Chapter 16
Managing Security Operations

THE CISSP TOPICS COVERED IN THIS CHAPTER INCLUDE:

- ✓ **Domain 2.0: Asset Security**
  - 2.3 Provision information and assets securely
    - 2.3.1 Information and asset ownership
    - 2.3.2 Asset inventory (e.g., tangible, intangible)
    - 2.3.3 Asset management
- ✓ **Domain 3: Security Architecture and Engineering**
  - 3.1 Research, implement and manage engineering processes using secure design principles
    - 3.1.2 Least privilege
    - 3.1.6 Segregation of Duties (SoD)
  - 3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
    - 3.5.6 Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
    - 3.5.11 Serverless
- ✓ **Domain 7: Security Operations**
  - 7.3 Perform configuration management (CM) (e.g., provisioning, baselining, automation)
  - 7.4 Apply foundational security operations concepts
    - 7.4.1 Need-to-know/least privilege
    - 7.4.2 Segregation of Duties (SoD) and responsibilities
    - 7.4.3 Privileged account management
    - 7.4.4 Job rotation
    - 7.4.5 Service-level agreements (SLA)

- 7.5 Apply resource protection
  - 7.5.1 Media management
  - 7.5.2 Media protection techniques
  - 7.5.3 Data at rest/data in transit
- 7.8 Implement and support patch and vulnerability management
- 7.9 Understand and participate in change management processes
- 7.15 Address personnel safety and security concerns
  - 7.15.1 Travel
  - 7.15.2 Security training and awareness (e.g., insider threat, social media impacts, two-factor authentication (2FA) fatigue)
  - 7.15.3 Emergency management
  - 7.15.4 Duress

✓ **Domain 8: Software Development Security**

- 8.4 Assess security impact of acquired software
  - 8.4.4 Managed services (e.g., enterprise applications)
  - 8.4.5 Cloud services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

Security operations includes a wide range of security foundational concepts and best practices. These include several core concepts that any organization needs to implement to provide basic security protection. The first section of this chapter covers these concepts.

Resource protection ensures that information and assets are securely provisioned when they're deployed and throughout their life cycle. Configuration management ensures that systems are configured correctly, and change management processes protect against outages from unauthorized changes. Patch and vulnerability management controls ensure that systems are up-to-date and protected against known vulnerabilities.

Apply Foundational Security Operations Concepts

The primary purpose of IT security operations practices is to safeguard assets such as information, systems, devices, facilities, and applications. These practices help identify threats and vulnerabilities and implement controls to reduce the risk to these assets.

In the context of IT security, due care and due diligence refer to taking reasonable care to protect an organization's assets on an ongoing basis. Senior management has a direct responsibility to exercise due care and due diligence. Implementing the common security operations concepts covered in the following sections, along with performing periodic security audits and reviews, demonstrates a level of due care and due diligence that will reduce senior management's liability when a loss occurs.

Exam Tip

Remember to keep the concepts of due care and due diligence top of mind. Chapter 1, “Security Governance Through Principles and Policies,” included a complete discussion of those topics.

Need-to-Know and Least Privilege

Need-to-know and the principle of least privilege are two standard principles followed in any secure IT environment. They help protect valuable assets by limiting access to these assets. Though they are related and many people use the terms interchangeably, there is a distinctive difference between the two.

Need-to-Know Access

The *need-to-know* principle imposes the requirement to grant users access only to data or resources they need to perform assigned work tasks. The primary purpose is to keep secret information secret. If you want to keep a secret, the best way is to tell no one. If you're the only person who knows it, you can ensure that it remains a secret. If you tell a trusted friend, it might remain secret. However, your trusted friend might tell someone else—such as another trusted friend. The risk of the secret leaking out to others increases as more and more people learn it. Limit the people who know the secret, and you increase the chances of keeping it secret.

Need-to-know is commonly associated with security clearances, such as a person having a Secret clearance. However, the clearance doesn't automatically grant access to the data. As an example, imagine that Sally has a Secret clearance. This indicates that she is cleared to access Secret data. However, the clearance doesn't automatically grant her access to all Secret data. Instead, administrators grant her access to only the Secret data she has a need-to-know for her job.

Although need-to-know is most often associated with military and government agencies' clearances, it can also apply in civilian organizations. For example, database administrators may need access to a database server to perform maintenance, but they don't need access to all the data within the server's databases. Restricting access on a need-to-know basis helps protect against unauthorized access that could result in a loss of confidentiality.

The Principle of Least Privilege

The *least privilege* principle states that subjects are granted only the privileges necessary to perform assigned work tasks and no more. Keep in mind that privilege in this context includes both permissions to data and rights to perform systems tasks. For data, it includes controlling the ability to read, write, create, alter, or delete data. Limiting and controlling privileges based on this concept protects confidentiality and data integrity. If users can modify only those data files that their work tasks require them to modify, it protects other files' integrity in the environment.

NOTE The least privilege principle relies on the assumption that all users have a well-defined job description that personnel understand. Without a specific job description, it is not possible to know what privileges users need.

This principle extends beyond just accessing data, though—it also applies to system access. For example, in many networks regular users can log on to any computer in the network using a network account. However, organizations commonly restrict this privilege by preventing regular users from logging on to servers or restricting users' access to a single workstation.

Organizations sometimes violate this principle by adding all users to the local Administrators group or granting root access to a computer. This gives the users full control over the computer. However, regular users rarely need this much access. When they have this much access, they can accidentally (or intentionally) damage the system, such as accessing or deleting valuable data.

Additionally, if a user logs on with full administrative privileges and inadvertently installs malware, the malware can assume full administrative privileges of the user's account. In contrast, if the user logs on with a regular user account, malware can only assume the regular account's limited privileges. Chapter 14, "Controlling and Monitoring Access," discussed this in more depth within the context of privilege escalation.

Least privilege is typically focused on ensuring that user privileges are restricted, but it also applies to other subjects, such as applications and system processes. For example, services and applications often run under the context of an account specifically created for the service or application. Historically, administrators often gave these service accounts full administrative privileges without considering the principle of least privilege. If attackers compromise the application, they can potentially assume the service account's privileges, granting the attacker full administrative privileges.

Segregation of Duties (SoD) and Responsibilities

Segregation of duties (SoD) and responsibilities ensures that no single person has total control over a critical function or system. This is necessary to ensure that no single person can compromise the system or its security. Instead, two or more people must conspire or collude against the organization, which increases the risk for these people.

Exam Tip

Segregation of duties is also known as separation of duties. Fortunately, both share the same SoD acronym. If you see either phrase on the CISSP exam, know that they are synonymous.

A segregation of duties policy creates a checks-and-balances system where two or more users verify each other's actions and must work in concert to accomplish necessary work tasks. This makes it more difficult for individuals to engage in malicious, fraudulent, or unauthorized activities and broadens the scope of detection and reporting. In contrast, individuals may be more tempted to perform unauthorized acts if they think they can get away with them. With two or more people involved, the risk of detection increases and acts as an effective deterrent.

Here's a simple example. Movie theaters use segregation of duties to prevent fraud. One person sells tickets. Another person collects the tickets and doesn't allow entry to anyone who doesn't have a ticket. If the same person collects the money and grants entry, this person can allow people in without a ticket or pocket the collected money without issuing a ticket. Of course, the ticket seller and the ticket collector can get together and concoct a plan to steal from the movie theater. This is collusion because it is an agreement between two or more persons to perform some unauthorized activity. However, collusion takes more effort and increases the risk to each of them. Segregation of duties policies help reduce fraud by requiring collusion between two or more people to perform unauthorized activity.

Similarly, organizations often break down processes into multiple tasks or duties and assign these duties to different individuals to prevent fraud. For example, one person approves payment for a valid invoice, but someone else makes the payment. If one person controlled the entire process of approval and payment, it would be easy to approve bogus invoices and defraud the company.

Another way segregation of duties is enforced is by dividing the security or administrative capabilities and functions among multiple trusted individuals. When the organization divides administration and security responsibilities among several users, no single person has sufficient access to circumvent or disable security mechanisms.

Two-Person Control

Two-person control (sometimes called the two-man rule) requires the approval of two individuals for critical tasks. For example, safe deposit boxes in banks often require two keys. A bank employee controls one key, and the customer holds the second key. Both keys are required to open the box, and bank employees allow a customer access to the box only after verifying the customer's identification.

Using two-person controls within an organization ensures peer review and reduces the likelihood of collusion and fraud. For example, an organization can require two individuals within the company (such as the chief financial officer and the chief executive officer) to approve key business decisions.

Additionally, some privileged activities can be configured so that they require two administrators to work together to complete a task. As an example, some privilege access management (PAM) solutions create special administrative accounts for emergency use only. The password is split in half so that two people need to enter the password to log on.

Split knowledge combines the concepts of segregation of duties and two-person control into a single solution. The basic idea is that the information or privilege required to perform an operation is divided among two or more users. This ensures that no single person has sufficient privileges to compromise the security of the environment.

Job Rotation

Job rotation (sometimes called rotation of duties) means that employees rotate through jobs or rotate job responsibilities with other employees. Using job rotation as a security control provides peer review, reduces fraud, and enables cross-training. Cross-training helps make an environment less dependent on any single individual.

A job rotation policy can act as both a deterrent and a detection mechanism. If employees know that someone else will be taking over their job responsibilities in the future, they are less likely to take part in fraudulent activities. If they choose to do so anyway, individuals taking over the job responsibilities later are likely to discover the fraud.

Mandatory Vacations

Many organizations require employees to take *mandatory vacations* in one-week or two-week increments. This provides a form of peer review and helps detect fraud and collusion. This policy ensures that another employee takes over an individual's job responsibilities for at least a week. If an employee is involved in fraud, the person taking over the responsibilities is likely to discover it.

Mandatory vacations can act as both a deterrent and a detection mechanism, just as job rotation policies can. Even though someone else will take over a person's responsibilities for just a week or two, this is often enough to detect irregularities.

NOTE Financial organizations are at risk of significant losses from fraud by employees. They often use job rotation, segregation of duties and responsibilities, and mandatory vacation policies to reduce these risks. Combined, these policies help prevent incidents and help detect them when they occur.

Privileged Account Management

Privileged account management (PAM) solutions restrict access to privileged accounts or detect when accounts use any elevated privileges. In this context, privileged accounts are administrator accounts or any accounts that have specific elevated privileges. This can include help desk workers who have been granted limited privileges to perform certain activities.

In Microsoft domains, this includes local administrator accounts (who have full control over a computer), users in the Domain Admins group (who have full control of any computers in a domain), and users in the Enterprise Admins group (who have full control over all the domains in a forest). In Linux, this includes anyone using the root account or granted root access via sudo.

NOTE Chapter 14 discussed some common Kerberos attacks allowing attackers to take control of admin accounts. It also discusses the sudo account.

Microsoft domains include a privileged access management (PAM) solution that can restrict privileged access. It's based on a Just-in-Time administration principle. Users are placed in a privileged group, but members of the group don't have elevated privileges. Instead, they request permission to use elevated privileges when they need them. The PAM solution approves this request behind the scenes and grants it within seconds by issuing a time-limited ticket. The user only has elevated privileges for a specific time, such as 15 minutes. After the time is up, the ticket expires. This approach thwarts common Kerberos attacks because the tickets quickly expire. Even if an attacker harvests one of these tickets, it is unusable.

On a more basic level, privileged account management monitors actions taken by privileged accounts. This includes creating new user accounts, adding new routes to a routing table, altering the configuration of a firewall, and accessing system log and audit files. Monitoring ensures that users granted these privileges do not abuse them.

> Monitoring special privileges is combined with other basic principles, such as least privilege and segregation of duties and responsibilities. Principles such as least privilege and segregation of duties help prevent security policy violations, and monitoring helps to deter and detect any violations that occur despite the use of preventive controls.

Employees filling these privileged roles are usually trusted employees. However, there are many reasons why an employee can change from a trusted employee to a disgruntled employee or malicious insider. Reasons that can change a trusted employee's behavior can be as simple as a lower-than-expected bonus, a negative performance review, or just a personal grudge against another employee. However, by monitoring usage of special privileges, an organization can deter an employee from misusing the privileges and detect the action if a trusted employee does misuse them.

Many automated tools are available that can monitor the usage of special privileges. When an administrator or privileged operator performs one of these activities, the tool can log the event and send an alert. Additionally, access review audits detect misuse of these privileges.

For example, many attackers use PowerShell scripts to escalate their privileges. By configuring a security information and event management (SIEM) system to detect and send alerts on certain events, it's possible to detect the use of malicious PowerShell scripts. There's more to this than just looking for specific Event IDs (such as Event ID 4104). After modifying registry entries, the SIEM can also record an entire PowerShell script and look for commands that attackers commonly use. Chapter 17, “Preventing and Responding to Incidents,” covers SIEM systems in more depth.

Detecting APTs

Monitoring the use of elevated privileges can also detect advanced persistent threat (APT) activities. For example, the U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) released a technical alert (TA17-239A) describing the activities of an APT targeting energy, nuclear, water, aviation, and some critical manufacturing sectors, along with some government entities.

The alert details how attackers infected a single system with a malicious phishing email or by exploiting server vulnerabilities. Once they exploited a single system, they escalated their privileges and began performing many common privileged operations, including the following:

- Accessing and deleting logs
- Creating and manipulating accounts (such as adding new accounts to the Administrators group)
- Controlling communication paths (such as opening port 3389 to enable the Remote Desktop Protocol and/or disabling the host firewall)
- Running various scripts (including PowerShell, batch, and JavaScript files)
- Creating and scheduling tasks (such as one that logged their accounts out after 8 hours to mimic the behavior of a regular user)

Monitoring common privileged operations can detect these activities early in the attack. In contrast, if the actions go undetected, the APT can remain embedded in the network for years.

Service-Level Agreements (SLAs)

A *service-level agreement (SLA)* is an agreement between an organization and an outside entity, such as a vendor. The SLA stipulates performance expectations and often includes penalties if the vendor doesn't meet these expectations.

As an example, many organizations use cloud-based services to rent servers. A vendor provides access to the servers and maintains them to ensure that they are available. The organization can use an SLA to specify availability, such as with uptimes and downtimes. With this in mind, an organization should have a clear idea of their requirements when working with third parties and ensure that the SLA includes these requirements.

In addition to an SLA, organizations sometimes use a memorandum of understanding (MOU). MOUs document the intention of two entities to work together toward a common goal. Although a MOU is similar to an SLA, it is less formal and doesn't include any monetary penalties if one of the parties doesn't meet its responsibilities.

Address Personnel Safety and Security

Personnel safety concerns are an essential element of security operations. It's possible to replace things such as data, servers, and even entire buildings. In contrast, it isn't possible to replace people. With that in mind, organizations should implement security controls that enhance personnel safety.

As an example, consider the exit door in a data center controlled by a pushbutton electronic cipher lock. If a fire results in a power outage, does the exit door automatically unlock or remain locked? An organization that values assets in the server room more than personnel safety might decide to ensure that the door remains locked when power isn't available. Doing so protects the physical assets in the data center, but it also risks the lives of personnel within the room because they won't be able to easily exit the room. In contrast, an organization that values personnel safety over the data center's assets will ensure that the locks unlock the exit door when power is lost.

Duress

Duress systems are useful when personnel are working alone. For example, a single guard might be guarding a building after hours. If a group of people break into the building, the guard probably can't stop them on their own. However, a guard can raise an alarm with a duress system. A simple duress system is just a button that sends a distress call. A monitoring entity receives the distress call and responds based on established procedures. The monitoring entity could initiate a phone call or text message back to the person who sent the distress call. In this example, the guard responds by confirming the situation.

Security systems often include code words or phrases that personnel use to verify that everything truly is okay or verify that there is a problem. For example, a code phrase indicating everything is okay could be “Everything is awesome.” If a guard inadvertently activated the duress system and the monitoring entity responded, the guard says, “Everything is awesome” and then explains what happened. However, if criminals apprehended the guard, the guard could skip the phrase and instead make up a story of how the duress system was accidentally activated. The monitoring entity would recognize that the guard skipped the code phrase and send help.

Some electronic cipher locks support two or more codes, such as one for regular use and one to raise an alarm. Normally, employees would enter a code (such as 1 2 3 4) to open the door to a secure area. In a duress situation, they could enter a different code (such as 5 6 7 8) that would open the door and set off a silent alarm.

Travel

Another safety concern is when employees travel because criminals might target an organization's employees while they are traveling. Training personnel on safe practices while traveling can enhance their safety and prevent security incidents. This includes simple things such as verifying a person's identity before opening the hotel door. If room service is delivering complimentary food, a call to the front desk can verify if this is valid or part of a scam.

Employees should also be warned about the many risks associated with electronic devices (such as smartphones, tablets, and laptops) when traveling. These risks include the following:

Sensitive Data Ideally, the devices should not contain any sensitive data. This prevents the loss of data if the devices are lost or stolen. If an employee needs this data while traveling, it should be protected with strong encryption.

Malware and Monitoring Devices There have been many reported cases of malware being installed on systems while employees were visiting a foreign country. Similarly, we have heard firsthand accounts of physical monitoring devices being installed inside devices after a trip to a foreign country. People might think their devices are safe in a hotel room as they go out to a local restaurant. However, this is more than enough time for someone who otherwise looks like hotel staff to enter your room, install malware in the operating system, and install a physical listening device inside the computer. Maintaining physical control of devices at all times can prevent these attacks. Additionally, security experts recommend that employees do not bring their personal devices but instead bring temporary devices to be used during the trip. After the trip, these can be wiped clean and reimaged.

Free Wi-Fi Free Wi-Fi often sounds appealing while traveling. However, it can easily be a trap configured to capture all the user's traffic. As an example, attackers can configure a Wi-Fi connection as an *on-path attack*, forcing all traffic to go through the attacker's system. The attacker can then capture all traffic. A sophisticated on-path attack (sometimes called a man-in-the-middle attack) can create an HTTPS connection between the client and the attacker's system and create another HTTPS connection between the attacker's system and an internet-based server. From the client's perspective, it looks like it is a secure HTTPS connection between the client's computer and the

Internet-based server. However, all the data is decrypted and easily viewable on the attacker's system. Instead, users should have a method of creating their own internet connection, such as through a smartphone or with a mobile wireless hotspot device.

VPNs Employers should have access to virtual private networks (VPNs) that they can use to create secure connections. These can be used to access resources in the internal network, including their work-related email.

Emergency Management

Emergency management plans and practices help an organization address personnel safety and security after a disaster. Disasters can be natural (such as hurricanes, tornadoes, or earthquakes) or the result of people's actions (such as fires, terrorist attacks, or cyberattacks causing massive power outages), as discussed in Chapter 18, “Disaster Recovery Planning.” Organizations will have different plans depending on the types of natural disasters they are likely to experience. The safety of personnel should be a primary consideration during any disaster.

Security Training and Awareness

Chapter 2, “Personnel Security and Risk Management Concepts,” covered security training and awareness programs in greater depth. If an organization has a training and awareness program in place, it's relatively easy to add personnel safety and security topics. These programs help ensure that personnel are aware of duress systems, travel best practices, emergency management plans, and general safety and security best practices.

When addressing personnel safety and security, training programs should stress the importance of protecting people. Military warships travel into war zones during times of conflict, putting personnel at risk. However, they also do endless training to protect lives. Organizations rarely face the same level of risk but should still prioritize the value of human lives.

Of course, as you learned in Chapter 2, security training and awareness programs should include comprehensive coverage of cybersecurity topics as well. Some important topics to include are:

- *Insider threat*. Educate employees on the risks associated with unauthorized access or misuse of company data by employees, contractors, or business partners. Highlight the signs of potential insider threats and the protocols for reporting suspicious behavior.
- *Social media impacts*. Address the risks and vulnerabilities associated with oversharing on social media platforms. Teach employees about potential social engineering attacks that leverage publicly available information and the importance of setting strict privacy settings.
- *Two-factor authentication (2FA) fatigue*. This segment can address the common issue where users become complacent or irritated with 2FA, often trying to bypass or minimize its use. Training should emphasize the importance of 2FA in protecting both personal and organizational data, ways to make 2FA more user-friendly, and the potential consequences of neglecting this security measure.

Provision Information and Assets Securely

An important consideration when provisioning information and assets securely is asset management. Chapter 13, "Managing Identity and Authentication," covered provisioning and deprovisioning for accounts as part of the identity and access provisioning life cycle. This section focuses on hardware, software, and information assets.

Information and Asset Ownership

Chapter 5, "Protecting Security of Assets," discussed the importance of identifying and classifying information and assets. It also discussed various data roles. As a reminder, the data owner is the person who has ultimate organizational responsibility for the data. This is a senior manager, such as the chief executive officer (CEO), president, or department head.

Similarly, senior managers are ultimately responsible for other assets, such as hardware assets. Consider an IT department that manages servers. The IT department owns these servers, and the senior management in the IT department is responsible for protecting them.

The key point is that by identifying the assets' owners, an organization also identifies the individuals responsible for protecting those assets. Data owners typically delegate data protection tasks to others in the organization. For example, employees in the data custodian security role typically perform daily tasks such as implementing access controls, performing backups, and managing data storage.

Asset Management

Asset management refers to managing both tangible and intangible assets. This typically starts with inventories of assets, tracking the assets, and taking additional steps to protect them throughout their lifetime.

Tangible assets include hardware and software assets owned by the company. *Intangible assets* include patents, copyrights, a company's reputation, and other assets representing potential revenue. By managing assets successfully, an organization prevents losses.

Many organizations use an automated configuration management system (CMS) to help with hardware asset management. The primary purpose of a CMS is configuration management, discussed later in this chapter. The CMS needs to connect to hardware systems when checking configuration settings. While doing so, it verifies that the system is still on the network and turned on.

Hardware Asset Inventories

Hardware assets are IT resources such as computers, servers, routers, switches, and peripherals. Many organizations use databases and inventory applications to perform inventories and track hardware assets through the entire equipment life cycle.

For example, bar-code systems are available that can print bar codes to place on equipment. The bar-code database includes relevant details on the hardware, such as the model, serial number, and location. When the hardware is purchased, it is bar-coded before it is deployed. On a regular basis, personnel scan all of the bar codes with a bar-code reader to verify that the organization still controls the hardware.

A similar method uses radio frequency identification (RFID) tags. These tags transmit information to RFID readers. Personnel place the RFID tags on the equipment and use the RFID readers to inventory the equipment. RFID tags and readers are more expensive than bar codes and bar-code readers. However, RFID methods significantly reduce the time needed to perform an inventory.

Before disposing of equipment, personnel sanitize it. Sanitizing equipment removes all data to ensure that unauthorized personnel do not gain access to sensitive information. When equipment is at the end of its lifetime, it's easy for individuals to lose sight of the data that it contains, so using checklists to sanitize the system is often valuable. Checklists can include steps to sanitize hard drives, nonvolatile memory, and removable media such as CDs, DVDs, and USB flash drives within the system. NIST 800-88r1 and Chapter 5 have more information on procedures to sanitize drives.

Portable media, such as USB drives, holding sensitive data is also managed as an asset. For example, an organization can label portable media with bar codes and use a bar-code inventory system to complete inventories on a regular basis. This approach allows them to inventory the media holding sensitive data on a regular basis.

Software Asset Inventories

Software assets are operating systems and applications. Organizations pay for software, and license keys are routinely used to activate the software. The activation process often requires contacting a licensing server over the Internet to prevent piracy. If the license keys are leaked outside the organization, it can invalidate the organization's use. It's also important to monitor license compliance to avoid legal issues.

For example, an organization could purchase a license key for five software product installations but only install and activate one instance immediately. If the key is stolen and installed on four systems outside the organization, those activations will succeed. When the organization tries to install the application on internal systems, the activation will fail. Any type of license key is highly valuable to an organization and should be protected.

Software licensing also refers to ensuring that systems do not have unauthorized software installed. Many tools are available that can inspect systems remotely to detect the system's details. This allows them to identify unauthorized software running on systems, and helps an organization ensure that it complies with software licensing rules.

Intangible Inventories

Organizations don't inventory intangible resources in the same way as tangible inventories. However, an organization needs to keep track of intangible assets to protect them. Because these are intellectual assets (such as intellectual property, patents, trademarks, a company's reputation, and copyrights) instead of physical assets, it's difficult to assign them a monetary value.

The senior management team is typically the owner of these assets. They attempt to determine the value of intangible assets by estimating the benefits the assets will bring to the organization. As an example, imagine a company sells a product based on a patent. The revenue from these sales can be used to assign a value to the patent. Utility and plant patents in the United States are valid for 20 years and design patents for 15 years, so this time frame can also be used when calculating the value. The United States requires payment of maintenance fees periodically to maintain the patent. Failing to pay these fees can result in a loss of the patent, stressing the importance of tracking patents.

Large organizations report the value of intangible assets on their balance sheets using generally accepted accounting principles (GAAP). This helps them review their intangible assets at least annually.

Apply Resource Protection

Organizations apply various resource protection techniques to ensure that resources are provisioned securely and managed throughout their life cycle. As an example, desktop computers are often deployed using imaging techniques to ensure that they start in a known secure state. Change management and patch management techniques ensure that the systems are kept up-to-date with required changes. Imaging, change management, and patch management topics are discussed later in this chapter.

Information is stored on media, so an essential part of resource protection is protecting media. This includes when storing media and when the media reaches the end of its life cycle.

Media Management

Media management refers to the steps taken to protect media and data stored on media. In this context, media is anything that can hold data. It includes tapes, optical media such as CDs and DVDs, portable USB drives, internal hard drives, solid-state drives, and USB flash drives. Many portable devices, such as smartphones, fall into this category because they include memory cards that can hold data. Backups are often contained on tapes, so media management directly relates to tapes. However, media management extends beyond just backup tapes to any type of media that can hold data. It also includes any type of hard-copy data.

Media Protection Techniques

When media includes sensitive information, it should be stored in a secure location with strict access controls to prevent losses due to unauthorized access. Additionally, any location used to store media should have temperature and humidity controls to prevent losses due to corruption.

Media management can also include technical controls to restrict device access from computer systems. As an example, many organizations use technical controls to block the use of USB drives and/or detect and record when users attempt to use them. In some situations, a written security policy prohibits the use of USB flash drives, and automated detection methods detect and report any violations.

> NOTE The primary risks from USB flash drives are malware infections and data theft. A system infected with a virus can detect when a user inserts a USB drive and infect it. When the user inserts this infected drive into another system, the malware attempts to infect the second system. Additionally, malicious users can easily copy and transfer large amounts of data and conceal the drive in their pocket.

Properly managing media directly addresses confidentiality, integrity, and availability. When media is marked, handled, and stored properly, it helps prevent unauthorized disclosure (loss of confidentiality), unauthorized modification (loss of integrity), and unauthorized destruction (loss of availability).

Controlling USB Flash Drives

Many organizations restrict the use of USB flash drives to specific brands purchased and provided by the organization. This strategy allows the organization to protect data on the drives and ensure that the drives are not being used to inadvertently transfer malicious software (malware) between systems. Users still have the benefit of USB flash drives, but this practice reduces risk for the organization without hampering the user's ability to use USB drives.

For example, some organizations sell IronKey flash drives that include multiple levels of built-in protection. Several authentication mechanisms are available to ensure that only authorized users can access data on the drive. Such drives protect data with built-in AES 256-bit hardware-based encryption. Active antimalware software on the flash drive helps prevent malware from infecting the drive.

Some products include additional management solutions, allowing administrators to manage the devices remotely. For example, administrators can reset passwords, activate auditing, and update the devices from a central location.

Tape Media

Organizations commonly store backups on tapes, and tapes are highly susceptible to loss due to corruption. As a best practice, organizations should keep at least two copies of backups. They should maintain one copy on-site for immediate usage if necessary and store the second copy at a secure location off-site. If a catastrophic disaster such as a fire destroys the primary location, the data is still available at the alternate location.

The cleanliness of the storage area will directly affect the life span and usefulness of tape media. Additionally, magnetic fields can act as a degausser and erase or corrupt data on the tape. With this in mind, tapes should not be exposed to magnetic fields that can come from sources such as elevator motors and some printers. Here are some useful guidelines for managing tape media:

- Keep new media in its original sealed packaging until it's needed to protect it from dust and dirt.
- When opening a media package, take extra caution not to damage the media in any way. This includes avoiding sharp objects and not twisting or flexing the media.
- Avoid exposing the media to temperature extremes; it shouldn't be stored close to heaters, radiators, air conditioners, or other sources of extreme temperatures.
- Do not use media that has been damaged, exposed to abnormal levels of dust and dirt, or dropped.
- Media should be transported from one site to another in a temperature-controlled vehicle.
- Media should be protected from exposure to the outside environment; avoid sunlight, moisture, humidity, heat, and cold. It should be acclimated for 24 hours before use.
- Appropriate security should be maintained over media from the point of departure to the secured off-site storage facility. Media is vulnerable to damage and theft at any point during transportation.
- Appropriate security should be maintained over media throughout the lifetime of the media based on the classification level of data on the media.
- Consider encrypting backups to prevent unauthorized disclosure of data if the backup tapes are lost or stolen.

Mobile Devices

Mobile devices include laptops, smartphones, tablets, and smartwatches. These devices have internal memory or removable memory cards that can hold a significant amount of data. Data can include email with attachments, contacts, and scheduling information. Additionally, many devices include applications that allow users to read and manipulate different types of documents.

Chapter 9, “Security Vulnerabilities, Threats, and Countermeasures,” covered mobile devices in much more depth. The key is to remember that mobile devices include data storage abilities. If they are storing sensitive data, it's important to take steps to protect that data.

Managing Media Life Cycle

All media has a useful but finite life cycle. Reusable media is subject to a *mean time to failure (MTTF)* that is sometimes represented in the number of times it can be reused or the number of years you can expect to keep it. For example, some tapes include specifications saying they can be reused as many as 250 times or last up to 30 years under ideal conditions. However, many variables affect the lifetime of media and can reduce these estimates. It's important to monitor backups for errors and use them as a guide to gauge the lifetime in your environment. When a tape begins to generate errors, technicians should rotate it out of use.

> **NOTE** Chapter 10, “Physical Security Requirements,” covered MTTF in more depth in the context of equipment failure.

Once backup media has reached its MTTF, it should be destroyed. The classification of data held on the tape will dictate the method used to destroy the media. Some organizations degauss highly classified tapes when they've reached the end of their lifetime and then store them until they can destroy the tapes. It's common to destroy tapes in bulk shredders.

Chapter 5 discusses some of the security challenges with solid-state drives (SSDs). Specifically, degaussing does not remove data from an SSD, and built-in erase commands often do not sanitize the entire disk. Instead of attempting to remove data from SSDs, many organizations destroy them.

MTTF is different from mean time between failures (MTBF). MTTF is normally calculated for items that will not be repaired when they fail, such as a tape. In contrast, MTBF refers to the amount of time expected to elapse between failures of an item that personnel will repair, such as a computer server.

Managed Services in the Cloud

Cloud-based assets include any resources that an organization accesses using cloud computing. You may see these referred to as *managed services*. Cloud computing refers to on-demand access to computing resources available from almost anywhere, and cloud computing resources are highly available and easily scalable. Organizations typically lease cloud-based resources from outside the organization, but they can also host on-premises resources within the organization.

One of the primary challenges with cloud-based resources hosted outside the organization is that they are outside the organization's direct control, making it more difficult to manage the risk. Although the on-premises cloud provides the organization with much greater control, hosting resources in the cloud offers convenience.

Some cloud-based services only provide data storage and access. When storing data in the cloud, organizations must ensure that security controls are in place to prevent unauthorized access to the data. Additionally, organizations should formally define requirements to store and process data stored in the cloud. For example, the Department of Defense (DoD) Cloud Computing Security Requirements Guide (CC SRG) defines specific requirements for U.S. government agencies to follow when evaluating the use of cloud computing assets. This document identifies computing requirements for assets labeled Secret and below using six separate information impact levels.

All sensitive data should be encrypted. This includes data in transit as it is sent to the cloud and data at rest while it's stored. The DoD CC SRG states that the customer should manage encryption, including controlling all encryption keys. In other words, customers should not use encryption controlled by the vendor. This eliminates risks related to insider threats at the vendor and supports data destruction using cryptographic erase methods. Cryptographic erase methods permanently remove the cryptographic keys. If a strong encryption method is used, cryptographic erase methods ensure that data remains inaccessible.

Shared Responsibility with Cloud Service Models

There are varying levels of maintenance and security responsibilities for assets, depending on the service model. This includes maintaining the assets, ensuring that they remain functional, and keeping the systems and applications up-to-date with current patches.

Figure 16.1 (derived from Figure 2 in the DoD CC SRG) shows how vendors and customers share the maintenance and security responsibilities for the three primary cloud service models. Refer to it as you read through the following bullets.

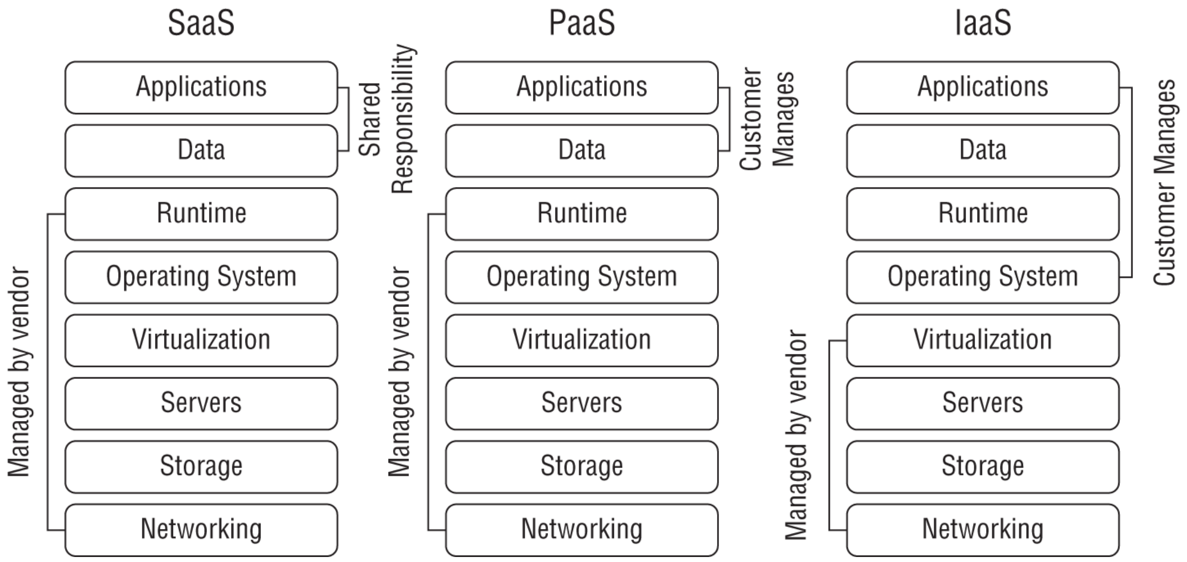

FIGURE 16.1 Cloud shared responsibility model

Software as a Service (SaaS) *Software as a service (SaaS)* models provide fully functional enterprise applications typically accessible via a web browser. For example, Google's Gmail is a SaaS application. The vendor (Google in this example) is responsible for all maintenance of the SaaS services. SaaS comes with shared responsibilities for data and applications. Customers may make configuration changes to their Gmail accounts. Customers also share responsibility for the data they keep and transmit via their Gmail accounts.

Platform as a Service (PaaS) *Platform as a service (PaaS)* models provide consumers with a computing platform, including hardware, operating systems, and a runtime environment. The runtime environment includes programming languages, libraries, services, and other tools supported by the vendor. Customers deploy applications that they've created or acquired, manage their applications, and possibly modify some configuration settings on the host. However, the vendor is responsible for maintenance of the host and the underlying cloud infrastructure.

Infrastructure as a Service (IaaS) *Infrastructure as a service (IaaS)* models provide basic computing resources to customers. This includes servers, storage, and networking resources. Customers install operating systems and applications and perform all required maintenance on the operating systems and applications. The vendor maintains the cloud-based infrastructure, ensuring that consumers have access to leased systems.

> TIP *NIST SP 800-145—The NIST Definition of Cloud Computing*, provides standard definitions for many cloud-based services. This includes definitions for service models (SaaS, PaaS, and IaaS), and definitions for deployment models (public, private, community, and hybrid). *NIST SP 800-144—Guidelines on Security and Privacy in Public Cloud Computing*, provides in-depth details on security issues related to cloud computing.

The cloud deployment model also affects the breakdown of responsibilities of the cloud-based assets. The four cloud deployment models available are as follows:

- A *public cloud* model includes assets available for any consumers to rent or lease and is hosted by an external CSP. Service-level agreements can effectively ensure that the CSP provides the cloud-based services at a level acceptable to the organization.
- The *private cloud* deployment model is used for cloud-based assets for a single organization. Organizations can create and host private clouds using their own on-premises resources. If so, the organization is responsible for all maintenance. However, an organization can also rent resources from a third party for exclusive use of the organization. Maintenance requirements are typically split based on the service model (SaaS, PaaS, or IaaS).
- A *community cloud* deployment model provides cloud-based assets to two or more organizations that have a shared concern, such as a similar mission, security requirements, policy, or compliance considerations. Assets can be owned and managed by one or more of the organizations.

Maintenance responsibilities are shared based on who is hosting the assets and the service models.

- A *hybrid cloud* model includes a combination of two or more clouds that are bound together by a technology that provides data and application portability. Similar to a community cloud model, maintenance responsibilities are shared based on who is hosting the assets and the service models in use.

Anything as a Service (XaaS)

Anything as a service (XaaS) is the catchall term to refer to any type of computing service or capability that can be provided to customers through or over a cloud solution. Many service providers that are rolling out new offerings to their clientele are more often hosting the technology in a cloud solution rather than on-premises equipment. This can enable rapid expansion, scalability, high availability, and more when compared to the previous means of deployment.

One area of growth in XaaS is security as a service (SECaaS), where various forms of security services are being offered through cloud solutions, including backup, authentication, authorization, auditing/accounting, antimalware, storage, SIEM, IDS/IPS analysis, and monitoring as a service (MaaS). An SECaaS is also referred to as a managed service provider (MSP) or a managed security service provider (MSSP).

MSPs and MSSPs are third-party (often cloud-based) services that provide remote oversight and management of on-premises IT or cloud IT. Some MSPs/MSSPs are general purpose, some focus on specific IT areas (e.g., backup, security, storage, firewall), and others are vertical management focused (e.g., legal, medical, financial, government).

Scalability and Elasticity

Scalability refers to the ability of a system to handle additional workloads by adding additional resources. As an example, imagine a server has 16 GB of random access memory (RAM), but it can support 64 GB of RAM. It's possible to shut down the server and add additional RAM to scale it up.

Elasticity refers to a system's ability to add and remove resources dynamically, based on increasing or decreasing load. As an example, imagine an e-commerce server with 16 GB of RAM and a four-core processor. Marketing launches an excellent advertising campaign along with a sale. Suddenly, the server is overwhelmed with traffic. A cloud provider that supports elasticity can dynamically add more RAM and processors to meet the increased workload. When the sale ends and the workload decreases, the cloud provider can dynamically remove the additional resources.

> TIP Chapter 9 covers virtualization concepts. Virtualization technologies commonly support elasticity, too.

A key point is that elasticity methods don't require shutting a system down to add the resources. The resources are automatically added or removed to match the demand. In contrast, scalability methods are not typically automatic or dynamic, though they can be designed for automatic scalability (horizontal and vertical scaling). They are usually set up for manual scalability, which requires manual intervention to add additional resources, such as an administrator shutting down a system to add more RAM.

Although the examples mention RAM and processor resources, scalability and elasticity methods can extend a system's capability by adding other resources. This includes adding more bandwidth, disk space, or even more servers.

Services Integration

Services integration, *cloud integration*, *systems integration*, and *integration platform as a service (iPaaS)* is the design and architecture of an IT/IS solution that stitches together elements from on-premises and cloud sources into a seamless productive environment. The goals of services integration are to eliminate data silos (a situation where data is contained in one area and thus inaccessible to other applications or business units), expand access, clarify processing visibility, and improve functional connectivity of on-site and off-site resources. This can also be viewed as an example of a software-defined data center (SDDC).

Serverless Architecture

Serverless architecture is a cloud computing concept where code is managed by the customer and the platform (i.e., supporting hardware and software) or server is managed by the cloud service provider (CSP). There is always a physical server running the code, but this execution model allows the software designer/architect/programmer/developer to focus on the logic of their code and not have to be concerned about the parameters or limitations of a specific server. This is also known as *function as a service (FaaS)*.

Applications developed on serverless architecture are similar to microservices, and each function is crafted to operate independently and autonomously. This allows each function to be independently scaled by the cloud service provider (CSP). This is distinct from PaaS, where an entire execution environment or platform is spun up to host an application, and it is always running, consuming resources and racking up costs, even when it is not actively being used. With serverless architecture or FaaS, the functions run only when called and then terminate when their operations are completed, thus minimizing costs.

Perform Configuration Management (CM)

Configuration management (CM) helps ensure that systems are deployed in a secure, consistent state and that they stay in a secure, consistent state throughout their lifetime. Baselines and images are commonly used to deploy systems.

Provisioning

Provisioning new systems refers to installing and configuring the operating system and needed applications. Deploying operating systems and applications using all of the defaults typically enables many vulnerabilities. Instead, new systems should be configured to reduce the vulnerabilities.

A key consideration when provisioning a system is to harden it based on its use. Hardening a system makes it more secure than the default configuration and includes the following:

- Disable all unused services. As an example, a file server needs services that allow users to access files, but file servers rarely use FTP. If the server is not using FTP, it should be disabled.
- Close all unused logical ports. These are often closed by disabling unused services.
- Remove all unused applications. Some applications automatically add additional applications. If these aren't used, they should be removed.
- Change default passwords. Many applications have default passwords for some accounts. Attackers know these, so the passwords should be changed.

Baselining

A *baseline* is a starting point. In the context of configuration management, it is the starting configuration for a system. An easy way to think of a baseline is as a list of settings. An operating system baseline identifies all the settings to harden specific systems. For example, a baseline for a file server identifies the configuration settings to harden the file server. Desktop computers would have a different baseline. Although baselines provide a starting point, administrators often modify them as needed for different systems within their organization.

Using Images for Baselining

Many organizations use images to deploy baselines. Figure 16.2 shows the process of creating and deploying baseline images in an overall three-step process. Here are the steps:

> NOTE In practice, more details are involved in this process, depending on the tools used for imaging. For example, the steps to capture and deploy images using one product are different from the steps to capture and deploy images using another product.

1. An administrator starts by installing the operating system and all desired applications on a computer (labeled as the baseline system in the figure). The administrator then configures the system with relevant security and other settings to meet the organization's needs. Personnel then perform extensive testing to ensure that the system operates as expected before proceeding to the next step.

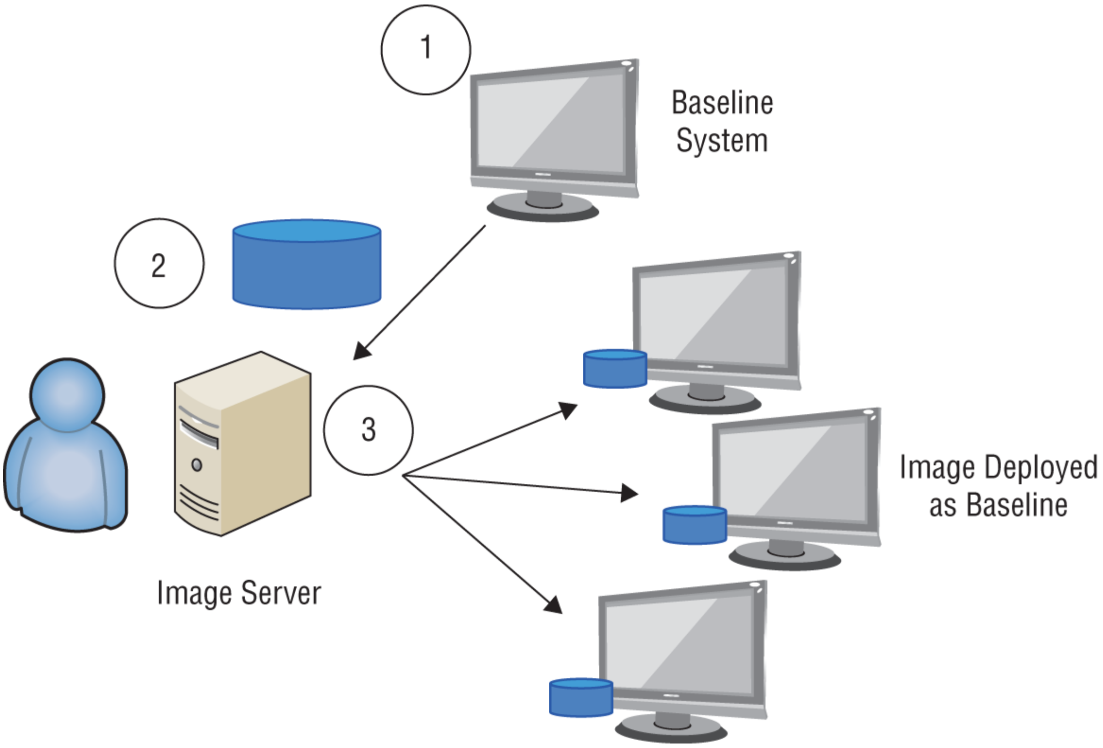

FIGURE 16.2 Creating and deploying images

2. Next, the administrator captures an image of the system using imaging software and stores it on a server (labeled as an Image Server in Figure 16.2). It's also possible to store images on external hard drives, USB drives, or DVDs.
3. Personnel then deploy the image to systems as needed. These systems often require additional configuration to finalize them, such as giving them unique names. However, the overall configuration of these systems is the same as the baseline system.

Baseline images improve the security of systems by ensuring that desired security settings are always configured correctly. Additionally, they reduce the amount of time required to deploy and maintain systems, thus reducing the overall maintenance costs. Deployment of a prebuilt image can require only a few minutes of a technician's time. If a user's system is corrupted, technicians can redeploy an image in minutes, instead of taking hours to troubleshoot the system or trying to rebuild it from scratch.

Organizations typically protect the baseline images to ensure that they aren't modified. In a worst-case scenario, malware can be injected into an image and then deployed to systems within the network.

Automation

It's common to combine imaging with other automated methods for baselines. In other words, administrators can create one image for all desktop computers within an organization. They then use automated methods to add additional applications, features, or settings for specific groups of computers. For example, computers in one department may have additional security settings or applications applied through scripting or other automated tools.

Microsoft's operating systems include Group Policy. Administrators can configure a Group Policy setting one time and automatically have the setting apply to all the computers in the domain. Other Group Policy settings can be configured to apply to all computers in a group, such as all file servers or all the accounting department's computers.

It's becoming common to make registry changes for some Windows systems. As an example, attackers are using PowerShell in offensive attacks quite often. Chapter 14 discusses PowerShell's use in privilege escalation attacks. By modifying some registry settings, administrators limit these attacks' effectiveness and detect them when they start. Some settings prevent an attacker from accessing PowerShell, and other settings enable additional logging so that administrators can see what the attackers are doing with PowerShell. Administrators can manipulate Group Policy settings to modify the appropriate registry settings.

Manage Change

Deploying systems in a secure state is a good start. However, it's also essential to ensure that systems retain that same level of security. *Change management* helps reduce unanticipated outages caused by unauthorized changes.

The primary goal of change management is to ensure that changes do not cause outages. Change management processes ensure that appropriate personnel review and approve changes before implementation and ensure that personnel test and document the changes.

Changes often create unintended side effects that can cause outages. For example, an administrator can change one system to resolve a problem but unknowingly cause a problem in other systems. Consider Figure 16.3. The web server is accessible from the Internet and accesses the database on the internal network. Administrators have configured appropriate ports on Firewall 1 to allow internet traffic to the web server and appropriate ports on Firewall 2 to allow the web server to access the database server.

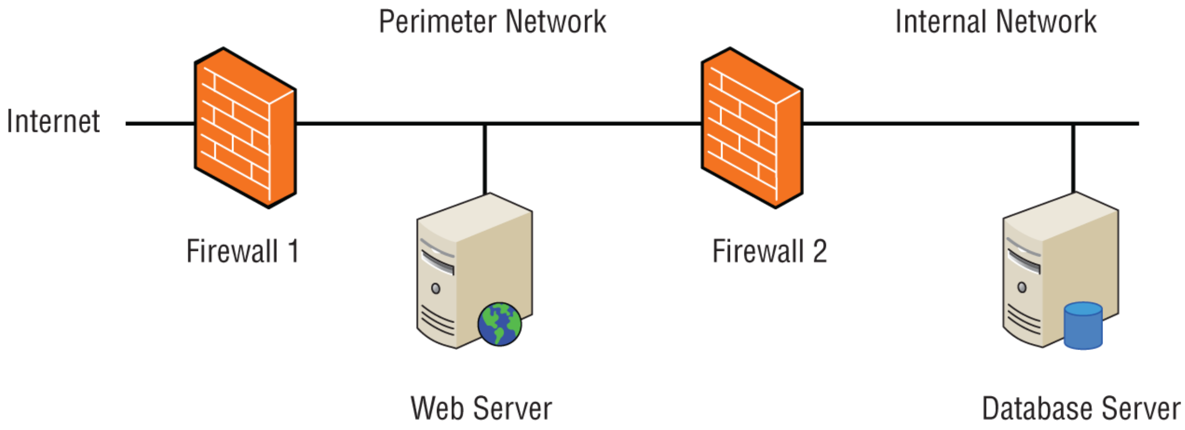

FIGURE 16.3 Web server and database server

A well-meaning firewall administrator may see an unrecognized open port on Firewall 2 and decide to close it in the interest of security. Unfortunately, the web server needs this port open to communicate with the database server, so when the port is closed, the web server will begin having problems. The help desk is soon flooded with requests to fix the web server, and people begin troubleshooting it. They ask the web server programmers for help, and after some troubleshooting, the developers realize that the database server isn't answering queries. They then call in the database administrators to troubleshoot the database server. After a bunch of hooting, hollering, blamestorming, and fingerpointing, someone realizes that a needed port on Firewall 2 is closed. They open the port and resolve the problem—at least until this well-meaning firewall administrator closes it again or starts tinkering with Firewall 1.

TIP Organizations constantly seek the best balance between security and usability. There are instances when an organization makes conscious decisions to improve the performance or usability of a system by weakening security. However, change management helps ensure that an organization takes the time to evaluate the risk of weakening security and compare it to the benefits of increased usability.

Unauthorized changes directly affect the *A* in the CIA Triad—availability. However, change management processes allow various IT experts to review proposed changes for unintended side effects before implementing the changes. These processes also give administrators time to check their work in controlled environments before implementing changes in production environments.

Additionally, some changes can weaken or reduce security. Imagine an organization isn't using an effective access control model to grant access to users. Administrators may not be able to keep up with the requests for additional access. Frustrated administrators may decide to add a group of users to an Administrators group within the network. Users will now have all the access they need, improving their ability to use the network, and they will no longer bother the administrators with access requests. However, granting administrator access in this way directly violates the least privilege principle and significantly weakens security.

NOTE Many of the configuration and change management concepts in use today are derived from ITIL (formally an acronym for Information Technology Infrastructure Library) documents originally published by the United Kingdom. Even though many of the concepts come from ITIL, organizations don't need to adopt ITIL to implement change and configuration management.

Change Management

A change management process ensures that personnel can perform a security impact analysis. Experts evaluate changes to identify any security impacts before personnel deploy the changes in a production environment.

Change management controls provide a process to control, document, track, and audit all system changes. This includes changes to any aspect of a system, including hardware and software configuration. Organizations implement change management processes through the life cycle of any system.

Common tasks within a change management process are as follows:

1. *Request the change.* Once personnel identify desired changes, they request the change. Some organizations use internal websites, allowing personnel to submit change requests via a web page. The website automatically logs the request in a database, which allows personnel to track the changes. It also allows anyone to see the status of a change request.
2. *Review the change.* Experts within the organization review the change. Personnel reviewing a change are typically from several different areas within the organization. In some cases, they may quickly complete the review and approve or reject the change. In other cases, the change may require

approval at a formal change review board or change advisory board (CAB) after extensive testing. Board members are the personnel who review the change request.

3. *Approve/reject the change.* Based on the review, these experts then approve or reject the change. They also record the response in the change management documentation. For example, if the organization uses an internal website, someone will document the results in the website's database. In some cases, the change review board might require the creation of a rollback or backout plan. This ensures that personnel can return the system to its original condition if the change results in a failure.
4. *Test the change.* Once the change is approved, it should be tested, preferably on a nonproduction server. Testing helps verify that the change doesn't cause an unanticipated problem.
5. *Schedule and implement the change.* The change is scheduled so that it can be implemented with the least impact on the system and the system's customer(s). This may require scheduling the change during off-duty or nonpeak hours. Testing should discover any problems, but it's still possible that the change causes unforeseen problems. Because of this, it's important to have a rollback plan. This allows personnel to undo the change and return the system to its previous state if necessary.
6. *Document the change.* The last step is the documentation of the change to ensure that all interested parties are aware of it. This step often requires a change in the configuration management documentation. If an unrelated disaster requires administrators to rebuild the system, the change management documentation provides them with information on the change. This ensures that they can return the system to the state it was in before the change.

There may be instances when an emergency change is required. For example, if an attack or malware infection takes one or more systems down, an administrator may need to make changes to a system or network to contain the incident. In this situation, the administrator still needs to document the changes. This ensures that the change review board can review the change for potential problems. Additionally, documenting the emergency change ensures that the affected system(s) will include the new configuration if it needs to be rebuilt.

When the change management process is enforced, it creates documentation for all changes to a system. This provides a trail of information if personnel need to reverse the change. If personnel need to implement the same change on other systems, the documentation also provides a roadmap or procedure to follow.

Change management control is a mandatory element for some security assurance requirements (SARs) in the ISO Common Criteria. However, change management controls are implemented in many organizations that don't require compliance with ISO Common Criteria. It improves the security of an environment by protecting against unauthorized changes that result in unintentional losses.

Versioning

Versioning typically refers to version control used in software configuration management. A labeling or numbering system differentiates between different software sets and configurations across multiple machines or at different points in time on a single machine. For example, the first version of an application may be labeled as 1.0. The first minor update would be labeled as 1.1, and the first major update would be 2.0. This helps keep track of changes over time to deployed software.

Although most established software developers recognize the importance of versioning and revision control with applications, many new web developers don't recognize its importance. These web developers have learned some excellent skills they use to create awesome websites, but don't always recognize the importance of underlying principles such as versioning control. If they don't control changes through some type of versioning control system, they can implement a change that effectively breaks the website.

Configuration Documentation

Configuration documentation identifies the current configuration of systems. It identifies who is responsible for the system and its purpose and lists all changes applied to the baseline. Years ago, many organizations used simple paper notebooks to record this information for servers, but it is much more common to store this information in files or databases today. Of course, the challenge with storing the documentation in a data file is that it can be inaccessible during an outage.

Manage Patches and Reduce Vulnerabilities

Patch and vulnerability management processes work together to help protect an organization against emerging threats. Bugs and security vulnerabilities are routinely discovered in operating systems and applications. As they are discovered, vendors write and test patches to remove the vulnerabilities. Patch management ensures that appropriate patches are applied, and vulnerability management helps verify that systems are not vulnerable to known threats.

Systems to Manage

It's worth stressing that patch and vulnerability management doesn't only apply to workstations and servers—it also applies to any computing device with an operating system. Network infrastructure systems such as routers, switches, firewalls, appliances (such as a unified threat management appliance), and printers all include some type of operating system. Some are Cisco-based, others are Microsoft-based, and others are Linux-based.

Embedded systems are any devices that have a CPU, that run an operating system, and that have one or more applications designed to perform one or more functions. Examples include camera systems, smart televisions, household appliances (such as burglar alarm systems, wireless thermostats, and refrigerators), automobiles, medical devices, and more. These devices are sometimes referred to as the Internet of Things (IoT).

These devices may have vulnerabilities requiring patches. For example, the massive distributed denial-of-service (DDoS) attack on Domain Name System (DNS) servers in late 2016 effectively took down the Internet by preventing users from accessing dozens of websites. Attackers reportedly used the Mirai malware to take control of IoT devices (such as Internet Protocol [IP] cameras, baby monitors, and printers) and join them to a botnet. Tens of millions of devices sent DNS lookup requests to DNS servers, effectively overloading them. Obviously, these devices should be patched to prevent a repeat of this attack, but many manufacturers, organizations, and owners don't patch IoT devices. Worse, many vendors don't even release patches.

Finally, if an organization allows employees to use mobile devices (such as smartphones and tablets) within the organizational network, these mobile devices should be managed. MDM software can deploy patches to mobile devices.

Patch Management

A *patch* is a blanket term for any type of code written to correct a bug or vulnerability or to improve existing software performance. The software can be either an operating system or an application. Patches are sometimes referred to as updates, quick fixes, and hot fixes. In the context of security, administrators are primarily concerned with security patches, which are patches that affect a system's vulnerability.

Even though vendors regularly write and release patches, these patches are useful only if they are applied. This may seem obvious, but many security incidents occur simply because organizations don't implement a patch management policy. As an example, one attack in May 2017 exploited a vulnerability in an Apache Struts web application that could have been patched in March 2017.

An effective *patch management* program ensures that systems are kept up-to-date with current patches. These are the common steps within an effective patch management program:

Evaluate patches. When vendors announce or release patches, administrators evaluate them to determine if they apply to their systems. For example, a patch released to fix a vulnerability on a Unix system configured as a Domain Name System (DNS) server is not relevant for a server running DNS on Windows. Similarly, a patch released to fix a feature running on a Windows system is not needed if the feature is not installed.

Test patches. Whenever possible, administrators test patches on an isolated nonproduction system to determine if the patch causes any unwanted side effects. The worst-case scenario is that a system will no longer start after applying a patch. For example, patches have occasionally caused systems to begin an endless reboot cycle. They boot into a stop error and keep trying to reboot to recover from the error. If testing shows this on a single system, it affects only one system. However, if an organization applies the patch to a thousand computers before testing it, it could have catastrophic results.

> Smaller organizations often choose not to evaluate, test, and approve patches but instead use an automatic method to approve and deploy the patches. Windows systems include Windows Update, which makes this easy. However, larger organizations usually take control of the process to prevent potential outages from updates.

Approve the patches. After administrators test the patches and determine them to be safe, they approve the patches for deployment. It's common to use a change management process (described earlier in this chapter) as part of the approval process.

Deploy the patches. After testing and approval, administrators deploy the patches. Many organizations use automated methods to deploy the patches. These can be third-party products or products provided by the software vendor.

Verify that patches are deployed. After deploying patches, administrators regularly test and audit systems to ensure that they remain patched. Many deployment tools include the ability to audit systems. Additionally, many vulnerability assessment tools include the ability to check systems to ensure that they have appropriate patches.

Patch Tuesday and Exploit Wednesday

Microsoft, Adobe, and Oracle regularly release patches on the second Tuesday of every month, commonly called Patch Tuesday or Update Tuesday. The regular schedule allows administrators to plan for the release of patches so that they have adequate time to test and deploy them. Many organizations that have support contracts with Microsoft have advance notification of the patches prior to Patch Tuesday. Some vulnerabilities are significant enough that Microsoft releases them “out-of-band.” In other words, instead of waiting for the next Patch Tuesday to release a patch, Microsoft releases some patches earlier.

Attackers realize that many organizations do not patch their systems right away. Some malicious actors have reverse-engineered patches to identify the underlying vulnerability and then created methods to exploit the vulnerability. These attacks often start within a day after Patch Tuesday, giving rise to the term *exploit Wednesday*.

However, many attacks occur on unpatched systems weeks, months, and even years after vendors release the patches. In other words, many systems remain unpatched, and attackers exploit them much later than a day after the vendor released the patch.

Vulnerability Management

Vulnerability management refers to regularly identifying vulnerabilities, evaluating them, and taking steps to mitigate risks associated with them. It isn't possible to eliminate risks. Similarly, it isn't possible to eliminate all vulnerabilities. However, an effective vulnerability management program helps an organization ensure that it is regularly evaluating vulnerabilities and mitigating the vulnerabilities that represent the greatest risks. Two common elements of a vulnerability management program are routine vulnerability scans and periodic vulnerability assessments.

> NOTE One of the most common vulnerabilities within an organization is an unpatched system, and so a vulnerability management program will often work in conjunction with a patch management program. In many cases, the duties of the two programs are separated between different employees. One person or group would be responsible for keeping systems patched, and another person or group would be responsible for verifying that the systems are patched. As with other segregation of duties implementations, this approach provides checks and balances within the organization.

Vulnerability Scans

Vulnerability scanners are software tools used to test systems and networks for known security issues. A vulnerability scan enumerates (or lists) all the vulnerabilities in a system. Attackers use vulnerability scanners to detect weaknesses in systems and networks, such as missing patches or weak passwords. After they detect the weaknesses, they launch attacks to exploit them. Administrators in many organizations use the same types of vulnerability scanners to detect vulnerabilities on their network. Their goal is to detect the vulnerabilities and mitigate them before an attacker discovers them.

Scanners include the ability to generate reports identifying any vulnerabilities they discover. The reports may recommend applying patches or making specific configuration or security setting changes to improve or impose security. These reports are passed on to personnel performing patch management and managing system settings. Simply recommending applying patches doesn't reduce the vulnerabilities. Administrators need to take steps to apply the patches.

However, there may be situations where it isn't feasible or desirable to do so. For example, if a patch fixing a minor security issue breaks an application on a system, management may decide not to implement the fix until developers create a workaround. The vulnerability scanner will regularly report the vulnerability, even though the organization has addressed the risk.

Management can choose to accept a risk rather than mitigate it. Any risk that remains after applying a control is residual risk. Any losses that occur from residual risk are the responsibility of management.

In contrast, an organization that never performs vulnerability scans will likely have many vulnerabilities. Additionally, these vulnerabilities will remain unknown, and management will not have the opportunity to decide which vulnerabilities to mitigate and which ones to accept.

Common Vulnerabilities and Exposures

Vulnerabilities are commonly referred to using the Common Vulnerabilities and Exposures (CVE) dictionary. The CVE dictionary provides a standard convention used to identify and describe vulnerabilities. MITRE maintains the CVE database, and you can view it here: www.cve.org.

MITRE looks like an acronym, but it isn't. The founders do have a history as research engineers at the Massachusetts Institute of Technology (MIT) and the name reminds people of that history. However, MITRE is not a part of MIT. MITRE receives funding from the U.S. Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) to maintain the CVE database.

Patch management and vulnerability management tools commonly use the CVE dictionary as a standard when scanning for specific vulnerabilities. As an example, CVE-2020-0601 identifies a vulnerability in the Windows CryptoAPI (`Crypt32.dll`). Microsoft patched this vulnerability in the January 2020 security update.

The CVE database makes it easier for companies that create patch management and vulnerability management tools. They don't have to expend any resources to manage the naming and definition of vulnerabilities, but instead focus on methods used to check systems for the vulnerabilities.

Summary

Several basic security principles are at the core of security operations in any environment. These include need-to-know, least privilege, segregation of duties (SoD) and responsibilities, job rotation and mandatory vacations, privileged account management, and service-level agreements (SLAs). Combined, these practices help prevent security incidents from occurring and limit the scope of incidents that do occur.

When addressing personnel safety and security, safety of personnel should always be a high priority. Duress systems allow guards to raise silent alarms in response to emergencies, and emergency management plans help the organization respond to disasters. Traveling presents unique risks to employees, such as the loss of data, malware installed on unattended systems, and intercepted data when using free Wi-Fi networks. Safety training and awareness programs ensure that personnel know the various risks and ways to mitigate them. Training and awareness programs should also address other critical issues, including the insider threat, social media use, and multifactor authentication fatigue.

Asset management extends beyond media to any asset considered valuable to an organization. This includes both tangible and intangible assets. Tangible assets include hardware and software, and organizations commonly inventory these assets to track them. Intangible assets include patents, trademarks, and copyrights, and organizations track these assets as well.

With resource protection, media and other assets that contain data are protected throughout their life cycle. Media includes anything that can hold data, such as tapes, internal drives, portable drives, CDs and DVDs, mobile devices, memory cards, and printouts. Media holding sensitive information should be marked, handled, stored, and destroyed using methods that are acceptable within the organization.

Managed services in the cloud include any resources stored in or accessed via the cloud. When negotiating with cloud service providers, you must understand who is responsible for maintenance and security. In general, the cloud service provider has the most responsibility with software as a service (SaaS) resources, less responsibility with platform as a service (PaaS) offerings, and the least responsibility with infrastructure as a service (IaaS) offerings. Cloud services commonly provide elasticity, which is the ability of services to dynamically respond to changing workload requirements.

Change and configuration management are two additional controls that help reduce outages. Configuration management ensures that systems are deployed in a consistent manner that is known to be secure. Imaging is a common configuration management technique that ensures that systems start with a known baseline. Change management helps reduce unintended outages from unauthorized changes and can also help prevent changes from weakening security.

Patch and vulnerability management procedures work together to keep systems protected against known vulnerabilities. Patch management keeps systems up-to-date with relevant patches. Vulnerability management includes vulnerability scans to check for a wide variety of known vulnerabilities (including unpatched systems).

Study Essentials

Know the difference between need-to-know and the least privilege principle. Need-to-know and the least privilege principle are two standard IT security principles implemented in secure networks. They limit access to data and systems so that users and other subjects can access only what they require. This limited access helps prevent security incidents and helps limit the scope of incidents when they occur. When these principles are not followed, security incidents result in far greater damage to an organization.

Understand segregation of duties and job rotation. Segregation of duties (SoD) is a basic security principle that ensures that no single person can control all critical functions or system elements. With job rotation, employees are rotated into different jobs, or tasks are assigned to different employees. Collusion is an agreement among multiple persons to perform some unauthorized or illegal actions. Implementing these policies helps prevent fraud by limiting actions individuals can do without colluding with others.

Know about monitoring privileged operations. Privileged entities are trusted, but they can abuse their privileges. Because of this, it's essential to monitor all assignment of privileges and the use of privileged operations. The goal is to ensure that trusted employees do not abuse the special privileges they are granted. Monitoring these operations can also detect many attacks because attackers commonly use special privileges during an attack. Advanced privileged account management practices can limit the time users have advanced privileges.

Understand service-level agreements. Organizations use service-level agreements (SLAs) with outside entities such as vendors. They stipulate performance expectations such as maximum downtimes and often include penalties if the vendor doesn't meet expectations.

Describe personnel safety and security concerns. Duress systems allow guards to raise alarms in response to emergencies, and emergency management plans help the organization respond to disasters. When employees travel, employees need to be aware of the risks, especially if they travel to different counties. Safety training and awareness programs ensure employees know about these risks and ways to mitigate them.

Understand secure provisioning concepts. Secure provisioning of resources includes ensuring that resources are deployed in a secure manner and are maintained in a secure manner throughout their life cycles. Asset management tracks tangible assets (hardware and software) and intangible assets (such as patents, trademarks, the company's goodwill, and copyrights).

Know how to manage and protect media. Media management techniques track media used to hold sensitive data. Media is protected throughout its lifetime and destroyed when it's no longer needed.

Know the difference between SaaS, PaaS, and IaaS. Software as a service (SaaS) models provide fully functional applications typically accessible via a web browser. Platform as a service (PaaS) models provide consumers with a computing platform, including hardware, operating systems, and a runtime environment. Infrastructure as a service (IaaS) models provide basic computing resources such as servers, storage, and networking resources.

Know about serverless architecture. Serverless architecture is a cloud computing concept where code is managed by the customer, and the platform (i.e., supporting hardware and software) or server is managed by the cloud service provider (CSP). There is always a physical server running the code, but this execution model allows the software designer/architect/programmer/developer to focus on the logic of their code and not have to be concerned about the parameters or limitations of a specific server. This is also known as function as a service (FaaS).

Recognize security issues with managed services in the cloud. Managed services in the cloud include any resources stored in or accessed via the cloud. Storing data in the cloud increases the risk, so additional steps may be necessary to protect the data, depending on its value. When leasing cloud-based services, you must understand who is responsible for maintenance and security. The cloud service provider provides the least amount of maintenance and security in the IaaS model.

Explain configuration and change control management. Many outages and incidents can be prevented with effective configuration and change management programs. Configuration management (CM) ensures that systems are configured similarly and the configurations of systems are known and documented. Baselining ensures that systems are deployed with a common baseline or starting point, and imaging is a common baselining method. Change management helps reduce outages or weakened security from unauthorized changes. A CM process requires changes to be requested, reviewed, approved, tested, scheduled and implemented, and documented. Versioning uses a labeling or numbering system to track changes in updated versions of software.

Understand patch management. Patch management ensures that systems are kept up-to-date with current patches. You should know that an effective patch management program will evaluate, test, approve, and deploy patches. Additionally, be aware that system audits verify the deployment of approved patches to systems. Patch management is often intertwined with change and configuration management to ensure that documentation reflects the changes. When an organization does not have an effective patch management program, it will often experience outages and incidents from known issues that could have been prevented.

Explain vulnerability management. Vulnerability management includes routine vulnerability scans and periodic vulnerability assessments. Vulnerability scanners can detect known security vulnerabilities and weaknesses such as the absence of patches or weak passwords. They generate reports that indicate the technical vulnerabilities of a system and are an effective check for a patch management program. Vulnerability assessments extend beyond just technical scans and can include reviews and audits to detect vulnerabilities.

Written Lab

1. Define the difference between need-to-know and the least privilege principle.
2. Describe the purpose of monitoring the assignment and usage of special privileges.
3. List the three primary cloud-based service models and identify the level of maintenance provided by the cloud service provider in each of the models.
4. Explain how change management processes help prevent outages.

Review Questions

1. Which security principle involves the knowledge and possession of sensitive material as an aspect of one's occupation?

   A. Principle of least privilege

   B. Segregation of duties

   C. Need-to-know

   D. As-needed basis