Chapter 11
Implementing Policies to Mitigate Risks

CompTIA Security+ objectives covered in this chapter:

2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

- Data sanitization tools

2.3 Given a scenario, troubleshoot common security issues.

- Personnel issues (Policy violation, Personal email)

4.4 Given a scenario, differentiate common account management practices.

- General Concepts (Onboarding/offboarding)

5.1 Explain the importance of policies, plans and procedures related to organizational security.

- Standard operating procedure, Agreement types (BPA, SLA, ISA, MOU/MOA), Personnel management (Mandatory vacations, Job rotation, Separation of duties, Clean desk, Background checks, Exit interviews, Role-based awareness training [Data owner, System administrator, System owner, User, Privileged user, Executive user], NDA, Onboarding, Continuing education, Acceptable use policy/rules of behavior, Adverse actions), General security policies (Social media networks/applications, Personal email)

5.4 Given a scenario, follow incident response procedures.

- Incident response plan (Documented incident types/category definitions, Roles and responsibilities, Reporting requirements/escalation, Cyber-incident response teams, Exercise), Incident response process (Preparation, Identification, Containment, Eradication, Recovery, Lessons learned)

5.5 Summarize basic concepts of forensics.

- Order of volatility, Chain of custody, Legal hold, Data

acquisition (Capture system image, Network traffic and logs, Capture video, Record time offset, Take hashes, Screenshots, Witness interviews), Preservation, Recovery, Strategic intelligence/counterintelligence gathering (Active logging), Track man-hours

5.8 Given a scenario, carry out data security and privacy practices.

- Data destruction and media sanitization (Burning, Shredding, Pulping, Pulverizing, Degaussing, Purging, Wiping), Data sensitivity labeling and handling (Confidential, Private, Public, Proprietary, PII, PHI), Data roles (Owner, Steward/custodian, Privacy officer), Data retention, Legal and compliance

**

Organizations often develop written security policies. These provide guiding principles to the professionals who implement security throughout the organization. These policies include personnel management policies and data protection policies. Combined with training for personnel to raise overall security awareness, they help mitigate risk and reduce security incidents. However, security incidents still occur, and incident response policies provide the direction on how to handle them.

Exploring Security Policies

Security policies are written documents that lay out a security plan within a company. They are one of many administrative controls used to reduce and manage risk. When created early enough, they help ensure that personnel consider and implement security throughout the life cycle of various systems in the company. When the policies and procedures are enforced, they help prevent incidents, data loss, and theft.

Policies include brief, high-level statements that identify goals based on an organization's overall beliefs and principles. After creating the policy, personnel within the organization create plans and procedures to support the policies. Although the policies are often high-level statements, the plans and procedures provide details on policy implementation.

As an example, organizations often create ***standard operating procedures (SOPs)*** to support security policies. These typically include step-

by-step instructions employees can use to perform common tasks or routine operations. Security controls such as those covered in Chapter 1, “Mastering Security Basics,” enforce the requirements of a security policy. For example, a security policy may state that internal users must not use peer-to-peer (P2P) applications. A firewall with appropriate rules to block these applications provides a technical implementation of this policy. Similarly, administrators can use port-scanning tools to detect applications running on internal systems that are violating the security policy.

A security policy can be a single large document or divided into several smaller documents, depending on the needs of the company. The following sections identify many of the common elements of a security policy.

Personnel Management Policies

Companies frequently develop policies to specifically define and clarify issues related to personnel management. This includes personnel behavior, expectations, and possible consequences. Personnel learn these policies when they are hired and as changes occur. Some of the policies directly related to personnel are acceptable use, mandatory vacations, separation of duties, job rotation, and clean desk policies. The following sections cover these and other personnel policies in more depth.

Remember this

Written security policies are administrative controls that identify a security plan. Personnel create plans and procedures to implement security controls and enforce the security policies.

Acceptable Use Policy

An ***acceptable use policy (AUP)*** defines proper system usage or the rules of behavior for employees when using information technology (IT) systems. It often describes the purpose of computer systems and networks, how users can access them, and the responsibilities of users when they access the systems.

Many organizations monitor user activities, such as what web sites they visit and what data they send out via email. For example, a proxy server typically logs all web sites that a user visits. The AUP may include statements informing users that systems are in place monitoring their activities.

In some cases, the AUP might include privacy statements informing users what computer activities they can consider private. Many users have an expectation of privacy when using an organization's computer systems and networks that isn't justified. The privacy policy statement helps to clarify the organization's stance.

The AUP often includes definitions and examples of unacceptable use. For example, it might prohibit employees from using company resources to access P2P sites or social media sites.

It's common for organizations to require users to read and sign a document indicating they understand the acceptable use policy when they're hired and in conjunction with annual security training. Other methods, such as logon banners or periodic emails, help reinforce an acceptable use policy.

Mandatory Vacations

Mandatory vacation policies help detect when employees are involved in malicious activity, such as fraud or embezzlement. As an example, employees in positions of fiscal trust, such as stock traders or bank employees, are often required to take an annual vacation of at least five consecutive workdays.

For embezzlement actions of any substantial size to succeed, an employee would need to be constantly present in order to manipulate records and respond to different inquiries. On the other hand, if an employee is forced to be absent for at least five consecutive workdays, someone else would be required to answer any queries during the employee's absence. This increases the likelihood of discovering illegal activities by employees. It also acts as an effective deterrent.

Mandatory vacations aren't limited to only financial institutions, though. Many organizations require similar policies for administrators. For example, an administrator might be the only person required to perform sensitive activities such as reviewing certain logs. A malicious administrator can overlook or cover up certain activities revealed in the logs. However, a mandatory vacation policy would require someone else to perform these activities, which increases the chance of discovery.

Of course, mandatory vacations by themselves won't prevent fraud. Most companies will implement the principle of defense in depth by using multiple layers of protection. Additional policies may include separation of duties and job rotation to provide as much protection as possible.

Remember this

Mandatory vacation policies require employees to take time away from their job. These policies help to deter fraud and discover malicious activities while the employee is away.

Separation of Duties

Separation of duties is a principle that prevents any single person or entity from being able to complete all the functions of a critical or sensitive process. It's designed to prevent fraud, theft, and errors.

Accounting provides a classic example. It's common to divide Accounting departments into two divisions: Accounts Receivable and Accounts Payable. Personnel in the Accounts Receivable division review and validate bills. They then send the validated bills to the personnel in the Accounts Payable division, who pay the bills. Similarly, this policy would ensure personnel are not authorized to print and sign checks. Instead, a separation of duties policy separates these two functions to reduce the possibility of fraud.

If Homer were the only person doing all these functions, it would be possible for him to create and approve a bill from Homer's Most Excellent Retirement Account. After approving the bill, Homer would then pay it. If Homer doesn't go to jail, he may indeed retire early at the expense of the financial health of the company.

Separation of duties policies also apply to IT personnel. For example, it's common to separate application development tasks from application deployment tasks. In other words, developers create and modify applications and then pass the compiled code to administrators. Administrators then deploy the code to live production systems. Without this policy in place, developers might be able make quick, untested changes to code, resulting in unintended outages. This provides a high level of version control and prevents potential issues created through uncontrolled changes.

As another example, a group of IT administrators may be assigned responsibility for maintaining a group of database servers. However, they would not be granted access to security logs on these servers. Instead, security administrators regularly review these logs, but these security administrators will not have access to data within the databases.

Imagine that Bart has been working as an IT administrator but recently

changed jobs and is now working as a security administrator. What should happen? Based on separation of duties, Bart should now have access to the security logs, but his access to the data within the databases should be revoked. If his permissions to the data are not revoked, he will have access to more than he needs, violating the principle of least privilege. A user rights and permissions review often discovers these types of issues.

Remember this

Separation of duties prevents any single person or entity from controlling all the functions of a critical or sensitive process by dividing the tasks between employees. This helps prevent potential fraud, such as if a single person prints and signs checks.

Job Rotation

Job rotation is a concept that has employees rotate through different jobs to learn the processes and procedures in each job. From a security perspective, job rotation helps to prevent or expose dangerous shortcuts or even fraudulent activity. Employees might rotate through jobs temporarily or permanently.

For example, your company could have an Accounting department. As mentioned in the "Separation of Duties" section, you would separate accounting into two divisions—Accounts Receivable and Accounts Payable. Additionally, you could rotate personnel in and out of jobs in the two divisions. This would ensure more oversight over past transactions and help ensure that employees are following rules and policies.

In contrast, imagine a single person always performs the same function without any expectation of oversight. This increases the temptation to go outside the bounds of established policies.

Job rotation policies work well together with separation of duties policies. A separation of duties policy helps prevent a single person from controlling too much. However, if an organization only used a separation of duties policy, it is possible for two people to collude in a scheme to defraud the company. If a job rotation policy is also used, these two people will not be able to continue the fraudulent activity indefinitely.

Job rotation policies also apply to IT personnel. For example, the policy can require administrators to swap roles on a regular basis, such as annually

or quarterly. This prevents any single administrator from having too much control over a system or network.

Remember this

Job rotation policies require employees to change roles on a regular basis. Employees might change roles temporarily, such as for three to four weeks, or permanently. This helps ensure that employees cannot continue with fraudulent activity indefinitely.

Clean Desk Policy

A ***clean desk policy*** directs users to keep their areas organized and free of papers. The primary security goal is to reduce threats of security incidents by ensuring the protection of sensitive data. More specifically, it helps prevent the possibility of data theft or inadvertent disclosure of information.

Imagine an attacker goes into a bank and meets a loan officer. The loan officer has stacks of paper on his desk, including loan applications from various customers. If the loan officer steps out, the attacker can easily grab some of the documents, or simply take pictures of the documents with a mobile phone.

Beyond security, organizations want to present a positive image to customers and clients.
Employees with cluttered desks with piles of paper can easily turn off customers.

However, a clean desk policy doesn't just apply to employees who meet and greet customers. It also applies to employees who don't interact with customers. Just as dumpster divers can sort through trash to gain valuable information, anyone can sort through papers on a desk to learn information. It's best to secure all papers to keep them away from prying eyes. Some items left on a desk that can present risks include:

- Keys
- Cell phones
- Access cards
- Sensitive papers
- Logged-on computer
- Printouts left in printer
- Passwords on Post-it notes
- File cabinets left open or unlocked
- Personal items such as mail with Personally Identifiable

Information (PII)

Some people want to take a clean desk policy a step further by scrubbing and sanitizing desks with antibacterial cleaners and disinfectants on a daily basis. They are free to do so, but that isn't part of a security-related clean desk policy.

Remember this

A clean desk policy requires users to organize their areas to reduce the risk of possible data theft. It reminds users to secure sensitive data and may include a statement about not writing down passwords.

I'll Go to Jail Before I Give You the Passwords! (Sidebar)

The city of San Francisco had an extreme example of the dangers of a single person with too much explicit knowledge or power. A network administrator with one of Cisco's highest certifications—Cisco Certified Internetwork Expert (CCIE)—made changes to the city's network, changing passwords so that only he knew them and ensuring that he was the only person with administrative access.

It could be that he was taking these actions to protect the network that he considered his "baby." He was the only CCIE, and it's possible he thought others did not have the necessary knowledge to maintain the network adequately. Over the years, fewer and fewer people had access to what he was doing, and his knowledge became more and more proprietary. Instead of being malicious in nature, he might have simply been protective, even if overly protective.

At some point, his supervisor recognized that all the proverbial information eggs were in the basket of this lone CCIE. It was just too risky. What if a bus, or one of San Francisco's famous trolleys, hit him? What would the organization do? His supervisor asked him for some passwords

and he refused, even when faced with arrest. Later, he gave law enforcement personnel passwords that didn't work.

Law enforcement personnel charged him with four counts of tampering with a computer network and courts kept him in custody with a $5 million bail. Ultimately, a court convicted him of one felony count and sentenced him to four years in prison. This is a far fall from his reported annual salary of $127,735.

The city of San Francisco had to bring in experts from Cisco and the city reported costs of $900,000 to regain control of their network. Following his conviction, the court also ordered the administrator to pay $1.5 million in restitution.

What's the lesson here? Internal security controls, such as creating and enforcing policies related to rotation of duties, separation of duties, and cross-training, might have been able to avoid this situation completely. If this CCIE truly did have good intentions toward what he perceived as his network, these internal controls might have prevented him from going over the line into overprotection and looking at the world through the bars of a jail cell.

Background Check

It's common for organizations to perform background checks on potential employees and even after employees are hired. A ***background check*** checks into a potential employee's history with the intention of discovering anything about the person that might make him a less-than- ideal fit for a job.

A background check will vary depending on job responsibilities and the sensitivity of data that person can access. For example, a background check for an associate at Walmart will be significantly less than a background check for a government employee who will handle Top Secret Sensitive Compartmented Information.

However, background checks will typically include a query to law enforcement agencies to identify a person's criminal history. In some cases, this is only to determine if the person is a felon. In other cases, it checks for

all potential criminal activity, including a review of a person's driving records.

Many organizations check a person's financial history by obtaining a credit report. For example, someone applying for a job in an Accounting department might not be a good fit if his credit score is 350 and he has a string of unpaid loans.

It is also common for employers to check a person's online activity. This includes social media sites, such as Facebook, LinkedIn, and Twitter. Some people say and do things online that they would rarely do in public. One reason is a phenomenon known as the online disinhibition effect. Just as a beer or glass of wine releases inhibitions in many people, individuals are often less inhibited when posting comments online. And what they post often reflects their true feelings and beliefs. Consider a person who frequently posts hateful comments about others. A potential employer might think that this person is unlikely to work cohesively in a team environment and hire someone else.

Note that some background checks require the written permission from the potential employee. For example, the Fair Credit Reporting Act (FCRA) requires organizations to obtain written permission before obtaining a credit report on a job applicant or employee. However, other background checks don't require permission. For example, anyone can look at an individual's social media profile.

NDA

A non-disclosure agreement (***NDA***) is used between two entities to ensure that proprietary data is not disclosed to unauthorized entities. For example, imagine BizzFad wants to collaborate with Costington's on a project. BizzFad management realizes they need to share proprietary data with Costington's personnel, but they want to ensure that distribution of the data is limited. The NDA is a legal document that BizzFad can use to hold Costington's legally responsible if the proprietary data is shared.

Similarly, many organizations use an NDA to prohibit employees from sharing proprietary data either while they are employed, or after they leave the organization. It's common to remind employees of an existing NDA during an exit interview.

Exit Interview

An ***exit interview*** is conducted with departing employees just before they leave an organization. Note that an exit interview isn't only conducted when employees are fired from their job. They are also done when employees leave voluntarily. The overall purpose is for the employer to gain information from the departing employee. Some common questions asked during an exit interview are:

- What did you like most (and/or least) about your job here?
- Do you think you had adequate training to do your job here?
- Can you tell me what prompted you to leave your current position?
- Can you describe the working relationship you had with your supervisor(s)?
- What skills and qualification does your replacement need to excel in this position?

Exit interviews are commonly conducted by an employee in the Human Resources (HR) department. In addition to seeking feedback from the employee, departing employees are sometimes required to sign paperwork, such as a reminder about a previously signed NDA. The NDA prevents the employee from sharing proprietary information with personnel outside the organization.

From a security perspective, it's also important to ensure other things occur during or before the exit interview. For example, the user's account should be disabled (or deleted depending on company policy). Ideally, this should occur during the interview. One way organizations do this is by informing the IT department of the time of the scheduled interview a day before. An administrator then disables the account after the interview starts. The key is that a departing employee should not have access to computing and network resources after the interview.

It's also important to collect any equipment (such as smartphones, tablets, or laptops), security badges, or proximity cards the organization issued to the employee. This is more than just a cost issue. Equipment very likely has proprietary data on it and the company needs to take steps to protect the data. Additionally, smart cards and proximity cards can allow individuals access to protected areas.

Remember this

Background checks investigate the history of an individual prior to employment and, sometimes, during employment. They may

include criminal checks, credit checks, and an individual's online activity. An exit interview is conducted when an individual departs an organization. User accounts are often disabled or deleted during the exit interview and everything issued to the employee is collected.

Onboarding

Onboarding is the process of granting individuals access to an organization's computing resources after being hired. This includes providing the employee with a user account and granting access to appropriate resources. One of the key considerations during the onboarding process is to follow the principle of least privilege. Grant the new employees access to what they need for their job, but no more.

Offboarding is the process of removing their access. When employees leave the company, it's important to revoke their access. This is often done during the exit interview.

Policy Violations and Adverse Actions

What do you do if an employee doesn't follow the security policy? What adverse actions should a supervisor take? Obviously, that depends on the severity of the policy violation.

Imagine that an employee sends out an email to everyone in the organization inviting them to his church. The supervisor might decide to verbally counsel the employee and make it clear that sending out personal emails like this is unacceptable. Based on how well the conversation goes, the supervisor might choose to document this as written counseling and place the warning in the employee's HR folder.

Some incidents require more severe responses. Imagine that an employee begins a cyberbullying campaign against another employee. He has been sending her hateful emails and posting hateful messages on social media pages. In most organizations, this bully will be looking for employment elsewhere once his activity is discovered.

Although it's possible to document specific adverse actions within a security policy, this is rarely recommended. Actual policy violations aren't always the same and if the policy requires a specific action in response to a policy violation, it doesn't always allow supervisors or managers to respond appropriately to a violation.

Other General Security Policies

From a more general perspective, an organization may implement personnel management policies that affect other areas of an employee's life. Some examples include behavior on social media networks and the use of email.

As a simple example, employees of a company should not post adverse comments about other employees or customers. Employees who engage in cyberbullying against fellow employees are typically fired. Similarly, employees who post derogatory comments about customers quickly find themselves looking for other employment.

You might think that people would know that what they post on the Internet can be seen by anyone, including their employer. However, if you do a quick Google search on "employee fired after Facebook post" or "employee fired after tweet," you'll find many examples where people ignored the possibility that their words would be seen by their employer.

Another consideration is personal email. Some organizations allow employees to use the organization's IT infrastructure to send and receive personal email, while other organizations forbid it. The key here is ensuring that employees understand the policy.

Social Media Networks and Applications

Millions of people interact with each other using social media networks and applications, such as Facebook and Twitter. Facebook allows people to share their lives with friends, family, and others. Twitter allows people to tweet about events as they are happening. From a social perspective, these technologies allow people to share information about themselves with others. A user posts a comment and a wide group of people instantly see it.

However, from a security perspective, they present some significant risks, especially related to inadvertent information disclosure. Attackers can use these sites to gain information about individuals and then use that information in an attack. Organizations typically either train users about the risks or block access to the social media sites to avoid the risks.

Users often post personal information, such as birth dates, their favorite colors or books, the high school they graduated from, graduation dates, and much more. Some sites use this personal information to validate users when they forget or need to change their password. Imagine Maggie needs to reset

her password for a bank account. The web site may challenge her to enter her birth date, favorite book, and graduation date for validation. This is also known as a cognitive password and, theoretically, only Maggie knows this information. However, if Maggie posts all this information on Facebook, an attacker can use it to change the password on the bank account.

As an example, David Kernell used Yahoo!'s cognitive password account recovery process to change former Alaska Governor Sarah Palin's password for her email account. At the time, Yahoo! asked questions such as her high school and birth date and Kernell obtained all the information from online searches. Of course, it didn't turn out well for him. A jury convicted him of a felony and he served more than a year in prison.

In some cases, attackers have used personal information from social networking sites to launch scams. For example, attackers first identify the name of a friend or relative using the social networking site. The attackers then impersonate the friend or relative in an email, claiming to have been robbed and stuck in a foreign country. Attackers end the email with a plea for help asking the victim to send money via wire transfer.

It's also worth considering physical security. While vacationing in Paris, Kim Kardashian West was regularly posting her status and location on social media. She also stressed that she didn't wear fake jewelry. Thieves robbed her at gunpoint in her Paris hotel room. They bound and gagged her and took one of her rings (that is worth an estimated $4.9 million) and a jewelry box (with jewelry worth an estimated $5.6 million). After being caught and arrested, one of the thieves later admitted that it was relatively easy to track her just by watching her online activity.

Remember this

Social media sites allow people to share personal comments with a wide group of people. However, improper use of social networking sites can result in inadvertent information disclosure. Attackers can also use information available on these sites to launch attacks against users or in a cognitive password attack to change a user's password. Training helps users understand the risks.

Banner Ads and Malvertisements

Attackers have been delivering malware through malicious banner ads

for several years now. These look like regular ads, but they contain malicious code. Many of these are Flash applets with malicious code embedded in them, but others just use code to redirect users to another server, such as one with a drive-by download waiting for anyone who clicks.

Although these malvertisements have been on many social media sites, they've also appeared on mainstream sites. For example, attackers installed a malvertisement on the *New York Times* web site where it ran for about 24 hours before webmasters discovered and disabled it.

Similarly, malvertising has appeared on the Yahoo! web site. Users who clicked on some Yahoo! ads were taken to sites hosting fake antivirus software. These sites included pop- ups indicating that users' systems were infected with malware and encouraging the users to download and install it. Users who took the bait installed malware onto their systems. Some of these ads sent users to sites in Eastern Europe that were hosting CryptoWall, according to research by Blue Coat Systems, Inc. CryptoWall is a malicious form of ransomware that encrypts user files and demands payment to decrypt them.

Attackers have used two primary methods to get these malvertisements installed on legitimate web sites. One method is to attack a web site and insert ads onto that web site. The second method is to buy ads. They often represent an ad agency pretending to represent legitimate clients. For example, one attacker convinced Gawker Media to run a series of Suzuki advertisements, which were actually malvertisements. Similarly, it's unlikely that Yahoo! was aware that it was hosting malvertising, but instead, these ads likely appeared as a result of attacks or by being tricked.

Social Networking and P2P

Peer-to-peer (P2P or file sharing) applications allow users to share files, such as music, video, and data, over the Internet. Instead of a single server providing the data to end users, all computers in the P2P network are peers, and any computer can act as a server to other clients.

The first widely used P2P network was Napster, an online music-sharing service that operated between 1999 and 2001. Users copied and distributed MP3 music files among each other, and these were often pirated music files. The files were stored on each user's system, and as long as the system was accessible on the Internet, other users could access and download the files. A court order shut down Napster due to copyright issues, but it later

reopened as an online music store. Other P2P software and P2P networks continue to appear and evolve.

Organizations usually restrict the use of P2P applications in networks, but this isn't because of piracy issues. One reason is because the P2P applications can consume network bandwidth, slowing down other systems on the network. Worse, a significant risk with P2P applications is data leakage. Users are often unaware of what data they are sharing. Another risk is that users are often unaware of what data the application downloads and stores on their systems, causing them to host inappropriate data. Two examples help illustrate these data leakage risks.

Information concentrators search P2P networks for information of interest and collect it. Investigators once discovered an information concentrator in Iran with over 200 documents containing classified and secret U.S. government data. This included classified information about Marine One, the helicopter used by the president. Although the information about Marine One made the headlines, the attackers had much more information. For example, this concentrator included Iraq status reports and lists of soldiers with privacy data.

How did this happen? Investigations revealed that a defense contractor installed a P2P application on a computer. The computer had access to this data, and the P2P application shared it.

The media latched onto the news about Marine One, so this story was widely published. However, it's widely believed that much more data is being mined via P2P networks. Most end users don't have classified data on their systems, but they do have PII, such as banking information or tax data. When an attacker retrieves data on a user's system and empties a bank account, it might be a catastrophe to the user, but it isn't news.

Organizations can restrict access to P2P networks by blocking access in firewalls. Additionally, port scanners can scan open ports of remote systems to identify P2P software. Organizations often include these checks when running a port scanner as part of a vulnerability scan.

Remember this

Data leakage occurs when users install P2P software and unintentionally share files. Organizations often block P2P software at the firewall.

Agreement Types

Organizations often utilize different types of agreements to help identify various responsibilities. Many are used when working with other organizations, but they can often be used when working with different departments within the same organization. These include:

- **Interconnection security agreement (ISA).** An ***ISA*** specifies technical and security requirements for planning, establishing, maintaining, and disconnecting a secure connection between two or more entities. For example, it may stipulate certain types of encryption for all data-in-transit. NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," includes more in-depth information on ISAs.
- **Service level agreement (SLA).** An ***SLA*** is an agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels. Organizations use SLAs when contracting services from service providers such as Internet Service Providers (ISPs). Many SLAs include a monetary penalty if the vendor is unable to meet the agreed-upon expectations.
- **Memorandum of understanding (MOU) or memorandum of agreement (MOA).** An ***MOU/MOA*** expresses an understanding between two or more parties indicating their intention to work together toward a common goal. An MOU/MOA is often used to support an ISA by defining the purpose of the ISA and the responsibilities of both parties. However, it doesn't include any technical details. You can also compare an MOU/ MOA with an SLA because it defines the responsibilities of each of the parties. However, it is less formal than an SLA and does not include monetary penalties. Additionally, it doesn't have strict guidelines in place to protect sensitive data.
- **Business partners agreement (BPA).** A ***BPA*** is a written agreement that details the relationship between business partners, including their obligations toward the partnership. It typically identifies the shares of profits or losses each partner will take, their responsibilities to each other, and what to do if a partner chooses to leave the partnership. One of the primary benefits of a BPA is that it

can help settle conflicts when they arise.

Remember this

A memorandum of understanding or memorandum of agreement (MOU/MOA) defines responsibilities of each party, but it is not as strict as a service level agreement (SLA) or interconnection security agreement (ISA). If the parties will be handling sensitive data, they should include an ISA to ensure strict guidelines are in place to protect the data while in transit. An MOU/MOA often supports an ISA.

Protecting Data

Every company has secrets. Keeping these secrets can often make the difference between success and failure. A company can have valuable research and development data, customer databases, proprietary information on products, and much more. If the company cannot keep private and proprietary data secret, it can directly affect its bottom line.

Data policies assist in the protection of data and help prevent data leakage. This section covers many of the different elements that may be contained in a data policy.

Information Classification

As a best practice, organizations take the time to identify, classify, and label data they use. Data classifications ensure that users understand the value of data, and the classifications help protect sensitive data. Classifications can apply to hard data (printouts) and soft data (files).

As an example, the U.S. government uses classifications such as Top Secret, Secret, Confidential, and Unclassified to identify the sensitivity of data. Private companies often use terms such as Proprietary, Private, Confidential, or Public. Note that while the U.S. government has published standards for these classifications, there isn’t a published standard that all private companies use.

For comparison, the following statements identify the typical meaning of these public classifications:

- ***Public data*** is available to anyone. It might be in brochures, press releases, or on web sites.
- ***Confidential data*** is information that an organization intends to keep secret among a certain group of people. For example, most companies consider salary data confidential. Personnel within the Accounting department and some executives have access to salary data, but they keep it secret among themselves. Many companies have specific policies in place telling people that they shouldn't even tell anyone else their salary amount.
- A proprietor is an owner and ***proprietary data*** is data that is related to ownership. Common examples are information related to patents or trade secrets.

- ***Private data*** is information about an individual that should remain private. Two classic examples within IT security are Personally Identifiable Information (PII) and Personal Health Information (PHI). Both PII and PHI are covered in more depth later in this chapter.

The labels and classifications an organization uses are not as important as the fact that they use labels and classifications. Organizations take time to analyze their data, classify it, and provide training to users to ensure the users recognize the value of the data. They also include these classifications within a data policy.

Data Sensitivity Labeling and Handling

Data ***labeling*** ensures that users know what data they are handling and processing. For example, if an organization classified data as confidential, private, proprietary, and public, it would also use labeling to identify the data. These labels can be printed labels for media such as backup tapes. It's also possible to label files using metadata, such as file properties, headers, footers, and watermarks.

Consider a company that spends millions of dollars on research and development (R&D) trying to develop or improve products. The company values this proprietary data much more than data publicly available on its web site, and needs to protect it. However, if employees have access to the R&D

data and it's not classified or labeled, they might not realize its value and might not protect it.

For example, a web content author might write an article for the company's web site touting its achievements. If the R&D data isn't classified and labeled, the author might include some of this R&D data in the article, inadvertently giving the company's competitors free access to proprietary data. Although the R&D employees will easily recognize the data's value, it's not safe to assume that everyone does. In contrast, if the data is labeled, anyone would recognize its value and take appropriate steps to protect it.

Chapter 9, "Implementing Controls to Protect Assets," presents information on backups. As a reminder, it's important to protect backups with the same level of protection as the original data. Labels on backup media help personnel easily identify the value of the data on the backups.

Remember this

Public data is available to anyone. Confidential data information is kept secret among a certain group of people. Proprietary data is data related to ownership, such as patents or trade secrets. Private data is information about individuals that should remain private. Data classifications and data labeling help ensure personnel apply the proper security controls to protect information.

Data Destruction and Media Sanitization

When computers reach the end of their life cycles, organizations donate them, recycle them, or sometimes just throw them away. From a security perspective, you need to ensure that the computers don't include any data that might be useful to people outside your organization or damaging to your organization if unauthorized people receive it.

It's common for organizations to have a checklist to ensure that personnel ***sanitize*** a system prior to disposing of it. The goal is to ensure that personnel remove all usable data from the system.

Hard drives represent the greatest risk because they hold the most information, so it's important to take additional steps when decommissioning old hard drives. Simply deleting a file on a drive doesn't actually delete it. Instead, it marks the file for deletion and makes the space available for use. Similarly, formatting a disk drive doesn't erase the data. There are many

recovery applications available to recover deleted data, file remnants, and data from formatted drives.

Data destruction isn't limited to only hard drives. Organizations often have a policy related to paper containing any type of sensitive data. Shredding or incinerating these papers prevents them from falling into the wrong hands. If personnel just throw this paper away, dumpster divers can sift through the trash and gain valuable information. An organization also takes steps to destroy other types of data, such as backup tapes, and other types of devices, such as removable media.

Some common methods used to destroy data and sanitize media are:

- **Purging.** ***Purging*** is a general sanitization term indicating that all sensitive data has been removed from a device.
- **File shredding.** Some applications remove all remnants of a file using a ***shredding*** technique. They do so by repeatedly overwriting the space where the file is located with 1s and 0s.
- **Wiping.** ***Wiping*** refers to the process of completely removing all remnants of data on a disk. A disk wiping tool might use a bit-level overwrite process that writes different patterns of 1s and 0s multiple times and ensures that the data on the disk is unreadable.
- **Erasing and overwriting.** Solid-state drives (SSDs) require a special process for sanitization. Because they use flash memory instead of magnetic storage platters, traditional drive wiping tools are not effective. Some organizations require personnel to physically destroy SSDs as the only acceptable method of sanitization.
- **Burning.** Many organizations burn materials in an incinerator. Obviously, this can be done with printed materials, but isn't as effective with all materials.
- **Paper shredding.** You can physically shred papers by passing them through a shredder. When doing so, it's best to use a cross-cut shredder that cuts the paper into fine particles. Large physical shredders can even destroy other hardware, such as disk drive platters removed from a disk drive.
- **Pulping.** ***Pulping*** is an additional step taken after shredding paper. It reduces the shredded paper to mash or puree.
- **Degaussing.** A degausser is a very powerful electronic magnet. Passing a disk through a ***degaussing*** field renders the data on tape and magnetic disk drives unreadable.

- **Pulverizing.** ***Pulverizing*** is the process of physically destroying media to sanitize it, such as with a sledge hammer (and safety goggles). Optical media is often pulverized because it is immune to degaussing methods and many shredders can't handle the size of optical media. It's also possible to remove disk platters from disk drives and physically destroy them.

It's also worth mentioning that hard drives and other media can be in devices besides just computers. For example, many copy machines include disk drives, and they can store files of anything that employees recently copied or printed. If personnel don't sanitize the drives before disposing of these devices, it can also result in a loss of confidentiality.

Cluster Tip Wiping (Sidebar)

Cluster tip wiping is a special process that removes the random data stored at the end of a file. It is useful when you want to keep a file, but remove the random data.

Files are stored in clusters and cluster sizes are typically about 4 KB. Files use as many clusters as they need, but the last cluster has some unused space that the operating system pads with random data.

As an example, imagine you are saving a 6 KB file. It will use two 4 KB clusters and the last 2 KB in the second cluster isn't used to store information for your file. However, this last 2 KB isn't empty. Instead, it contains random data pulled from memory. If someone was recently working with proprietary data, the last 2 KB might hold some of that data. Cluster tip wiping tools can sanitize files stored on a system, and eliminate this issue.

Data Retention Policies

A ***data retention policy*** identifies how long data is retained, and sometimes specifies where it is stored. This reduces the amount of resources, such as hard drive space or backup tapes, required to retain the data. Retention policies also help reduce legal liabilities. For example, imagine if a retention policy states that the company will only keep email for one year. A court order requiring all email from the company can only expect to receive email from the last year.

On the other hand, if the organization doesn't have a retention policy, it might need to provide email from the past 10 years or longer in response to a court order. This can require an extensive amount of work by administrators to recover archives or search for specific emails. Additionally, investigations can uncover other embarrassing evidence from previous years. The retention policy helps avoid these problems.

Some laws mandate the retention of data for specific time frames, such as three years or longer. For example, laws mandate the retention of all White House emails indefinitely. If a law applies to an organization, the retention policy reflects the same requirements.

PII and PHI

Personally Identifiable Information (***PII***) is personal information that can be used to personally identify an individual. Personal Health Information (***PHI***) is PII that includes health information.

Some examples of PII are:

- Full name
- Birthday and birth place
- Medical and health information
- Street or email address information
- Personal characteristics, such as biometric data
- Any type of identification number, such as a Social Security number (SSN) or driver's license number

In general, you need two or more pieces of information to make it PII. For example, "John Smith" is not PII by itself because it can't be traced back to a specific person. However, when you connect the name with a birth date, an address, medical information, or other data, it is PII.

When attackers gain PII, they often use it for financial gain at the expense of the individual. For example, attackers steal identities, access credit cards, and empty bank accounts. Whenever possible, organizations should minimize the use, collection, and retention of PII. If it's not kept, it can't be compromised. On the other hand, if they collect PII and attackers compromise the data, the company is liable.

The number of security breach incidents resulting in the loss of PII continues to rise. For example, a Veteran's Affairs (VA) employee copied a database onto his laptop that contained PII on over 26 million U.S. veterans. He took the laptop home and a burglar stole it. The VA then went through the

painful and expensive process of notifying all of the people who were vulnerable to identity theft, and the affected individuals spent countless hours scouring their records for identity theft incidents. Even though police later recovered the laptop, the VA paid $20 million to settle a lawsuit in the case.

This is not an isolated incident. The Identity Theft Resource Center tracks data breaches and lists them on their site (*http://www.idtheftcenter.org/*). Their 2015 report reported the number of known U.S. data breaches at 780, exposing more than 177 million records containing PII and/or PHI. Some data breaches were small, affecting only a few hundred people. Others were large such as the attack on Scottrade, accessing more than 4.6 million records. Many times, the companies don't even report how many records were accessed, so the number of data records in the hands of criminals is very likely much higher.

Each of these instances resulted in potential identity theft and the loss of goodwill and public trust of the company. Both customers and employees were negatively impacted, and the companies were forced to spend time and energy discussing the incident, and spend money trying to repair their reputations.

Protecting PII and PHI

Organizations have an obligation to protect PII. There are many laws that mandate the protection of PII, including international laws, federal laws, and local regulations. Organizations often develop policies to identify how they handle, retain, and distribute PII, and these policies help ensure they are complying with relevant regulations. When a company doesn't use a specific PII policy, it usually identifies methods used to protect PII in related data policies.

Many laws require a company to report data losses due to security breaches. If an attack results in the loss of customer PII data, the company is required to report it and notify affected individuals. As an example, Arizona enacted a security breach notification law that requires any company doing business in Arizona to notify customers of security breaches. Most states in the United States have similar laws, and similar international laws exist.

One of the common reasons data seems to fall into the wrong hands is that employees don't understand the risks involved. They might not realize the value of the data on a laptop, or they might casually copy PII data onto a USB flash drive. As mentioned previously, data classification and labeling procedures help employees recognize the data's value and help protect

sensitive data.

Training is also important. One of the goals of security professionals is to reinforce the risks of not protecting PII. When employees understand the risks, they are less likely to risk customer and employee data to identity theft.

Additionally, if employees need to transmit PII over a network, they can ensure it's protected by using encryption. As mentioned previously in this book, encrypting data-in-transit provides strong protection against loss of confidentiality.

Many governments have enacted laws mandating the protection of both PII and PHI. Also, there are many documents that provide guidance on how to protect it. The National Institute of Standards and Technology (NIST) created Special Publication (SP) 800-122 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)." It identifies many specific safeguards that organizations can implement to protect PII along with steps to take in response to a data breach involving PII. You can access all the NIST publications at *http://csrc.nist. gov/publications/PubsSPs.html*.

Remember this

Personally Identifiable Information (PII) includes information such as a full name, birth date, biometric data, and identifying numbers such as a SSN. PHI is PII that includes medical or health information. Organizations have an obligation to protect PII and PHI and often identify procedures for handling and retaining PII in data policies.

Legal and Compliance Issues

Organizations have a responsibility to follow all laws that apply to them, and ensure that they remain in compliance. Within the context of data security and privacy, the following laws are often a key concern:

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA).** HIPAA mandates that organizations protect PHI. This includes any information directly related to the health of an individual that might be held by doctors, hospitals, or any health facility. It also applies to any information held by an organization related to health plans offered to employees. Fines for not complying with the law

have been as high as $4.3 million.

- **Gramm-Leach Bliley Act (GLBA).** This is also known as the Financial Services Modernization Act and includes a Financial Privacy Rule. This rule requires financial institutions to provide consumers with a privacy notice explaining what information they collect and how that information is used.
- **Sarbanes-Oxley Act (SOX).** SOX was passed after several accounting scandals by major corporations, such as Enron and WorldCom. Companies were engaging in accounting fraud to make their financial condition look better than it was and prop up their stock price. For example, Enron's stock value was over $90 in 2000, but executives knew of problems and began selling their stock. As the scandal emerged, the stock crashed to $42 a year later, and $15 in October of 2001. In December 2002, the stock was worthless at six cents a share, effectively wiping out $60 billion in investments. SOX requires that executives within an organization take individual responsibility for the accuracy of financial reports. It also includes specifics related to auditing, and identifies penalties to individuals for noncompliance.
- **General Data Protection Regulation (GDPR).** This European Union (EU) directive supersedes the Data Protection Directive (also known as Directive 95/46/EC). Both mandate the protection of privacy data for individuals within the EU.

While this section outlined four specific laws related to data, there are others. The key is that organizations have a responsibility to know which laws apply to them and remain in compliance with the laws.

Data Roles and Responsibilities

Many people within the organization handle data. However, an organization often assigns specific roles to some people. Each of these roles has specific responsibilities as outlined in the following list:

- **Owner.** The data owner is the individual with overall responsibility for the data. It is often a high-level position such as the chief executive officer (CEO) or a department head. The data owner is responsible for identifying the classification of the data, ensuring the data is labeled to match the classification, and ensuring security

controls are implemented to protect the data.

- **Steward/custodian.** A data steward or data custodian handles the routine tasks to protect data. For example, a data custodian would ensure data is backed up in accordance with a backup policy. The custodian would also ensure that backup tapes are properly labeled to match the classification of the data and stored in a location that provides adequate protection for the classification of the data. Data owners typically delegate tasks to the data custodian.
- **Privacy officer.** A privacy officer is an executive position within an organization. This person is primarily responsible for ensuring that the organization is complying with relevant laws. For example, if the organization handles any PHI, the privacy officer ensures the organization complies with HIPAA. If SOX applies to the organization, the privacy officer ensures that the organization is complying with SOX.

Remember this

Key data roles within an organization are responsible for protecting data. The owner has overall responsibility for the protection of the data. A steward or custodian handles routine tasks to protect data. A privacy officer is an executive responsible for ensuring the organization complies with relevant laws.

Responding to Incidents

Many organizations create ***incident response*** policies to help personnel identify and respond to incidents. A ***security incident*** is an adverse event or series of events that can negatively affect the confidentiality, integrity, or availability of data or systems within the organization, or that has the potential to do so.

Some examples include attacks, release of malware, security policy violations, unauthorized access of data, and inappropriate usage of systems. For example, an attack resulting in a data breach is a security incident. Once the organization identifies a security incident, it will respond based on the incident response policy.

Organizations regularly review and update the policy. Reviews might occur on a routine schedule, such as annually, or in response to an incident

after performing a lessons learned review of the incident.

As an example, in the early days of computers, one hacker broke into a government system and the first thing he saw was a welcome message. He started poking around, but authorities apprehended him. Later, when the judge asked him what he was doing, he replied that when he saw the welcome message, he thought it was inviting him in. The lesson learned here was that a welcome message can prevent an organization from taking legal action against an intruder. Government systems no longer have welcome messages. Instead, they have warning banners stressing that only authorized personnel should be accessing the system. It's common to see similar warning banners when logging on to any system today.

NIST SP 800-61 Revision 2, "Computer Security Incident Handling Guide," provides comprehensive guidance on how to respond to incidents. It is 79 pages so it's obviously more in-depth than this section, but if you want to dig deeper into any of these topics, it's an excellent resource. Use your favorite search engine and search for "NIST SP 800-61."

Remember this

An incident response policy defines a security incident and incident response procedures. Incident response procedures start with preparation to prepare for and prevent incidents. Preparation helps prevent incidents such as malware infections. Personnel review the policy periodically and in response to lessons learned after incidents.

Incident Response Plan

An ***incident response plan (IRP)*** provides more detail than the incident response policy. It provides organizations with a formal, coordinated plan personnel can use when responding to an incident. Some of the common elements included with an incident response plan include:

- **Definitions of incident types.** This section helps employees identify the difference between an event (that might or might not be a security incident) and an actual incident. Some types of incidents include attacks from botnets, malware delivered via email, data breach, and a ransom demand after a criminal encrypts an organization's data. The plan may group these incident types using specific category definitions, such as attacks, malware infections, and

data breaches.

- **Cyber-incident response teams.** A cyber-incident response team is composed of employees with expertise in different areas. Organizations often refer to the team as a ***cyber-incident response team***, a computer incident response team (CIRT), or a security incident response team. Combined, they have the knowledge and skills to respond to an incident. Due to the complex nature of incidents, the team often has extensive training. Training includes concepts, such as how to identify and validate an incident, how to collect evidence, and how to protect the collected evidence.
- **Roles and responsibilities.** Many incident response plans identify specific roles for an incident response team along with their responsibilities. For example, an incident response team might include someone from senior management with enough authority to get things done, a network administrator or engineer with the technical expertise necessary to understand the problems, a security expert who knows how to collect and analyze evidence, and a communication expert to relay information to the public if necessary.
- **Escalation.** After identifying an incident, personnel often need to escalate it. Escalation can require a technician to inform his supervisor that he discovered a malware infection and is resolving it. If critical servers are under attack from a protracted distributed denial- of-service (DDoS) attack, escalation can require all members of the incident response team to get involved in responding to the incident.
- **Reporting requirements.** Depending on the severity of the incident, security personnel might need to notify executives within the company of the incident. Obviously, they wouldn't notify executives of every single incident. However, they would notify executives about serious incidents that have the potential to affect critical operations. If the incident involves a data breach, personnel need to identify the extent of the loss, and determine if outside entities are affected. For example, if attackers successfully attacked a system and collected customer data such as credit information, the organization has a responsibility to notify customers of the data breach as soon as possible. The incident response plan outlines who needs to be notified and when.
- **Exercises.** One method of preparing for incident response is to

perform exercises. These can test the response of all members of the team. For example, a technical exercise can test the administrator's ability to rebuild a server after a simulated attack. Mock interviews or press conferences can test the team's responses to the media. NIST SP 800- 84, "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities," provides much more in-depth information about performing exercises.

Incident Response Process

Incident response includes multiple phases. It starts with creating an incident response policy and an incident response plan. With the plan in place, personnel are trained and given the tools necessary to handle incidents. Ideally, incident response preparation will help an organization prevent an incident. However, this isn't realistic for most organizations, but with an effective plan in place, the organization will be able to effectively handle any incidents that occur.

Some of the common phases of an ***incident response process*** are:

- **Preparation.** This phase occurs before an incident and provides guidance to personnel on how to respond to an incident. It includes establishing and maintaining an incident response plan and incident response procedures. It also includes establishing procedures to prevent incidents. For example, preparation includes implementing security controls to prevent malware infections.
- **Identification.** All events aren't security incidents so when a potential incident is reported, personnel take the time to verify it is an actual incident. For example, intrusion detection systems (IDSs) might falsely report an intrusion, but administrators would investigate it and verify if it is a false positive or an incident. If the incident is verified, personnel might try to isolate the system based on established procedures.
- **Containment.** After identifying an incident, security personnel attempt to isolate or contain it. This might include quarantining a device or removing it from the network. This can be as simple as unplugging the system's network interface card to ensure it can't communicate on the network. Similarly, you can isolate a network

from the Internet by modifying access control lists on a router or a network firewall. This is similar to how you'd respond to water spilling from an overflowing sink. You wouldn't start cleaning up the water until you first turn off the faucet. The goal of isolation is to prevent the problem from spreading to other areas or other computers in your network, or to simply stop the attack.

- **Eradication.** After containing the incident, it's often necessary to remove components from the attack. For example, if attackers installed malware on systems, it's important to remove all remnants of the malware on all hosts within the organization. Similarly, an attack might have been launched from one or more compromised accounts. Eradication would include deleting or disabling these accounts.
- **Recovery.** During the recovery process, administrators return all affected systems to normal operation and verify they are operating normally. This might include rebuilding systems from images, restoring data from backups, and installing updates. Additionally, if administrators have identified the vulnerabilities that caused the incident, they typically take steps to remove the vulnerabilities.
- **Lessons learned.** After personnel handle an incident, security personnel perform a lessons learned review. It's very possible the incident provides some valuable lessons and the organization might modify procedures or add additional controls to prevent a reoccurrence of the incident. A review might indicate a need to provide additional training to users, or indicate a need to update the incident response policy. The goal is to prevent a future reoccurrence of the incident.

Remember this

The first step in the incident response process is preparation. After identifying an incident, personnel attempt to contain or isolate the problem. This is often as simple as disconnecting a computer from a network. Eradication attempts to remove all malicious components from an attack and recovery returns a system to normal operation. Reviewing lessons learned allows personnel to analyze the incident and the response with a goal of preventing a future occurrence.

Implementing Basic Forensic Procedures

A forensic evaluation helps the organization collect and analyze data as evidence it can use in the prosecution of a crime. In general, forensic evaluations proceed with the assumption that the data collected will be used as evidence in court. Because of this, forensic practices protect evidence to prevent modification and control evidence after collecting it.

Once the incident has been contained or isolated, the next step is a forensic evaluation. What do you think of when you hear forensics? Many people think about the TV program *CSI* (short for "crime scene investigation") and all of its spin-offs. These shows demonstrate the phenomenal capabilities of science in crime investigations.

Computer forensics analyzes evidence from computers to determine details on computer incidents, similar to how CSI personnel analyze evidence from crime scenes. It uses a variety of different tools to gather and analyze computer evidence. Computer forensics is a growing field, and many educational institutions offer specialized degrees around the science. Although you might not be the computer forensics expert analyzing the evidence, you should know about some of the basic concepts related to gathering and preserving the evidence.

Forensic experts use a variety of forensic procedures to collect and protect data after an attack. A key part of this process is preserving the evidence during the data acquisition phase. In other words, they ensure that they don't modify the data as they collect it, and they protect it after collection. A rookie cop wouldn't walk through a pool of blood at a crime scene, at least not more than once. Similarly, employees shouldn't access systems that have been attacked or power them down.

For example, files have properties that show when they were last accessed. However, in many situations, accessing the file modifies this property. If the file is evidence, then accessing it has modified the evidence. This can prevent an investigation from identifying when an attacker accessed the file. Additionally, data in a system's memory includes valuable evidence, but turning a system off deletes this data. In general, an incident response team does not attempt to analyze evidence until they have taken the time to

collect and protect it.

Forensic experts have specialized tools they can use to capture data. For example, many experts use EnCase Forensic by Guidance Software or Forensic Toolkit (FTK) by AccessData. These tools can capture data from memory or disks. This includes documents, images, email, webmail, Internet artifacts, web history, chat sessions, compressed files, backup files, and encrypted files. They can also capture data from smartphones and tablets.

Kali Linux includes a wide variety of forensic tools. Feel free to dig into any of them to learn more. They are available via the Applications > Forensics menu.

Order of Volatility

Order of volatility refers to the order in which you should collect evidence. Volatile doesn't mean it's explosive, but rather that it is not permanent. In general, you should collect evidence starting with the most volatile and moving to the least volatile.

For example, random access memory (RAM) is lost after powering down a computer. Because of this, it is important to realize you shouldn't power a computer down if you suspect it has been involved in a security incident and might hold valuable evidence.

A processor can only work on data in RAM, so all the data in RAM indicates what the system was doing. This includes data users have been working on, system processes, network processes, application remnants, and much more. All of this can be valuable evidence in an investigation, but if a rookie technician turns the computer off, the evidence is lost.

Many forensic tools include the ability to capture volatile data. For example, Kali Linux includes the application Volatility (available in Applications > Forensics > Volatility) that can capture the contents of RAM. Once it's captured, experts can analyze it and gain insight into what the computer and user were doing.

In contrast, data on a disk drive remains on the drive even after powering a system down. This includes any files and even low-level data such as the Master Boot Record on a drive. However, it's important to protect the data on the disk before analyzing it, and a common method is by capturing an image of the disk.

The order of volatility from most volatile to least volatile is:

- Data in cache memory, including the processor cache and hard drive

cache

- Data in RAM, including system and network processes
- A paging file (sometimes called a swap file) on the system disk drive
- Data stored on local disk drives
- Logs stored on remote systems
- Archive media

In case you don't remember from your CompTIA A+ days, the page file is an extension of RAM and it is stored on the hard drive. However, the page file isn't a typical file and it's rebuilt when the system is rebooted, making it more volatile than other files stored on hard drives.

Remember this

When collecting data for a forensic analysis, you should collect it from the most volatile to the least volatile. The order of volatility is cache memory, regular RAM, swap or paging file, hard drive data, logs stored on remote systems, and archived media.

Data Acquisition and Preservation of Evidence

When performing data acquisition for evidence, it's important to follow specific procedures to ensure that the evidence is not modified. The following sections provide more information on these procedures.

Capture System Image

A forensic image of a disk captures the entire contents of the drive. Some tools use bit-by- bit copy methods that can read the data without modifying it. Other methods include hardware devices connected to the drive to write-protect it during the copy process.

Chapter 5, "Securing Hosts and Data," introduces disk images as a common method used to deploy systems. These system disk images include mandatory security configurations and help ensure a system starts in a secure state. A distinct difference between standard system images and forensic images is that a forensic image is an exact copy and does not modify the original. This isn't always true with system imaging tools.

One of the oldest disk imaging tools used for forensics is the dd command available in Linux systems, including Kali Linux. It can also be

installed on Windows systems. To see how dd works, check out the labs for this chapter at *http://gcgapremium.com/501labs/.*

These methods capture the entire contents of the disk, including system files, user files, and files marked for deletion but not overwritten. Similarly, many tools include the ability to capture data within volatile memory and save it as an image.

After capturing an image, experts create a copy and analyze the copy. They do not analyze the original disk and often don't even analyze the original image. They understand that by analyzing the contents of a disk directly, they can modify the contents. By creating and analyzing forensic copies, they never modify the original evidence.

Take Hashes

Hashing is an important element of forensic analysis to provide proof that collected data has retained integrity. Chapter 10, "Understanding Cryptography and PKI," covers hashes and hashing. As a reminder, a hash is simply a number. You can execute a hashing algorithm against data as many times as you want, and as long as the data is the same, the hash will be the same. The focus in Chapter 10 is on using hashes with files and messages. A captured forensic image (from RAM or a disk) is just a file, and you can use hashing with forensic images to ensure image integrity.

If you do the dd lab mentioned previously, it includes steps to create a copy of the image. After creating the copy, you also have a chance to use the sha1sum command to create and compare hashes.

For example, after capturing an image of a disk, an expert can create a hash of the image. The expert can then write-protect the image to prevent accidental modifications during the analysis. Later, the expert can take another hash of the image and compare it with the original hash. As long as both hashes are the same, it provides proof that the image is the same and the analysis did not modify it.

Forensic analysts sometimes make a copy of the image to analyze, instead of analyzing the first image they capture. If they ever need to verify the integrity of the copy, they run the same hashing algorithm against it. Again, as long as the hash is the same, they know the analyzed data is the same as the captured data.

Similarly, some tools allow you to create a hash of an entire drive. These verify that the imaging process has not modified data. For example,

you can create a hash of a drive before capturing the image and after capturing the image. If the hashes are the same, it verifies that the imaging process did not modify the drive.

Remember this

A forensic image is a bit-by-bit copy of the data and does not modify the data during the capture. Experts capture an image of the data before analysis to preserve the original and maintain its usability as evidence. Hashing provides integrity for captured images, including images of both memory and disk drives. You can take a hash of a drive before and after capturing an image to verify that the imaging process did not modify the drive contents.

Network Traffic and Logs

A forensic investigation often includes an analysis of network traffic and available logs. This information helps the investigators re-create events leading up to and during an incident.

As an example, an organization might want to prove that a specific computer was involved in an attack. One way is to match the media access control (MAC) address used by the attacking computer with an existing computer. The MAC address is permanently assigned to a network interface card, and even though the operating system can be manipulated to use a different MAC, the actual MAC isn't changed. In contrast, the IP address and name of the computer are not permanently assigned, and it is relatively easy to change them.

Chapter 8, "Using Risk Management Tools," covers protocol analyzers used to analyze data packets. Data within packets identifies the computers involved in a conversation based on their IP address and their MAC address. If a data capture shows a MAC address matches the actual MAC address of a suspected computer, it provides a strong indication the computer was involved in the attack.

Similarly, if the attack came from the Internet, you can trace the IP address back to the Internet Service Provider (ISP). ISPs issue IP addresses to users and the ISP logs identify exactly who was issued an IP address at any given time. This is often effective at catching amateur hackers, but professional criminals use a variety of tools to mask their actual address.

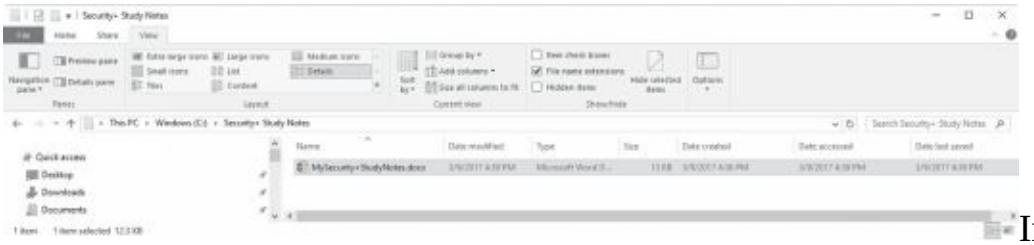
Chapter 8 presents information on logs. Logs record what happened during an event, when it happened, and what account was used during the event. You might remember that a Security log records logon and logoff events. Similarly, many applications require users to authenticate, and applications log authentication events. All of these logs can be invaluable in re-creating the details of an event after a security incident, including the identity of the account used in the attack.

Capture Video

Video surveillance methods such as closed-circuit television (CCTV) systems are often used as a detective control during an investigation. If a person is recorded on video, the video provides reliable proof of the person's location and activity. For example, if a person is stealing equipment or data, video might provide proof.

As an example, I remember a high school student was working nights at a local grocery store. The store had a delivery of beer in a tractor-trailer that hadn't been unloaded yet but was kept backed up to the store loading dock overnight. The student stole several cases of beer thinking the crime was undetectable. However, the entire scene was recorded on video. When he showed up for work the next evening, the store promptly called the police and provided a copy of the video. The video provided reliable proof that simply couldn't be disputed.

Record Time Offset



In some cases, it's easy to identify the time of an event such as in Figure 11.1. In the figure, you can easily identify the exact dates and times when someone created, modified, last saved, and last accessed the file. However, in some cases, you need to consider a time offset.

Figure 11.1: File Explorer showing exact dates and times

For example, Greenwich Mean Time (GMT) identifies the time at the Royal Observatory in Greenwich, London. Other times are often expressed as a relationship to GMT. For example, I live in the Eastern Standard Time (EST) zone, which has a four-hour offset. You can express the Date Accessed time as 5:10 p.m. EST. Using GMT, you can express the same time as 9:10 p.m. GMT. One benefit of using GMT is that it doesn't change for daylight saving time, so it stays constant.

Many video recorders use a ***record time offset*** to identify times on tape recordings rather than the actual time. For example, a recording might use a displayed counter to identify the time that has passed since the recording started. Imagine that the counter advances 1,000 ticks or counts per hour. If the counter indicates an event occurred at an offset time of 1,500 and the recording started at midnight, then the time of the event was 1:30 a.m.

When analyzing timestamps of any evidence, it's important to understand that these times are often based on an offset. If you can't identify the offset, you might not be able to identify the actual time.

Screenshots

Screenshots are simply pictures of what you can see displayed on a computer screen. If you want to capture exactly what a user was doing, or specific displays, a screenshot is the perfect solution.

For example, Figure 11.1, shown previously, is a screenshot of File Explorer. You can save screenshots as graphics files and embed these graphics into documents. Many operating systems include the ability to capture the screen and save it to the Clipboard. For example, you can capture the screen of almost any system by pressing the PrtScn key found on most keyboards. Many applications such as the Windows Snipping Tool or Snagit by TechSmith allow you to capture screenshots from specific windows or applications, any region of the screen, and even scrolling windows such as a long web page.

Witness Interviews

Another element of an investigation is interviewing witnesses. Witnesses provide firsthand reports of what happened and when it happened. However, witnesses won't necessarily come forward with relevant information unless someone asks them. Often witnesses don't recognize what

information is valuable.

For example, imagine a tailgating incident where an attacker follows closely behind an employee. The employee uses a proximity card to get in, but the attacker just walks right in behind the employee. The employee might notice, but not give it much thought, especially if tailgating is common in the organization. If the attack resulted in loss of equipment or data, an investigator might get a good description of the attacker just by interviewing witnesses.

Chain of Custody

A key part of incident response is collecting and protecting evidence. A ***chain of custody*** is a process that provides assurances that evidence has been controlled and handled properly after collection. Forensic experts establish a chain of custody when they first collect evidence.

Security professionals use a chain of custody form to document this control. The chain of custody form provides a record of every person who was in possession of a physical asset collected as evidence. It shows who had custody of the evidence and where it was stored the entire time since collection. Additionally, personnel often tag the evidence as part of a chain of custody process. A proper chain of custody process ensures that evidence presented in a court of law is the same evidence that security professionals collected.

As an example, imagine that Homer collected a hard drive as part of an investigation. However, instead of establishing a chain of custody, he simply stores the drive on his desk with the intention of analyzing it the next day. Is it possible that someone could modify the contents of the drive overnight? Absolutely. Instead, he should immediately establish a chain of custody and lock the drive in a secure storage location.

If evidence is not controlled, someone can modify, tamper, or corrupt it. Courts will rule the evidence inadmissible if there is a lack of adequate control, or even a lack of documentation showing that personnel maintained adequate control. However, the chain of custody provides proof that personnel handled the evidence properly.

Legal Hold

A ***legal hold*** refers to a court order to maintain different types of data as evidence. As an example, imagine that Ziffcorp is being sued for fraud and is

being investigated by the Securities and Exchange Commission. A court orders them to maintain digital and paper documents for the past three years related to the case. Ziffcorp now needs to take steps to preserve the data.

This data may include emails; databases; backup tapes; data stored on servers in file shares and document libraries; and data stored on desktop computers, laptops, tablets, and smartphones owned by the company. The first step management needs to take is to direct the data custodians to preserve this data. On the surface, this might sound easy, but it can be tremendously complex, especially if it is not clear to data custodians what data should be maintained. They might preserve too much data, resulting in a significant cost to store it. They might preserve too little data, subjecting the company to more litigation in a suspected cover-up.

Data retention policies also apply here. As an example, imagine that the data retention policy states that email older than six months is deleted. If administrators rigorously followed the policy, the company wouldn't have any emails from more than six months ago. That's OK if the policy is in writing and administrators are following it.

What if the administrators didn't follow the data retention policy? What if they have email from as long as two years ago? In this scenario, administrators need to maintain these emails. If they take steps to delete the emails after receiving the court order, it looks like they are trying to withhold evidence and puts the organization into legal jeopardy for a cover-up.

Remember this

A chain of custody provides assurances that evidence has been controlled and handled properly after collection. It documents who handled the evidence and when they handled it. A legal hold is a court order to preserve data as evidence.

Recovery of Data

Generically, data recovery refers to restoring lost data, such as restoring a corrupt file from a backup. In the context of forensics, data recovery goes further. Even without backups, it's often possible to recover data that has been intentionally or accidentally deleted.

When a user deletes a file, the operating system typically just marks it for deletion and makes the space the file is consuming available to use for other files. However, the file is still there. Many file systems place the file in

a recycle bin or trash can and you can just retrieve it from there. Even if the user empties the trash after deleting a file, forensic experts can use tools to undelete the files.

Formatting a drive appears as though it has overwritten all the data on the drive. However, just as forensic experts have tools to undelete files, they also have tools they can use to unformat drives. It's worth noting that criminals have access to these same tools, too, and can recover data from systems that haven't been sanitized.

Active Logging for Intelligence Gathering

It's often appropriate for organizations to engage in strategic intelligence or counterintelligence gathering by increasing the amount of data that they collect. For example, an active logging strategy can help an organization gather a significant amount of data on attackers.

Typically, a network infrastructure is configured to log only the data needed for daily operations. If the network is under attack, administrators might increase the logging capabilities at some point while the attack is happening. However, they might not have valuable data if they had those same logging capabilities enabled when the attack began.

An active logging strategy increases the amount of logged data collected on a routine basis. Ideally, network administrators will have filters available so that they can view only the data they need for daily operations. However, if an attack begins, security professionals can view all the logged data.

Track Man-Hours and Expense

Investigations can take an extraordinary amount of time and, for any business, time is money. When budget time rolls around, the departments that can accurately identify how much time and money they spent are more likely to get their requested budget approved.

Additionally, quantitative risk assessments base decisions on using specific monetary amounts, such as cost and asset values. If an incident required involvement by security professionals on an incident response team, the man-hours and expenses incurred by the incident response team need to be included in the assessment. Including this data improves the accuracy of the cost values used in the quantitative risk assessment.

Providing Training

Organizations commonly provide training to users on a variety of issues. This includes training personnel on security policies and continuing education training to help ensure personnel remain up to date with current technologies.

Role-Based Awareness Training

Role-based awareness training is targeted to personnel based on their roles. The primary goal is to minimize the risk to the organization, and by giving users the training they need, they are better prepared to avoid threats. The following roles often require role-based training:

- **Data owner.** Data owners need to understand their responsibilities related to data that they own. This includes ensuring that the data is classified correctly and ensuring that the data is labeled to match the classification. They are also responsible for ensuring adequate security controls are implemented to protect the data. While they often delegate day-to-day tasks to data custodians, they cannot delegate their responsibility.
- **System administrator.** System administrators are responsible for the overall security of a system. They often need technical training so that they understand the software capabilities and vulnerabilities, and how to ensure the system is operating in a secure state. As a simple example, if an organization purchases a new hardware firewall, system administrators need training to ensure they know how to implement it securely.
- **System owner.** A system owner is typically a high-level executive or department head who has overall responsibility for the system. While system owners won't perform daily maintenance on their systems, they are responsible for ensuring that system administrators have the skills and knowledge to maintain them.
- **User.** Regular end users need to understand common threats, such as malware and phishing attacks. They also need to understand the risk posed by clicking an unknown link and how drive-by downloads can infect their system. Training can include a wide variety of topics

depending on the organization and can be delivered via different methods. For example, security experts can send emails informing users of current threats. Some training is delivered via web sites, in a classroom, or informally by supervisors. Training is often included when users review and sign an organization's AUP.

- **Privileged user.** A privileged user is any user with more rights and permissions than typical end users. Privileged users need training on the classification and labeling of data that they handle. Administrators are often required to use two accounts, one for regular use and one for administrative use. For administrators to follow this policy, they need to understand why it's implemented and the potential repercussions if the administrator always uses the administrator account.
- **Executive user.** Executives need high-level briefings related to the risks that the organization faces, along with information on the organization's overall information security awareness program. Additionally, executives should be trained on whaling attacks because attackers target executives with malicious phishing emails.
- **Incident response team.** An incident response team needs detailed training on how to respond to incidents. Even within the team, personnel might require different training. For example, security personnel responsible for forensic investigations need specialized forensic training.

The success of any security awareness and training plan is directly related to the support from senior management. If senior management supports the plan, middle management and employees will also support it. On the other hand, if senior management does not show support for the plan, it's very likely that personnel within the organization will not support it either.

Remember this

Role-based training ensures that employees receive appropriate training based on their roles in the organization. Common roles that require role-based training are data owners, system administrators, system owners, end users, privileged users, and executive users.

Continuing Education

Training is rarely a once and done event. Instead, personnel need to regularly receive additional training to ensure they are up to date on current threats, vulnerabilities, and technologies. If network administrators are still using the same practices and technologies they learned 10 years ago, their networks are very likely vulnerable to a multitude of attacks.

This concept is used in many different professions. For example, your doctor is required to regularly attend continuing education to update her knowledge. That's a good thing. When you're receiving medical treatment and advice, you don't want treatment and advice that was valid a decade ago, but might not be valid today. Similarly, many certifications (including the CompTIA Security+ certification) have formal continuing education requirements.

Continuing education within an organization can take many forms. It's often possible to send personnel to classes to update their knowledge. When many people need the same training, an organization will often bring in a trainer to teach a class in-house.

Training and Compliance Issues

There are many situations where training is required to maintain compliance with existing laws, best practices, and standards. As an example, many laws exist covering PII. Although these laws have many similarities, there can be minor differences in different localities. It's important for personnel handling any PII to understand the laws that apply.

Best practices often prevent a wide range of incidents when users understand and follow them. This book has covered many best practices, including developing and following a security policy, ensuring users do not share accounts, using strong passwords, following the principle of least privilege, and much more. Unless personnel know about them, and understand them, they might not be implementing them.

Additionally, many organizations should abide by certain standards. For example, organizations handling credit card information need to comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS includes six control objectives and 12 specific requirements that help prevent fraud.

Administrators might understand how to implement many of these without any additional training. However, some of the requirements might

require additional training to maintain compliance. PCI DSS isn't foolproof, but it has helped reduce many of the risks associated with credit card fraud.

Troubleshooting Personnel Issues

One of the objectives for the CompTIA exam is to troubleshoot common security issues, including personnel issues. While I've covered these topics in different chapters, I am summarizing them here. The personnel issues are insider threat, personal email, policy violation, social engineering, and social media.

The way to detect an insider threat depends on the activity. Imagine Bart is trying to copy proprietary data onto an external drive or send proprietary data outside the network via email. Data loss prevention (DLP) techniques provide the best method to detect these activities. DLP systems typically send notifications to security personnel, who can then take steps to stop Bart. Audits and reviews can often detect insider threats, too. As an example, usage auditing will detect what users are doing. This includes showing what files and folders they're accessing, and how they are using their rights and permissions. If they're doing things outside their job role, it should be investigated.

Two of these issues (personal email and social media) refer to users not following the security policy. For example, a policy might say that users can't use email for personal purposes and can't associate themselves with the organization when posting to social media. These activities are often detected by other employees and reported to management. A training program reminding users of the policies can minimize these incidents.

When policy violations are detected, management acts based on the organization's policies.

This can include anything from verbal counseling to termination. The best way to detect social engineering tactics is to educate personnel on common tactics. When they detect a social engineer, employees should report them. Security personnel can take additional steps to raise the awareness of these incidents through training and awareness programs.

Chapter 11 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Exploring Security Policies

- Written security policies are administrative controls that identify an overall security plan for an organization and help to reduce overall risk. Plans and procedures identify security controls used to enforce security policies.
- An acceptable use policy defines proper system usage for users and spells out rules of behavior when accessing systems and networks. It often provides specific examples of unacceptable usage, such as visiting certain web sites, and typically includes statements informing users that the organization monitors user activities. Users are required to read and sign an acceptable use policy when hired, and in conjunction with refresher training.
- Mandatory vacation policies require employees to take time away from their job. These policies help to reduce fraud and discover malicious activities by employees.
- A separation of duties policy separates individual tasks of an overall function between different entities or different people, and helps deter fraud. For example, a single person shouldn’t be able to approve bills and pay them, or print checks and then sign them.
- Job rotation policies require employees to change roles on a regular basis. Employees might swap roles temporarily, such as for three to four weeks, or permanently. These policies help to prevent employees from continuing with fraudulent activities, and help detect fraud if it occurs.
- Clean desk policies require users to organize their desks and surrounding areas to reduce the risk of possible data theft and password compromise.
- Background checks are performed before hiring an employee. Once hired, onboarding processes give employees access to resources. An exit interview is conducted before an employee departs the

organization, and the account is typically disabled during the interview.

- Improper use of social networking sites can result in inadvertent information disclosure. Attackers gather information from these sites to launch attacks against users, such as cognitive password attacks to change users' passwords. Training reduces these risks.
- A non-disclosure agreement helps ensure that proprietary data is not shared.
- A service level agreement (SLA) is an agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels.
- An interconnection security agreement (ISA) specifies technical and security requirements for connections and ensures data confidentiality while data is in transit.
- A memorandum of understanding or memorandum of agreement (MOU/MOA) supports an ISA, but doesn't include technical details.

Protecting Data

- Information classification practices help protect sensitive data by ensuring users understand the value of data. Data labeling ensures that users know what data they are handling and processing.
- Public data is available to anyone. Confidential data is information that an organization intends to keep secret among a certain group of people. Proprietary data is data that is related to ownership, such as patents or trade secrets. Private data includes PII and PHI.
- Destruction and sanitization methods ensure that sensitive data is removed from decommissioned systems. File shredders remove all remnants of a file. Wiping methods erase disk drives.
- Degaussing a disk magnetically erases all the data. Physically destroying a drive is the most secure method of ensuring unauthorized personnel cannot access proprietary information.
- Retention policies identify how long data is retained. They can limit a company's exposure to legal proceedings and reduce the amount of labor required to respond to court orders.
- Personally Identifiable Information (PII) is used to personally identify an individual. Examples include the full name, birth date, address, and medical information of a person. Personal Health Information (PHI) is PII that includes medical or health-related

information.

- PII/PHI requires special handling for data retention. Many laws mandate the protection of both, and require informing individuals when an attack results in the compromise of PII or PHI.
- A data owner has overall responsibility for data. A steward or custodian handles routine tasks to protect data. A privacy officer is responsible for ensuring an organization complies with relevant laws to protect privacy data, such as PII or PHI.

Responding to Incidents

- An incident response policy defines an incident and response procedures. Organizations review and update incidents periodically and after reviewing lessons learned after actual incidents.
- The first step in incident response is preparation. It includes creating and maintaining an incident response policy and includes prevention steps such as implementing security controls to prevent malware infections.
- Before acting, personnel verify an event is an actual incident. Next, they attempt to contain or isolate the problem. Disconnecting a computer from a network will isolate it.
- Eradication attempts to remove all malicious components left after an incident. Recovery restores a system to its original state. Depending on the scope of the incident, administrators might completely rebuild the system, including applying all updates and patches.
- A review of lessons learned helps an organization prevent a reoccurrence of an incident.
- The order of volatility for data from most volatile to least volatile is cache memory, regular RAM, a paging file, hard drive data, logs stored on remote systems, and archived media.
- Forensic experts capture an image of the data before analysis to preserve the original and maintain its usability as evidence.
- Hard drive imaging creates a forensic copy and prevents the forensic capture and analysis from modifying the original evidence. A forensic image is a bit-by-bit copy of the data and does not modify the data during the capture.

- Hashing provides integrity for images, including images of both memory and disk drives. Taking a hash before and after capturing a disk image verifies that the capturing process did not modify data. Hashes can reveal evidence tampering or, at the very least, that evidence has lost integrity.
- A chain of custody provides assurances that personnel controlled and handled evidence properly after collecting it. It may start with a tag attached to the physical item, followed by a chain of custody form that documents everyone who handled it and when they handled it.
- A legal hold requires an organization to protect existing data as evidence.

Providing Training

- Security awareness and training programs reinforce user compliance with security policies and help reduce risks posed by users.
- Role-based training ensures that personnel receive the training they need. For example, executives need training on whaling attacks.
- Common roles that require role-based training are data owners, system administrators, system owners, end users, privileged users, and executive users.
- Continuing education programs ensure that personnel are kept up to date on current technologies, threats, and vulnerabilities.

Online References

- Do you know how to answer performance-based questions? Check out the online extras at *http://gcgapremium.com/501-extras.*

Chapter 11 Practice Questions

1. Management within your organization wants to ensure that users understand the rules of behavior when they access the organization's computer systems and networks. Which of the following BEST describes what they would implement to meet this requirement?

   A. AUP
   B. NDA
   C. BYOD
   D. DD

2. Martin has worked as a network administrator for several years within your organization. Over time, he has been tasked with performing several jobs, including database administration and application development. Security personnel are concerned that his level of access represents a serious risk. Which of the following is the BEST solution to reduce this risk?

   A. Mandatory vacations
   B. Exit interview
   C. Change management
   D. Separation of duties

3. After a recent security audit, management has decided to upgrade the security policy. Among other items, they want to identify a policy that will reduce the risk of personnel within an organization colluding to embezzle company funds. Which of the following is the BEST choice to meet this need?

   A. AUP
   B. Training
   C. Mandatory vacations
   D. Background check

4. After a major data breach, Lisa has been tasked with reviewing security policies related to data loss. Which of the following is MOST closely related to data loss?

   A. Clean desk policy
   B. Legal hold policy
   C. Job rotation policy

D. Background check policy

5. An organization is preparing to hire additional network administrators. They decide to perform background checks on all personnel after obtaining written permission. Which of the following items is NOT appropriate to include in a background check?

A. Social media presence
B. Criminal background
C. Financial history
D. Medical history

6. Dan has been working at your company as an accountant. However, after a disagreement with an executive, he decides to leave the company and work at the local mall. He has a user account allowing him to access network resources. Which of the following is the MOST appropriate step to take?

A. Ensure his account is disabled when he announces that he will be leaving the company.
B. Immediately terminate his employment.
C. Force him to take a mandatory vacation.
D. Ensure his account is disabled during his exit interview.

7. Your organization is planning to implement an incident response plan in response to a new incident response security policy. Which of the following items is the FIRST step in an incident response process?

A. Preparation
B. Identification
C. Containment
D. Eradication

8. Waylon reported suspicious activity on his computer. After investigating, you verify that his computer is infected with malware. Which of the following steps should you take NEXT?

A. Identification
B. Preparation
C. Containment
D. Eradication

9. After a recent incident, a forensic analyst was given several hard drives to analyze. Which of the following should the analyst do FIRST?

A. Take screenshots and capture drive images.

B. Take hashes and screenshots.
C. Take hashes and capture drive images.
D. Perform antivirus scans and create chain of custody documents.

10. You need to create an image of a large hard drive for forensic analysis from a Linux system. Which of the following will you MOST likely use?
A. hashing
B. screenshots
C. dd
D. logs

11. The BizzFad company decides to partner with Costington's to bid on a contract. Management in both companies realize that they need to share proprietary data. However, they want to ensure that distribution of this data is limited within each of the companies. Which of the following will BEST meet this need?
A. MOU
B. BPA
C. NDA
D. ISA

12. You are reviewing incident response procedures related to the order of volatility. Which of the following is the LEAST volatile?
A. Hard disk drive
B. Memory
C. RAID-10 cache
D. CPU cache

13. After learning that an employee had unauthorized material on his computer, management directed security personnel to confiscate his computer. Later, a security expert captured a forensic image of the system disk. However, he reported that the computer was left unattended for several hours before he captured the image. Which of the following is a potential issue if this incident goes to court?
A. Chain of custody
B. Order of volatility
C. Time offset
D. Screenshot

14. Your organization is involved in a lawsuit. A judge issued a court order requiring your organization to keep all emails from the last three

years. Your data retention policy states that email should only be maintained from the last 12 months. After investigating, administrators realize that backups contain email from the last three years. What should they do with these backups?

A. Backups older than 12 months should be deleted to comply with the data retention policy.

B. Backups for the last 12 months should be protected to comply with the legal hold.

C. Backups for the last two years should be protected to comply with the legal hold.

D. Backups for the last three years should be protected to comply with the legal hold.

15. Your organization has decided to implement a more aggressive training and continuing education program using role-based training. Management wants to ensure that each role gets the necessary training based on the role. Which of the following BEST describes the responsibilities of data owners and indicates what training they need?

A. Ensuring data is backed up in accordance with the data policy

B. Ensuring data is classified and labeled correctly

C. Complying with laws related to privacy

D. Understanding common threats, such as malware and phishing attacks

Chapter 11 Practice Question Answers

1. **A.** An acceptable use policy (AUP) informs users of company expectations when they use computer systems and networks, and it defines acceptable rules of behavior. A non- disclosure agreement (NDA) ensures that individuals do not share proprietary data with others. A bring your own device (BYOD) policy identifies requirements for employee- owned mobile devices. The dd command (short for data duplicator) is available on Linux systems to copy files or entire disk images. Forensic analysts use it to create an image of a disk without modifying the original disk.

2. **D.** A separation of duties policy prevents any single person from performing multiple job functions that might allow the person to commit fraud. In this scenario, the administrator has accumulated privileges across several job functions, which represents the risk. A mandatory vacation policy is useful to discover fraud committed by an individual, but this scenario clearly indicates this individual controls too many job functions. An exit interview is performed when an employee leaves the organization. Change management ensures changes are reviewed before being implemented.

3. **C.** Mandatory vacations help to reduce the possibility of fraud and embezzlement. An acceptable use policy informs users of company policies and even though users sign them, they don't deter someone considering theft by embezzling funds. Training can help reduce incidents by ensuring personnel are aware of appropriate policies. A background check is useful before hiring employees, but it doesn't directly reduce risks related to employees colluding to embezzle funds.

4. **A.** A clean desk policy requires users to organize their areas to reduce the risk of possible data theft and password compromise. A legal hold refers to a court order to protect datathat might be needed as evidence. A legal hold policy may state that the organization will comply with the court order, but it isn't related to data theft. Job rotation policies require

employees to change roles on a regular basis and can expose fraudulent activity. A background check policy typically identifies what to check for when hiring an employee.

5. **D.** Medical history is not appropriate to include in a background check. However, it is common to check a potential employee's social media presence, criminal background, and financial history.

6. **D.** His account should be disabled (or deleted if that is the company policy) during the exit interview. It's appropriate to conduct an exit interview immediately before an employee departs. Employees often give a two-week or longer notice. If their access is revoked immediately, they won't be able to do any more work. While some companies do terminate employment when someone gives notice, from a security perspective, it's best to take action related to the user account. The purpose of a mandatory vacation is to detect fraud, but if the employee is leaving, any potential fraud will be detected when that employee leaves.

7. **A.** The first step in an incident response process is preparation. When a potential incident occurs, the next step is identification. If the event is a security incident, the next step is containment to isolate the incident and limit the damage. Next, personnel take steps to eradicate all elements that caused the incident, such as malware or compromised accounts.

8. **C.** After identifying an incident, the next step is containment. The scenario indicates you have identified the incident as a malware infection. Preparation is the first step in an incident response process. Eradication attempts to remove all elements of the incident after first containing it.

9. **C.** Forensic analysts capture drive images and take hashes before beginning analysis, and they only analyze the imaged copies, not the original drive. Screenshots are taken when a computer is running. An antivirus scan might modify the drive and chain of custody documents are created when evidence is collected.

10. **C.** The dd command is available on Linux systems and it is used to copy files for analysis. As an example, the dd if=/dev/sda2 of=sd2disk.img command creates an image of a disk without modifying

the original disk. None of the other choices creates an image of a drive. Hashing algorithms create a hash of a file. Screenshots create a graphic from a computer screen. Logs record log entries in files.

11. **C.** A non-disclosure agreement (NDA) helps ensure that proprietary data is not shared. It can be written to ensure that employees don't share proprietary data or business partners don't share proprietary data. A memorandum of understanding (MOU) expresses an understanding between two or more parties indicating their intention to work together toward a common goal. A business partners agreement (BPA) details the relationship between business partners, including their obligations toward the partnership. An interconnection security agreement (ISA) specifies the technical and security requirements for planning, establishing, maintaining, and disconnecting a secure connection between two or more entities.

12. **A.** Data on a hard disk drive is the least volatile of those listed. All other sources are some type of memory, which will be lost if a system is turned off. This includes data in normal memory, a redundant array of inexpensive disks 10 (RAID-10) cache, and the central processing unit's (CPU's) cache.

13. **A.** Chain of custody is the primary issue here because the computer was left unattended for several hours. It's difficult to prove that the data collected is the same data that was on the employee's computer when it was confiscated. Data captured from a disk is not volatile, so volatility is not an issue in this scenario. The time offset refers to logged times and is not related to this question. Screenshots are pictures of a screen at a moment in time, but are not related to this question.

14. **D.** The court order specified a legal hold on email from the last three years, so all the backups for the last three years should be kept. If the backups had been destroyed before the court order, they wouldn't be available, so the legal hold wouldn't apply to them. Deleting them after the court order is illegal. Protecting only the backups from the last 12 months or the last two years doesn't comply with the court order.

15. **B.** Owners are responsible for identifying the proper classification of data, ensuring it is labeled correctly, and ensuring security controls are implemented to protect the data. A data steward is responsible for

routine daily tasks such as backing up data. A privacy officer is responsible for ensuring the organization is complying with relevant laws. End users need to be trained on common threats, such as malware and phishing attacks.