secure solution because IPSec is required in most L2TP implementations. A VPN device or server must have inbound port 1701 open to enable incoming L2TP connections.	Port 1701

Table 8-2 Summary of Authentication Technologies

Authentication Type	Description
802.1X	An IEEE standard that defines port-based Network Access Control (PNAC). 802.1X is a Data Link Layer authentication technology used to connect devices to a LAN or WLAN.
LDAP	An Application Layer protocol used for accessing and modifying directory services data. It is part of the TCP/IP suite. Originally used in WAN connections, it has morphed into a protocol commonly used by services such as Microsoft Active Directory.
Kerberos	An authentication protocol designed at MIT that enables computers to prove their identity to each other in a secure manner. It is used most often in a client-server environment; the client and the server both verify each other's identity.

continues

Table 8-2 Continued

Authentication Type	Description
RAS	A service that enables dial-up and various types of VPN connections from remote clients.
CHAP	An authentication scheme used by the Point-to-Point Protocol (PPP) that is the standard for dial-up connections. It utilizes a challenge-response mechanism with one-way encryption.
RADIUS	Used to provide centralized administration of dial-up, VPN, and wireless authentication. It can be used with EAP and 802.1X.
TACACS	Another remote authentication protocol, similar to RADIUS, and used more often in UNIX networks though it is deprecated.
TACACS+	Remote authentication developed by Cisco, similar to RADIUS but separates authentication and authorization into two separate processes.

Chapter 9

Mandatory Access Control

- **Rule-based access control—**Also known as label-based access control, this defines whether access should be granted or denied to objects by comparing the object label and the subject label.
- **Lattice-based access control—**Used for more complex determinations of object access by subjects. Somewhat advanced mathematics are used to create sets of objects and subjects and define how the two interact.

Table 9-1 Summary of Access Control Models

Tunneling Protocol	Key Points
DAC	Every object in the system has an owner. Permissions are determined by the owner.
MAC	Permissions are determined by the system. Can be rule-based or lattice-based. Labels are used to identify security levels of subjects and objects.
RBAC	Based on roles, or sets of permissions involved in an operation. Controlled by the system.

Here are a couple more tips when it comes to user accounts, passwords, and logons:

- **Rename and password protect the Administrator account—**It's nice that Windows has incorporated a separate administrator account: The problem is that by default the account has no password. To configure this account, navigate to **Computer Management > System Tools > Local Users and Groups > Users** and locate the **Administrator** account. In a domain, this would be in **ADUC > Domain name > Users**. By right-clicking the account, you see a drop-down menu in which you can rename it and/or give it a password. (Just remember the new username and password!) Now it's great to have this additional administrator account on the shelf just in case the primary account fails; however, some OSs such as Vista disable the account by default. To enable it, right-click the account and select **Properties**. In the General tab, deselect the **Account Is Disabled** check box. Alternatively, open the command line and type **net user administrator /active:yes**. The way that the administrator account behaves by default will depend on the version of Windows. The Linux/UNIX counterpart is the root account. The same types of measures should be employed when dealing with this account.

- **Verify that the Guest account (and other unnecessary accounts) are disabled—** This can be done by right-clicking the account in question, selecting **Properties** and then selecting the checkbox named **Account Is Disabled**. It is also possible to delete accounts (aside from built-in accounts such as the Guest account); however, companies usually opt to have them disabled instead so that the company can retain information linking to the account. So if an employee is terminated, the system administrator should generally implement the policy of account disablement. By disabling the account, the employee in question can no longer log in to the network, but the system administrator still has access to the history of that account.

- **Use Ctrl+Alt+Del—**Pressing Ctrl+Alt+Del before the logon adds a layer of security to the logon process. This can be added as a policy on individual Windows computers. It is implemented by default with computers that are members of a domain.

- **Use policies—**Policies governing user accounts, passwords, and so on can help you to enforce your rules, as discussed in the next section. Large organizations with a lot of users will usually implement a self-service password management system. This means that users reset their own passwords after a given amount of time (set in a group policy); the administrator does not create passwords for users.

Chapter 10

Table 10-2 Summary of Risk Assessment Types

Risk Assessment Type	Description	Key Points
Qualitative risk assessment	Assigns numeric values to the probability of a risk, and the impact it can have on the system or network.	Numbers are arbitrary. Examples: 1–10 or 1–100.
Quantitative risk assessment	Measures risk by using exact monetary values. It attempts to give an expected yearly loss in dollars for any given risk.	Values are specific monetary amounts. SLE × ARO = ALE

Table 10-3 Summary of Chapter 10 Security Tools

Security Tool	Description
LAN Surveyor	Network mapping tool
Network Magic	Network mapping tool
Microsoft Visio	Network diagramming tool
Nessus	Vulnerability scanner
Nmap	Port scanner
Wireshark	Protocol analyzer
Fluke	Handheld protocol analyzer/network sniffer
Cain and Abel	Password cracking tool
John the Ripper	Password cracking tool

Chapter 11

Table 11-1 Summary of Monitoring Methodologies

Monitoring Methodology	Description
Signature-Based Monitoring	Network traffic is analyzed for predetermined attack patterns. These attack patterns are known as signatures.
Anomaly-Based Monitoring	Establishes a performance baseline based on a set of normal network traffic evaluations. Requires a baseline.
Behavior-Based Monitoring	Looks at the previous behavior of applications, executables, and/or the operating system and compares that to current activity on the system. If an application later behaves improperly, the monitoring system will attempt to stop the behavior. Requires a baseline.

Network adapters can work in one of two different modes: promiscuous and non-promiscuous.

- **Promiscuous mode—**When the network adapter captures all packets that it has access to regardless of the destination of those packets.
- **Non-promiscuous mode—**When a network adapter captures only the packets that are addressed to it specifically.

Chapter 12

Table 12-3 Summary of Symmetric Algorithms

Algorithm Acronym	Full Name	Maximum/Typical Key Size
DES	Data Encryption Standard	56-bit
3DES	Triple DES	168-bit
AES	Advanced Encryption Standard	256-bit
RC4	Rivest Cipher version 4	128-bit typical
RC5	Rivest Cipher version 5	64-bit typical
RC6	Rivest Cipher version 6	256-bit typical

Chapter 14

Table 14-1 RAID Descriptions

RAID Level	Description	Fault Tolerant?	Minimum Number of Disks
RAID 0	Striping Data is striped across multiple disks to increase performance.	No	Two
RAID 1	Mirroring Data is copied to two identical disks. If one disk fails, the other continues to operate. See Figure 14-1 for an illustration. This RAID version allows for the least amount of downtime because there is a complete copy of the data ready to at a moment's notice. When each disk is connected to a separate controller, this is known as disk duplexing.	Yes	Two (and two only)

Table 14-1 RAID Descriptions

RAID Level	Description	Fault Tolerant?	Minimum Number of Disks
RAID 5	Striping with Parity Data is striped across multiple disks; fault-tolerant parity data is also written to each disk. If one disk fails, the array can reconstruct the data from the parity information. See Figure 14-2 for an illustration.	Yes	Three
RAID 6	Striping with Double Parity Data is striped across multiple disks as it is in RAID 5, but there are two stripes of parity information. This usually requires another disk in the array. This system can operate even with two failed drives and is more adequate for time-critical systems.	Yes	Four
RAID 0+1	Combines the advantages of RAID 0 and RAID 1. Requires a minimum of four disks. This system contains two RAID 0 striped sets. Those two sets are mirrored.	Yes	Four
RAID 1+0	Combines the advantages of RAID 1 and RAID 0. Requires a minimum of two disks but will usually have four or more. This system contains at least two mirrored disks that are then striped.	Yes	Two (usually four)

Redundant Sites

- **Hot site—**A near duplicate of the original site of the organization that can be up and running within minutes (maybe longer). Computers and phones are installed and ready to go, a simulated version of the server room stands ready, and vast majority of the data is replicated to the site on a regular basis in the event that the original site is not accessible to users for whatever reason. Hot sites are used by companies that would face financial ruin in the case that a disaster makes their main site inaccessible for a few days of even a few hours. This is the only type of redundant site that can facilitate a *full* recovery.

- **Warm site—**Will have computers, phones, and servers, but they might require some configuration before users can start working on them. The warm site will have backups of data that might need to be restored; they will probably be several days old. This is chosen the most often by organizations because it has a good amount of configuration, yet remains less expensive than a hot site.
- **Cold site—**Has tables, chairs, bathrooms, and possibly some technical setup; for example basic phone, data, and electric lines. Otherwise, a lot of configuration of computers and data restoration is necessary before the site can be properly utilized. This type of site is used only if a company can handle the stress of being nonproductive for a week or more.

Data Backup

- **Full backup—**When all the contents of a folder are backed up. It can be stored on one or more tapes. If more than one is used, the restore process would require starting with the oldest tape and moving through the tapes chronologically one by one. Full backups can use a lot of space, causing a backup operator to make use of a lot of backup tapes which can be expensive. Full backups can also be time-consuming if there is a lot of data. So, quite often, incremental and differential backups are used with full backups as part of a backup plan.
- **Incremental backup—**Backs up only the contents of a folder that has changed since the last full backup or the last incremental backup. An incremental backup must be preceded by a full backup. Restoring the contents of a folder or volume would require a person to start with the full backup tape and then move on to each of the incremental tapes chronologically, ending with the latest incremental backup tape. Incremental backups started in the time of floppy disks when storage space and backup speed were quite limited. Some operating systems and backup systems will associate an archive bit (or archive flag) to any file that has been modified; this indicates to the backup program that it should be backed up during the next backup phase. If this is the case, the incremental backup will reset the bit after backup is complete.

- **Differential backup—**Backs up only the contents of a folder that has changed since the last full backup. A differential backup must be preceded by a full backup. To restore data, a person would start with the full backup tape and then move on to the differential tape. Differential backups do not reset the archive bit when backing up. This means that incremental backups will not see or know that a differential backup has occurred.

Other Backup Schemes

- **10 tape rotation—**This method is simple and provides easy access to data that has been backed up. It can be accomplished during a 2-week backup period, each tape is used once per day for 2 weeks. Then the entire set is recycled. Generally, this will be similar to the one-week schedule shown previously, however, the second Monday might be a differential backup instead of a full backup. And the second Friday might be a full backup, which is archived. There are several options; you would need to run some backups and see which is best for you given the amount of tapes required and time spent running the backups.
- **Grandfather-father-son—**This backup rotation scheme is probably the most common backup method used. When attempting to use this scheme, three sets of backup tapes must be defined—usually they are daily, weekly, and monthly, which correspond to son, father, and grandfather. Backups are rotated on a daily basis; normally the last one of the week will be graduated to father status. Weekly (father) backups are rotated on a weekly basis with the last one of the month being graduated to grandfather status. Quite often, monthly (grandfather) backups, or a copy of them, are archived offsite.
- **Towers of Hanoi—**This backup rotation scheme is based on the mathematics of the Towers of Hanoi puzzle. This also uses three backup sets, but they are rotated differently. Without getting into the mathematics behind it, the basic idea is that the first tape is used every 2nd day, the second tape is used every 4th day, and the third tape is used every 8th day. Table 14-3 shows an example of this. Keep in mind that this can go further; a fourth tape can be used every 16th day, and a fifth tape every 32nd day, and so on, although it gets much more complex to remember what tapes to use to backup and which order to go by when restoring. The table shows an example with three tape sets represented as set A, B, and C.

Chapter 15

Table 15-1 Summary of Social Engineering Types

Type	Description
Pretexting	When a person invents a scenario, or pretext, in the hope of persuading a victim to divulge information.
Diversion theft	When a thief attempts to take responsibility for a shipment by diverting the delivery to a nearby location
Phishing	The attempt at fraudulently obtaining private information, usually done electronically. Vishing is done by phone. Spear phishing targets specific individuals. Whaling targets senior executives.
Hoax	The attempt at deceiving people into believing something that is false.
Shoulder surfing	When a person uses direct observation to find out a target's password, PIN, or other such authentication information.
Eavesdropping	When a person uses direct observation to "listen" in to a conversation. This could be a person hiding around the corner or a person tapping into a phone conversation.
Dumpster diving	When a person literally scavenges for private information in garbage and recyclable containers.
Baiting	When a malicious individual leaves malware-infected removable media such as a USB drive or optical disc lying around in plain view in the hopes that unknowing people will bring it back to their computer and access it.
Piggybacking/ Tailgating	When an unauthorized person tags along with an authorized person to gain entry to a restricted area.

Table 15-4 Acts Passed Concerning the Disclosure of Data and PII

Act	Acronym	Description
Privacy act of 1974	n/a	Establishes a code of fair information practice. Governs the collection, use, and dissemination of personally identifiable information about persons' records maintained by federal agencies.
Sarbanes-Oxley	SOX	Governs the disclosure of financial and accounting information. Enacted in 2002.

Table 15-4 Acts Passed Concerning the Disclosure of Data and PII

Act	Acronym	Description
Health Insurance Portability and Accountability Act	HIPAA	Governs the disclosure and protection of health information. Enacted in 1996.
Gramm-Leach-Bliley Act	GLB	Enables commercial banks, investment banks, securities firms, and insurance companies to consolidate. Protects against pretexting. Individuals need proper authority to gain access to nonpublic information, such as Social Security numbers.
California SB 1386	SB 1386	Requires California businesses that store computerized personal information to immediately disclose breaches of security. Enacted in 2003.

Table 15-5 Summary of Policy Types

Type	Description
Acceptable use	Policy that defines the rules that restrict how a computer, network, or other system may be used.
Change management	A structured way of changing the state of a computer system, network, or IT procedure.
Separation of duties	When more than one person is required to complete a task
Job rotation	When a particular task is rotated among a group of employees
Mandatory vacations	When an organization requires employees to take X amount of consecutive days vacation over the course of a year as part of their annual leave.
Due diligence	Ensuring that IT infrastructure risks are known and managed
Due care	The mitigation action that an organization takes to defend against the risks that have been uncovered during due diligence
Due process	The principle that an organization must respect and safeguard personnel's rights