PART 5

ENTERPRISE SECURITY

The modules in Part 5 deal with issues primarily pertaining to enterprise security. In Module 12, you learn about authentication credentials. Module 13 covers incident preparation, response, and investigation, while Module 14 looks at cybersecurity resilience. Finally, in Module 15, you learn about risk management and data privacy protections.

MODULE 14
CYBERSECURITY RESILIENCE

MODULE 15
RISK MANAGEMENT AND DATA PRIVACY

MODULE 12

AUTHENTICATION

After completing this module, you should be able to do the following:

1. Describe the different types of authentication credentials
2. Explain the different attacks on authentication
3. Describe how to implement authentication security solutions

Front-Page Cybersecurity

What would happen if a massive security breach at a financial institution involving the theft of user identifiers such as passwords? Most likely, all users would be required to change their passwords to prevent attackers from accessing the accounts. But what would happen if there was a similar security breach—a theft not of passwords but of biometric user identifiers such as facial scans or fingerprints? What could users do? Obviously, they cannot change their face or fingerprint as they can change a password.

Security researchers have worried over such a scenario since biometrics have become commonplace. Recently, such a breach occurred. The implications of millions of users having their biometric data stolen may affect them for the rest of their lives.

BioStar 2 is a web-based security platform that allows customers to control access to secure areas of facilities, record activity logs, and manage user permissions. The BioStar 2 system is currently in use by more than 5,700 organizations in 83 countries with 1.5 million installations—including large multinational businesses, small local businesses, governments, banks, and even the United Kingdom Metropolitan Police. As is common today with controlling access in facilities, BioStar 2 employs facial recognition and fingerprinting technology to identify users.

Security researchers from vpnMentor discovered in 2019 that BioStar 2's online database of was unprotected. Once vpnMentor uncovered the vulnerabilities, the security researchers tried to privately contact BioStar to make the company aware of the problem. However, they had difficulty getting anyone to talk to them. (In one instance, a BioStar employee in Germany even hung up on them.) The security researchers finally managed to have BioStar in France take them seriously, and the vulnerabilities were closed—but too late.

The unprotected BioStar 2 data included almost 28 million records (23 gigabytes of data) that contained the personal employee information of customers who were using BioStar 2. This included employee home addresses and emails, their security levels and clearances, work start dates, usernames and passwords, biometric data such as fingerprint information and facial scans, along with other data. The online database itself that contained this information was never designed for this type of usage, and was unprotected to the point that records could be added, deleted, or modified by anyone with a web browser. In addition, the passwords and biometric data were stored in plaintext.

Attackers could take over an account on the BioStar 2 online database to access security settings and change user permissions and lock approved employees out of a secure facility. They could also create new user accounts, add their own facial recognition and fingerprint information, and give themselves access to secure areas within a building or facility. Attackers could even create libraries of fingerprints and facial scans to be used any time they wanted to enter a secure location without being detected. Because they also had access to activity logs, attackers could delete or alter the data to hide their activities. In the words of the researchers, "A hacked building's entire security infrastructure becomes useless. Anybody with this data will have free movement to go anywhere they choose, undetected."

BioStar 2 was the first publicized wide-scale biometric breach. While the full potential danger of this theft is still unknown, what is known is that once your fingerprint or facial scan is stolen, unlike a password, it cannot be changed. When attackers develop technology to replicate your fingerprint from stolen data, they will gain access to all the private information on any device that uses biometrics or any door that unlocks based on your biometrics. For example, attackers could manipulate your biometric data to allow them to enter a nuclear power plant in which you were authorized to enter based on your biometrics, and then lock you and everyone else out—while they melt it down.

Users are urged to think twice about using biometrics until there are regulations in place. While it may be inconvenient to type a password to access a device instead of using a fingerprint, remember that once your biometric data is stolen, it potentially affects you for the rest of your life—and by then, there's nothing you can do about it.

Authentication in information security is the process of ensuring that the person or system desiring access to resources is *authentic* and not an imposter. In this module, you study authentication and the secure management techniques that enforce authentication. First, you will look at the different types of authentication credentials that can be used to verify a user's identity. Then you will look into the techniques and technology used to manage user accounts in a secure fashion.

TYPES OF AUTHENTICATION CREDENTIALS

CERTIFICATION

- 1.2 Given a scenario, analyze potential indicators to determine the type of attack.
- 1.3 Given a scenario, analyze potential indicators associated with application attacks.
- 2.4 Summarize authentication and authorization design concepts.
- 3.5 Given a scenario, implement secure mobile solutions.
- 3.8 Given a scenario, implement authentication and authorization solutions.
- 4.1 Given a scenario, use the appropriate tool to assess organizational security.

Consider this scenario: Riker, Peyton, and Paolo work on a local military base, and each afternoon, they go to the gym on the base to exercise. As they reach the entrance to the building, each must press a finger to the fingerprint reader to enter the building. (A "no tailgating" policy is strictly enforced.) As they walk to the receptionist's desk, Riker holds up his ID card to the RFID reader so the door to the locker room opens for him. As Peyton searches for his card, the receptionist, Li, waves him through to the locker room because she knows him. Riker laughs and says to Li, "It's only because of Peyton's flaming red hair that you recognize him, and it runs in his family!" Paolo, however, is new to the base and must sign in. After Li compares his signature to his membership application on file, she allows him to enter. In the locker room, each of them opens his locker using a combination lock with a series of memorized numbers.

In this scenario, the three men have been demonstrated to be *genuine* or *authentic* and not an imposter, by the seven separate elements listed in Table 12.1.

Table 12-1 Elements that prove authenticity

Element	Description	Scenario example
Somewhere you are	Restricted location	Restricted military base
Something you are	Unique biological characteristic that cannot be changed	Fingerprint reader to enter building
Something you have	Possession of an item that nobody else has	Riker's RFID card
Someone you know	Validated by another person	Li knows Peyton
Something you exhibit	Genetically determined characteristic	Peyton's flaming red hair
Something you can do	Perform an activity that cannot be exactly copied	Paolo's signature
Something you know	Knowledge that nobody else possesses	Combination to unlock locker

Because only the real or "authentic" person possesses one or more of these elements, they can be considered as types of **authentication**, which is proof of genuineness. These types of authentications can confirm a person's identity and thus give access to restricted areas or materials while also denying access by an imposter. In information technology (IT), these types of elements are known as *authentication credentials* and are presented to an IT system to verify the genuineness of the user.

NOTE 1

Three of these elements (something you know, something you have, and something you are) are called *factors* while the remaining four (somewhere you are, something you can do, something you exhibit, and someone you know) are called *attributes*. The element *something you exhibit* is often linked to more specialized attributes than the color of hair in the scenario and may even include neurological traits that can be identified by specialized medical equipment.

Although any of these elements can be used as an authentication credential, the most common in IT are something you know, something you have, something you are, and something you can do.

NOTE 2

Although many authentication credentials can be presented to an IT system to verify the genuineness of the user, all credentials can be classified into one of these seven categories.

Something You Know: Passwords

The most common IT authentication credential is providing information that only the user would know. A **password** is a secret combination of letters, numbers, and/or characters. Despite their widespread use, passwords provide weak protection and are constantly under attack.

NOTE 3

The person credited with inventing the computer password, Fernando "Corby" Corbato, who passed away in late 2019, was a researcher for MIT and worked on the Compatible Time-Sharing System (CTSS), which allowed multiple users to share computer time. He devised a way to isolate users from each other with password-protected user accounts. In his later years, Corbato lamented that passwords had become problematic. He said that the Internet made logins with passwords a "kind of a nightmare."

Password Weaknesses

The weakness of passwords centers on human memory. Human beings can memorize only a limited number of items. Passwords place heavy loads on human memory in multiple ways:

- The most effective passwords are long and complex. However, these are difficult for users to memorize and then accurately recall when needed.
- Users must remember multiple passwords for many accounts. Most users have accounts for different computers and mobile devices at work, school, and home; multiple email accounts; online banking; Internet site accounts; and so on. According to one study, in the United States, the average number of online accounts registered to a single email address is 130. The average number of accounts per Internet user is estimated to be 207.
- For the highest level of security, each account password should be unique, which further strains human memory.
- Many security policies mandate that passwords expire after a set period of time, such as every 45–60 days, when a new one must be created. Some security policies even prevent a previously used password from being recycled and used again, forcing users to repeatedly memorize new passwords.

NOTE 4

In recognition of the difficulties surrounding expired passwords, a growing trend has been to drop this requirement. In 2019, Microsoft changed its long-held policy and recommended that password expiration be dropped, and in 2017, guidelines released by the National Institute of Standards and Technology (NIST) also recommended that password expiration should no longer be used. However, the Payment Card Industry (PCI) still requires that merchants and other providers change their passwords every 90 days. Some security professionals are calling for a modified password expiration so that the length of the password dictates its expiration. For example, a user who creates a 30-character password would not have to change that password for two years, while a password that is 15-25 characters in length would expire annually, and one of fewer than 15 characters would have to be reset every 90 days. One company that tried this approach found that calls to its help desk for password resets declined by 70 percent.

Because of the burdens that passwords place on human memory, users take shortcuts to help them memorize and recall their passwords. One shortcut is to create and use a *weak password*. Weak passwords use a common word as a password (*princess*), a short word (*desk*), a predictable sequence of characters (*abc123*), or personal information (*Hannah*) in a password. Another common shortcut that dramatically weakens passwords is to reuse the same password (or a slight derivation of it) for multiple accounts: although this makes it easier for the user, it also makes it easier for an attacker who compromises one account to access all other accounts.

Even when users attempt to create stronger passwords, they generally follow predictable patterns:

- *Appending.* When users combine letters, numbers, and punctuation (*character sets*), they do it in a pattern. Most often they only add a number after letters (*caitlin1* or *cheer99*). If they add all three character sets, it is in the sequence *letters+punctuation+number* (*braden.8* or *chris#6*).
- *Replacing.* Users also use replacements in predictable patterns. Generally, a zero is used instead of the letter *o* (*passw0rd*), the digit *1* for the letter *i* (*denn1s*), or a dollar sign for an *s* (*be$tfriend*).

CAUTION Attackers are aware of these patterns in passwords and can search for them, making it faster and easier to crack the password.

The widespread use of weak passwords can be illustrated easily. An analysis of more than 562 million stolen passwords revealed that the most common length of a password was only nine characters, while fewer than 1 percent of the passwords were more than 14 characters. In addition, the percentage of passwords that used characters other than lowercase letters was remarkably low: uppercase characters were found in only 6 percent of passwords while special symbols were in just 4 percent. The 10 most common passwords in the 562 million stolen passwords are very weak and are listed in Table 12-2.[1]

Table 12-2 Ten most common passwords

Rank	Password
1	123456
2	123456789
3	abc123
4	password
5	password1
6	12345678
7	111111
8	1234567
9	12345
10	1234567890

A noted security expert summarized the password problem well by stating the following:

> *The problem is that the average user can't and won't even try to remember complex enough passwords to prevent attacks. As bad as passwords are, users will go out of the way to make it worse. If you ask them to choose a password, they'll choose a lousy one. If you force them to choose a good one, they'll write it [down] and change it back to the password they changed it from the last month. And they'll choose the same password for multiple applications.*[2]

NOTE 5

A recent study looked at users who had been told that the password to their account had been stolen in a data breach. Only one-third of the users then changed their passwords. And the users were in no rush to change their passwords: only 3 percent changed their password within 30 days after the breach, while 12 percent waited between 60 and 90 days. Incredibly, only 14 percent of users changed their password to a *stronger* password; all others created passwords that were actually weaker or the same strength as the stolen password by reusing character sequences from their previous password or creating a new password that was similar to other weak passwords they use.

Attacks on Passwords

While some attacks on passwords involve the attacker entering a password "guess" at a login prompt, these attacks have a low rate of success. Instead, attackers use a different technique that generates a high success rate.

When a user creates a password, it is not stored (or it should not be stored) in an unencrypted plaintext format; this would make it too easy for attackers to use stolen passwords. Instead, a one-way hash algorithm creates a message digest (or hash) of the password. This digest is then stored instead of the original plaintext password. When a user later enters a password to log in, a digest is created from the entered password. This digest is compared against the stored digest, and if they match, the user is authenticated.

NOTE 6

Hash algorithms are covered in Module 6.

Attackers work to steal the file of password digests. Once that file is in the hands of threat actors, it can be used in one of two ways. One method is to use a stolen hash to impersonate the user. This has been used to take advantage of a vulnerability in the Microsoft Windows NTLM (New Technology LAN Manager) hash for storing passwords on a Windows endpoint computer. An attacker who can steal the digest of an NTLM password could pretend to be the user by sending that hash to the remote system to then be authenticated. This is known as a **pass the hash** attack.

A more common use of a stolen file of password digests is for the threat actors to load that file onto their own computers and then use a sophisticated **password cracker**, which is software designed to break passwords. Password crackers create known digests (called *candidates*) and then compare them against the stolen digests. When a match occurs, the attacker knows the underlying password. Password crackers differ as to *how* the candidates are created. These different means of creating candidates include brute force, rule, dictionary, rainbow tables, and password collections.

NOTE 7

Password crackers do not "unravel" a digest to determine the underlying password; rather, they compare a digest created by a known word to a password digest created by an unknown word; when the digests match, the password has been "cracked." For example, using a password cracker, an attacker might create the digest *2602ab347f0ba5c63a0c936eba832ec5* from the word *Sunday* and then search the stolen digest file for that specific digest. If a match of digests occurs, then the attacker knowns the password is *Sunday*.

NOTE 8

When cracking passwords using a brute force attack, attackers often use computers with multiple graphics processing units (GPUs). Whereas the central processing unit (CPU) of a computer can do a wide variety of tasks, a GPU, which is separate from the CPU, is used to render screen displays on computers. GPUs are very good at performing video processing, which involves the repetitive work of performing the same function over and over on large groups of pixels on the screen. This makes GPUs superior to CPUs at repetitive tasks like breaking passwords.

Password Spraying One password attack that does not attempt to steal a file of password digests instead uses a type of "targeted guessing." A **password spraying** attack selects one or a few common passwords (*Password1* or *123456*) and then enters the same password when trying to login to several user accounts. Because this targeted guess is spread across many accounts, instead of attempting multiple password variations on a single account, it is much less likely to raise any alarms or lock out the user account from too many failed password attempts. Although password spraying may result in occasional success, it is not considered the optimal means for breaking into accounts.

Brute Force Attack In an automated **brute force attack**, every possible combination of letters, numbers, and characters is attempted to determine the user's password. The attack is not done in a random fashion but instead uses a meticulous approach to create the passwords.

Unlike a password spraying attack, in which one password is used on multiple accounts, in an **online brute force attack,** the same account is continuously attacked (called *pounded*) by entering different passwords. However, an online brute force attack is rarely used by attackers because it is impractical. Even at two or three tries per second, it could take thousands of years to guess the right password. In addition, most accounts can be set to disable all logins after a limited number of incorrect attempts (such as five), thus putting an end to the threat.

An **offline brute force attack** begins with a stolen digest file. An attacker loads this file onto a computer and then uses password cracking software to create candidate digests of every possible combination of letters, numbers, and characters. The candidates are matched against those in a stolen digest file to find a match. This is the slowest yet most thorough method.

Rule Attack A *rule attack* conducts a statistical analysis on the stolen passwords. The results of this analysis is then used to create a *mask* of the format of the candidate password. A mask of *?u ?l ?l ?l ?l ?d ?d ?d ?d* (*u* = uppercase, *l* = lowercase, and *d* = digit) would tell the password cracking program, *Use an uppercase letter for the first position, a lowercase letter for the next four positions, and digits for the remaining four positions*. Using a mask will significantly reduce the time needed to crack a password. There are three basic steps in a rule attack:

1. A small sample of the stolen password plaintext file is obtained.
2. Statistical analysis is performed on the sample to determine the length and character sets of the passwords, as seen in Figure 12-1.

```
[*] Length Statistics...
[+]                         8: 62% (612522)
[+]                         6: 18% (183307)
[+]                         7: 14% (146152)
[+]                         5: 02% (26438)
[+]                         4: 01% (15088)
[+]                         3: 00% (2497)
[+]                         2: 00% (308)
[+]                         1: 00% (113)

[*] Charset statistics...
[+]             loweralphanum: 47% (470580)
[+]                loweralpha: 46% (459208)
[+]                   numeric: 05% (56637)
```

Figure 12-1 Rule attack statistical analysis

3. A series of masks is generated that will be most successful in cracking the highest percentage of passwords. This is illustrated in Figure 12-2.

```
[*] Advanced Mask statistics...
[+]         ?l?l?l?l?l?l?l?l: 04% (688053)
[+]             ?l?l?l?l?l?l: 04% (601257)
[+]           ?l?l?l?l?l?l?l: 04% (585093)
[+]       ?l?l?l?l?l?l?l?l?l: 03% (516862)
[+]           ?d?d?d?d?d?d?d: 03% (487437)
[+]     ?d?d?d?d?d?d?d?d?d?d: 03% (478224)
[+]         ?d?d?d?d?d?d?d?d: 02% (428306)
[+]         ?l?l?l?l?l?l?d?d: 02% (420326)
[+]     ?l?l?l?l?l?l?l?l?l?l: 02% (416961)
[+]             ?d?d?d?d?d?d: 02% (390546)
[+]       ?d?d?d?d?d?d?d?d?d: 02% (307540)
[+]           ?l?l?l?l?l?d?d: 02% (292318)
[+]       ?l?l?l?l?l?l?l?d?d: 01% (273640)
```

Figure 12-2 Rule attack generated masks

NOTE 9

A rule attack is not intended to crack every password but instead gives the highest probability of the largest number of passwords that can be broken.

Dictionary Attack Another common password attack is a **dictionary attack**. A dictionary attack begins with the attacker creating digests of common dictionary words as candidates and then comparing them against those in a stolen digest file. A dictionary attack is shown in Figure 12-3. Dictionary attacks are successful because users often create passwords from simple dictionary words.

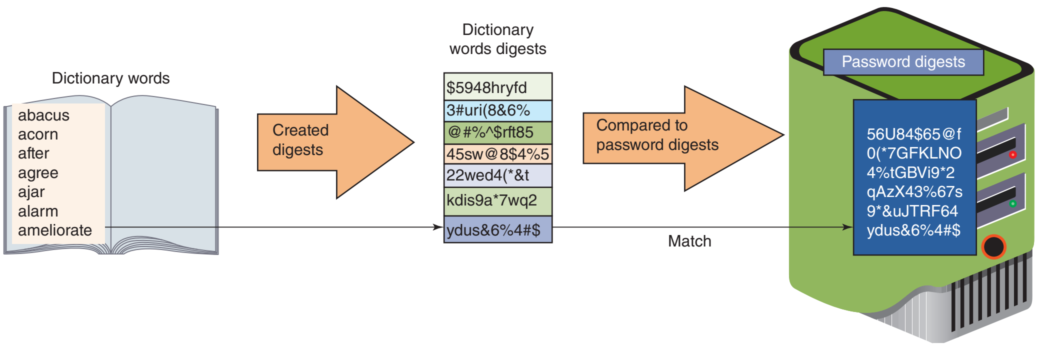


Figure 12-3 Dictionary attack

A dictionary attack that uses a set of dictionary words and compares it with the stolen digests is known as a *pre-image attack*, in that one known digest (dictionary word) is compared to an unknown digest (stolen digest). A *birthday attack* is slightly different, in that the search is for *any* two digests that are the same. A password attack that is a combination of a dictionary attack and a mask attack is called a *hybrid attack*.

NOTE 10

Birthday attacks are covered in Module 6.

Rainbow Tables **Rainbow tables** make password attacks easier by creating a large pregenerated data set of candidate digests. A rainbow table is a compressed representation of passwords that are related and organized in a sequence (called a *chain*).

Although generating a rainbow table requires a significant amount of time, once it is created, it has three significant advantages over other password attack methods. A rainbow table can be used repeatedly for attacks on other passwords; rainbow tables are much faster than dictionary attacks; and the amount of memory needed on the attacking machine is greatly reduced.

NOTE 11

Although once popular, rainbow tables are not used as extensively today due to advances in other password attack tools.

Password Collections A watershed moment in password attacks occurred in late 2009. An attacker using an SQL injection attack broke into a server belonging to a developer of several popular social media applications. This server contained more than 32 million user passwords, all in cleartext. These passwords were later posted on the Internet.

Attackers quickly seized upon this opportunity. This "treasure trove" collection of passwords gave attackers, for the first time, a large corpus of real-world passwords. Because users repeat their passwords on multiple accounts, attackers could now use these passwords as candidate passwords in their attacks with a high probability of success.

Using stolen password collections as candidate passwords is the foundation of password cracking today, and almost all password cracking software tools accept these stolen "wordlists" as input. Websites host lists of these leaked passwords that attackers can download along with important statistics and masks for a rule attack. These sites also attempt to crack submitted password collections. One website boasts more than 1.45 *trillion* cracked hashes.

NOTE 12

Password collections provide attackers advanced insight into the strategic thinking of how users create passwords. For example, on those occasions when users mix uppercase and lowercase in passwords, users tend to capitalize at the beginning of the password, much like writing a sentence. Likewise, punctuation and numbers are more likely to appear at the end of the password, again mimicking standard sentence writing. A high percentage of passwords was comprised of a name and date, such as *Braden2008*. Such insights are valuable in rule attacks, significantly reducing the amount of time needed to break a password when compared to a raw brute force attack.

Most threat actors do not use a single password attack tool but use several in combination. Table 12-3 lists a common sequence of attack tools on passwords.

Table 12-3 Common sequence of password attack tools

Order	Password attack	Explanation
1	Custom wordlist	Download a stolen password collection
2	Custom wordlist using rule attack	Generate password statistics using a rule attack to create specialized masks
3	Dictionary attack	Perform a dictionary attack on passwords
4	Dictionary attack using rules	Conduct a refined dictionary attack using results from a rule attack
5	Updated custom wordlist using rules	Input any cracked passwords from previous steps to create more refined rules
6	Hybrid attack	Perform a focused dictionary attack with a mask attack
7	Mask attack	Conduct a mask attack on harder passwords that have not already been cracked
8	Brute force attack	Last-resort effort on any remaining passwords

NOTE 13

Note that Table 12-3 assumes that a sample of the passwords in plaintext can be examined; if this is not available, then most attacks will skip to Step 3, which results in enough cracked passwords so that rules can be developed for the next step.

Something You Have: Smartphone and Security Keys

Another type of authentication credential is based on the approved user having a specific item in his possession (something you have). Such items are often used along with passwords. Because this involves more than one type of authentication credential—both what a user knows (the password) and what the user has—this type of authentication credential is called **multifactor authentication (MFA)**. Using just one type of authentication is called *single-factor authentication*, and using two types is called *two-factor authentication (2FA)*. The most common items that are used for this type of authentication are specialized devices, smartphones, and security keys.

Specialized Devices

Two specialized devices provide authentication based on something you have. These are smart cards and windowed tokens.

Smart Cards A **smart card** is a credit-card-sized plastic card that can hold information to be used as part of the authentication process. Smart cards used for authentication generally require that the card be inserted into a card reader that is connected to the computer, although some cards are contactless cards that only require it to be in close proximity to the reader.

Smart cards are used in specialized settings. For example, one type of smart card is currently being distributed by the U.S. government. A *common access card (CAC)* is a U.S. Department of Defense (DoD) smart card that is used for identification of active-duty and reserve military personnel along with civilian employees and special contractors. In addition to an integrated circuit chip, it has a bar code and magnetic stripe along with the bearer's picture and printed information. This card can be used to authenticate the owner as well as for encryption.

NOTE 14

The smart card standard covering all U.S. government employees is the Personal Identity Verification (PIV) standard.

There are several disadvantages to smart cards. Each device that uses smart card authentication must have a specialized hardware reader and device driver software installed. Also, smart cards that have a magnetic strip (called *magnetic stripe cards*) are subject to unauthorized duplication called **card cloning**. Stealing this information is often done by a process called **skimming,** in which a threat actor attaches a small device that fits just inside the card readers so that when the card is inserted and removed, both the actual reader and the skimming device capture the information from the magnetic strip.

Windowed Tokens A hardware windowed **token** is typically a small device (usually one that can be affixed to a keychain called a *key fob*) with a window display. A windowed token is shown in Figure 12-4. A windowed token does not display a value that never changes (**static code**); instead, the value dynamically changes. This value is a *one-time password (OTP)*, which is an authentication code that can be used only once or for a limited period of time.

Figure 12-4 Windowed token

There are two types of OTPs. A **time-based one-time password (TOTP)** changes after a set period of time. As illustrated in Figure 12-5, the windowed token and a corresponding authentication server share an algorithm (each user's token has a different algorithm), and the token generates a code from the algorithm once every 30 to 60 seconds. (This code is valid for only the brief period that it is displayed on the token.) The user logs in by entering a username along with the code currently being displayed on the token. When the authentication server receives it, the server looks up the algorithm associated with that specific user, generates its own code, and then compares it with what the user entered. If they are identical, the user is authenticated.

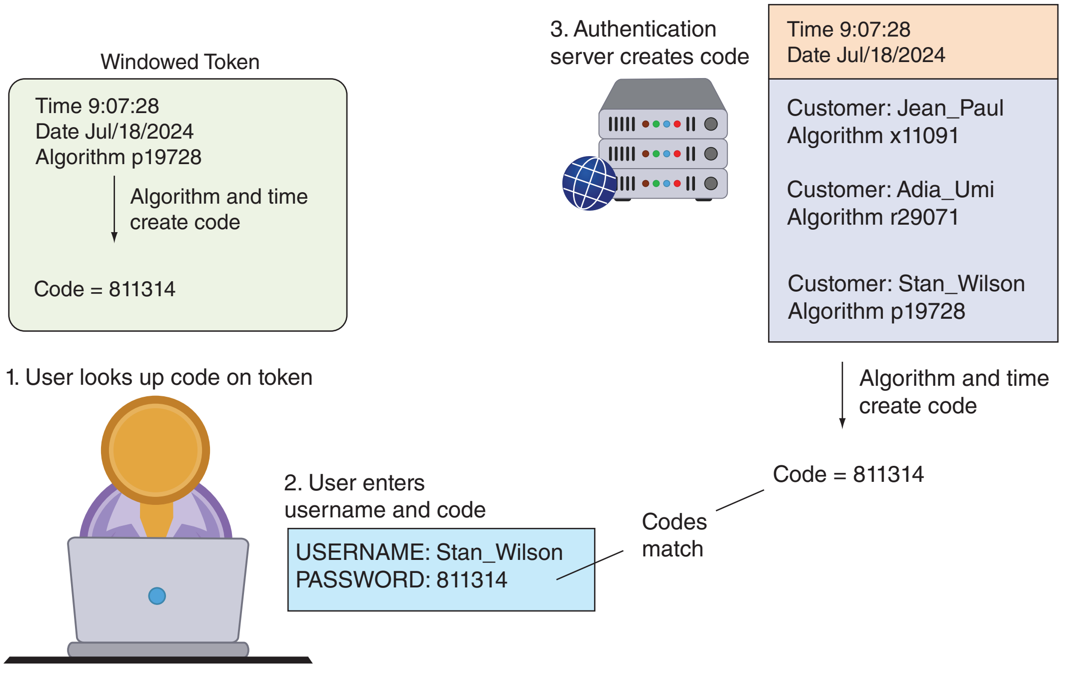


Figure 12-5 Time-based one-time password (TOTP)

NOTE 15

The TOTP is not transmitted to the token; instead, both the token and authentication server have the same algorithm and time setting.

Instead of changing after a set number of seconds, an **HMAC-based one-time password (HOTP)** password is "event driven" and changes when a specific event occurs, such as when a user enters a personal identification number (PIN) on the token's keypad, which triggers the token to create a random code. For example, after entering the PIN *1729*, the code *833854* is displayed.

While windowed tokens have some advantages, such as creating dynamic OTPs, they are considered cumbersome to use. Once an OTP is received, it must then be manually entered on the endpoint device. Because the OTP is valid for only a short time, the user must enter it quickly.

Smartphones

Whereas smart cards and windowed tokens are specialized devices, using a smartphone for authentication is considered a more practical approach. Because smartphones are ubiquitous and carried by users virtually everywhere, they can be used for authentication by a wide range of users without the need for an additional device.

Once users enter their username and password on the endpoint, their smartphone (something they have) is then used for the second authentication factor. Authentication through using a smartphone can be accomplished by the following:

- *Phone call*. An automated **phone call** to the user's smartphone asks if the user has requested to log in and, if so, to press a digit on the keypad for approval or to decline if the user has not just tried to log in.
- *SMS text message*. Another option is for the user to receive an OTP in an SMS text message. The user must then manually enter the OTP.
- *Authentication app*. An **authentication app** can be installed on the smartphone to authenticate the user. When the app is first installed, the user goes through a verification process. Whenever a user attempts to log in to an account by entering a username and password, a message is displayed on a specified phone (called a **push notification**) through the authentication app that asks the user to approve or deny the request. Using an authentication app is seen in Figure 12-6.

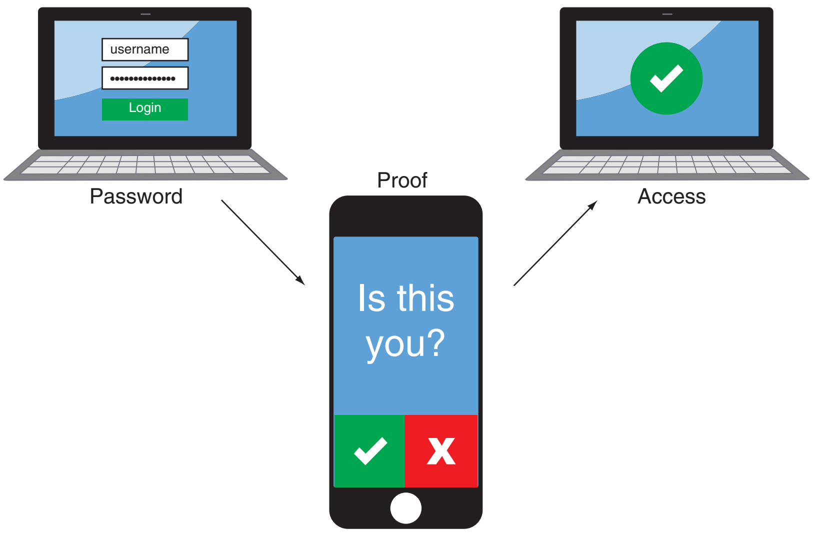


Figure 12-6 Authentication app

Despite its convenience and ability to reach a wide range of users, using a smartphone for authentication is not considered to be a secure option. An OTP received through an SMS text message can be "phished" (when a user is tricked into providing it to an attacker through a phishing attack), SMS text messages can be intercepted, and a malware infection on the phone can target the authentication app.

NOTE 16

Another authentication method involves certificate-based authentication, which is using digital certificates to authenticate a user before granting access. For example, when users go to a website that requires authentication, the web browser will prompt users for their client certificate. However, a user must select the correct certificate and the user's identity is then transmitted through the browser. Certificate-based authentication is not considered to be a viable option.

Security Keys

A secure option that is gaining acceptance is using a dedicated **token key**, more commonly called a **security key**. As seen in Figure 12-7, a security key is a dongle that is inserted into the USB port (Windows and Apple) or Lightning port (Apple) or held near the endpoint (such as a smartphone using near field communication, or NFC). It contains all the necessary cryptographic information to authenticate the user.

Source: Google LLC

Figure 12-7 Security keys

One feature of security keys is **attestation**. Attestation is a key pair that is "burned" into the security key during manufacturing time and is specific to a device model. It can be used to cryptographically prove that a user has a specific model of device when it is registered. When a user creates a new credential key pair (that links to a specific service like Facebook or PayPal), the public key that is sent to the service is signed with the attestation private key. The service that is creating the new account for the user can verify that the attestation signature on the newly created public key came from the device.

Generally speaking, attestation keys have associated attestation certificates, and those certificates chain to a root certificate that the service trusts. This is how the service establishes its trust in the authenticator's attestation key.

Security keys can be used when logging in to an endpoint device and when accessing online accounts. Some security key systems require that users must initially enroll *two* security keys in the event that one is lost or destroyed. Once the keys are enrolled, all devices that may be logged in to the user's account are then automatically logged out and can only be logged back in using one of the keys as a second factor. Users must also use the keys when logging in from any new endpoint devices for the first time. However, once a device is authenticated, by default, it no longer needs the security key during subsequent logins.

NOTE 17

Security keys do not transmit OTPs that can be intercepted or phished and are considered easier to use. Many security professionals recommend that users consider security keys as alternatives to other types of MFA.

Something You Are: Biometrics

In addition to authentication based on what a person knows or has, another category rests on the features and characteristics of the individual. This type of authentication, something you are, involves physiological biometrics and cognitive biometrics.

Physiological Biometrics

Physiological means *relating to the way in which a body part functions*. For authentication, physiological biometrics uses the way in which a body part uniquely functions in an individual. Several unique characteristics of a person's body can be used to authenticate a user. These can be divided into those that require specialized biometric scanners and those that use standard technology input devices for recognition. However, there are several issues regarding using biometrics.

Specialized Biometric Scanners Some types of biometric authentication require specialized and dedicated biometric scanners that are inspect a person's features. A retinal scanner uses the human **retina** as a biometric identifier. The retina is a layer at the back (posterior) portion of the eyeball that contains cells sensitive to light, which trigger nerve impulses that pass these through the optic nerve to the brain, where a visual image is formed. Due to the complex structure of the capillaries that supply the retina with blood, each person's retina is unique.

A retinal scanner maps the unique patterns of a retina by directing a beam of low-energy infrared light (IR) into people's eyes as they look in the scanner's eyepiece (the beam cannot be detected by a user). Because retinal blood vessels are more absorbent of IR than the rest of the eye, the amount of reflection varies during the scan. This pattern of variations is recorded and used for comparison when the user attempts to authenticate.

NOTE 18

The network of blood vessels in the retina is so complex that even identical twins do not share a similar pattern. Even though retinal patterns may be altered in cases of diabetes, glaucoma, or retinal degenerative disorders, the retina generally remains unchanged through a person's lifetime.

Using a **fingerprint** as a biometric identifier has become the most common type of biometric authentication. Every user's fingerprint consists of several ridges and valleys, with ridges being the upper skin layer segments of the finger and valleys the lower segments. In one method of fingerprint scanning, the scanner locates the point where these ridges end and split, converts them into a unique series of numbers, and then stores the information as a template. A second method creates a template from selected locations on the finger.

There are two basic types of fingerprint scanners. A *static fingerprint scanner* requires the user to place the entire thumb or finger on a small oval window on the scanner. The scanner takes an optical "picture" of the fingerprint and compares it with the fingerprint image on file. The other type of scanner is known as a *dynamic fingerprint scanner*. A dynamic fingerprint scanner has a small slit or opening, as shown in Figure 12-8.

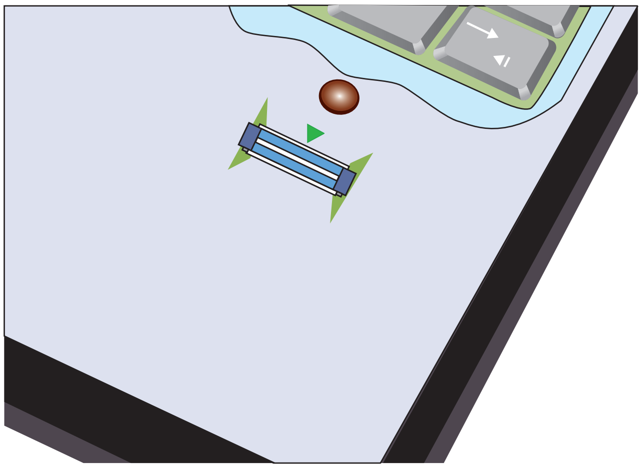


Figure 12-8 Dynamic fingerprint scanner

NOTE 19

Dynamic fingerprint scanners work on the same principle as stud finders that carpenters use to locate wood studs behind drywall. This is known as capacitive technology.

Another human characteristic that can be used for authentication is a person's **vein** (one of the "tubes" that form part of the blood circulation system in the human body that carries oxygen-depleted blood back toward the heart). Typically vein images in a user's palm or finger for authentication can be identified through a vein-scanning tablet.

A person's **gait**, or manner of walking, can also uniquely authenticate an individual. Research has shown that gait recognition can achieve greater than 99 percent accuracy. Typically, small sensors less than an inch in height can be placed on a floor at intervals of about 65 feet (20 meters) to measure gait.

NOTE 20

The payment provider Mastercard is working on developing a system that would uniquely identify mass transit passengers so that they do not need to swipe a transit card.

Standard Input Devices Unlike some biometric identifiers that require specialized scanners, other types of biometrics can use standard computer input devices for recognition, such as a microphone or camera.

Because all users' voices are different, **voice** recognition, using a standard computer microphone, can be used to authenticate users based on the unique characteristics of a person's voice. Several characteristics make each person's voice unique, from the size of the head to age. These differences can be quantified to create a user voice template.

CAUTION Voice recognition is not to be confused with speech recognition, which accepts spoken words for input as if they had been typed on the keyboard.

NOTE 21

To protect against even the remote possibility of an attacker attempting to mimic a user's voice, identification phrases can be selected that would rarely (if ever) come up in normal speech.

One of the concerns regarding voice recognition is that an attacker could record the user's voice and then create a recording to use for authentication. However, this would be difficult to do. Humans speak in phrases and sentences instead of isolated words. The *phonetic cadence*, or speaking two words together in a way that one word "bleeds" into the next word, becomes part of each user's speech pattern. It would be difficult to capture several hours of someone's voice, parse it into separate words, and then combine the words in real time to defeat voice recognition security.

An iris scanner, which can use a standard computer webcam, uses the unique characteristic of the **iris**, which is a thin, circular structure in the eye. A human iris is seen in Figure 12-9. The iris is responsible for controlling the diameter and size of the pupils to regulate the amount of light reaching the retina. Iris recognition identifies the unique random patterns in an iris for authentication.

creativemarc/Shutterstock.com

Figure 12-9 Iris

NOTE 22

A person's eye color is actually the color of the iris, which is most often brown, blue, or green. In some cases, it can be hazel, grey, violet, or even pink.

A biometric authentication that is becoming increasingly popular—but also controversial—is **facial recognition**. Every person's face has several distinguishable "landmarks" that make up their facial features. These landmarks are called *nodal points*. Each human face has approximately 80 nodal points, such as the width of the nose, the depth of the eye sockets, the shape of the cheekbones, and the length of the jaw line. Using a standard computer webcam, facial recognition software can measure the nodal points and create a numerical code (*faceprint*) that represents the face.

NOTE 23

Facial recognition is frequently used by law enforcement agencies to scan crowds for missing children, fugitive criminals, or even terrorists. This type of recognition is much less precise than personal facial recognition using a smartphone or computer for authentication. This is because variations in the lighting in a large crowd make recognition difficult, a cap or hat can obscure the subject's face, or the subject might not look directly into the camera. These limitations can partially be overcome by using a 3-D camera to compare against 3-D images.

Biometric Disadvantages Using biometrics has four disadvantages. The first is the cost for specialized biometric scanners. These scanners must be installed at each location where authentication is required.

The second disadvantage is that biometric authentication is not foolproof: genuine users may be rejected while imposters are accepted. The **false acceptance rate (FAR)** or *false positive* is the frequency at which imposters are accepted as genuine, while the **false rejection rate (FRR)** or *false negative* is the frequency that legitimate users are rejected. Biometric systems are tuned so that the FAR and FRR are equal over the size of the population (called the **crossover error rate (CER)**). Ideally, the CER should be as low as possible to produce the lowest number of accepted imposters and rejected legitimate users.

Not only do biometric sensors provide false positives and false negatives; often biometric systems can be "tricked." Security researchers have demonstrated that fingerprints can be collected from water glasses and used to trick fingerprint readers on smartphones. Tricking an iris recognition system requires taking a picture of the authentic user's eye with a digital camera in "night" mode or with the infrared filter removed. The iris picture is then printed by a color laser printer. To emulate the curvature of the eye, a normal contact lens is placed on top of the print. This can successfully trick the iris recognition system into thinking the user's real eye is in front of the camera.

A final concern with biometrics is the **efficacy rate**. *Efficacy* may be defined as the benefit achieved. While biometrics can aid in authentication, some experts question the sacrifice of user privacy: as individuals provide their biometric characteristics, how can this data be kept secure? Who can have access to it? How can it be used? The trade-offs continue to be weighed across society.

NOTE 24

Currently, six states have biometric privacy laws in place. The first and oldest regulation dating back to 2008 is the Illinois Biometric Information Privacy Act (BIPA). It regulates the collection and storage of biometric information including retina scans, iris scans, fingerprints, palm prints, voice recognition, facial-geometry recognition, DNA recognition, gait recognition, and even scent recognition. A 2019 court ruling held that people do not have to prove they were actually harmed by the use of their biometric data in order to file a case.

Cognitive Biometrics

Whereas most biometrics considers a person's physical characteristics, the field of *cognitive biometrics* is related to the perception, thought process, and understanding of the user. Cognitive biometrics is considered to be much easier for the user to remember because it is based on the user's life experiences. This also makes it more difficult for an attacker to imitate. Cognitive biometrics is also called **knowledge-based authentication**.

One type of cognitive biometrics introduced by Microsoft is called Windows Picture Password for Windows 10 touch-enabled devices. Users select a picture that has at least 10 "points of interest" that can serve as "landmarks" or places to touch, connect with a line, or draw a circle around. Specific gestures—tap, line, or circle—are then used to highlight any parts of the picture while these gestures are recorded. When logging in, a user reproduces those same gestures on the photograph, as illustrated in Figure 12-10. For attackers to replicate these actions, they would need to know the parts of the image that were highlighted, the order of the gestures, the direction, and the starting and ending points of the circles and lines. However, security researchers have found that one of the most common methods used in Picture Password was using a photo of a person and triple tapping on the face, with the most common face tap is the eyes, followed by nose and jaw.

Figure 12-10 Picture password authentication

NOTE 25

Other examples of cognitive biometrics include requiring someone to identify specific faces or recall "memorable events," such as taking a special vacation, celebrating a personal achievement, or attending a specific family dinner. The user is asked specific questions about that memorable event, such as what type of food was served, how old the person was when the event occurred, where the event was located, who was in attendance, and the reason for the event. The user authenticates by answering the same series of questions when logging in.

Something You Do: Behavioral Biometrics

Another type of authentication is based on actions that the user is uniquely qualified to perform, or something you do. This is sometimes called *behavioral biometrics*.

One type of behavioral biometrics is *keystroke dynamics*, which recognizes a user's unique typing rhythm. Keystroke dynamics uses two unique typing variables. The first is known as *dwell time*, which is the time it takes for a key to be pressed and then released. The second characteristic is *flight time*, or the time between keystrokes (both "down" when the key is pressed and "up" when the key is released are measured). After collecting multiple typing samples, a user template can be formed so that when the user enters a username and password to log in, the typing rhythm is compared to the template. If both what was entered (the password) and how it was entered (the typing rhythm) are correct, then the user is authenticated; otherwise, the user is rejected. This is shown in Figure 12-11.

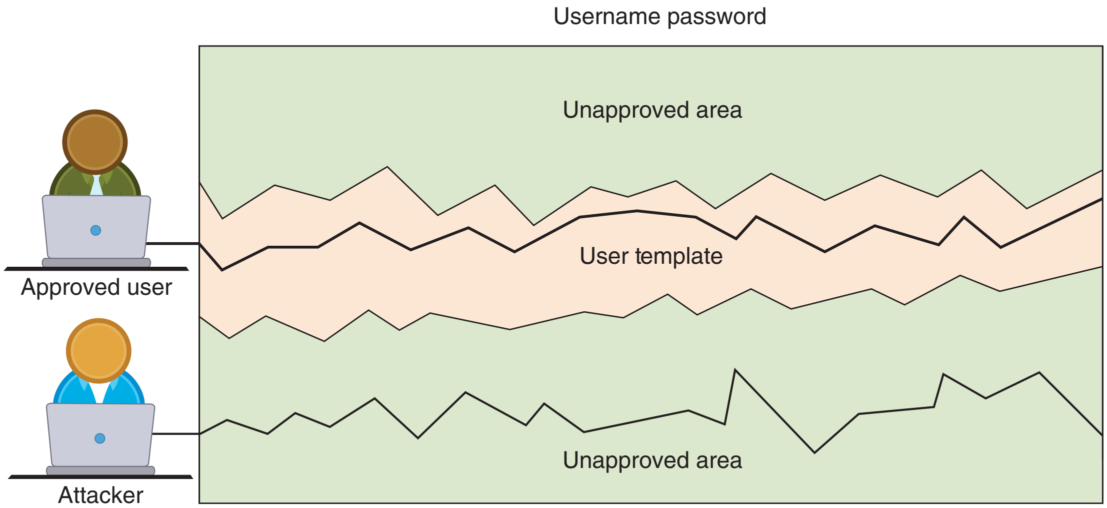


Figure 12-11 Authentication by keystroke dynamics

Keystroke dynamics holds a great deal of potential. Because it requires no specialized hardware and because the user does not have to take any additional steps beyond entering a username and password, some security experts predict that keystroke dynamics will become more widespread in the near future.

TWO RIGHTS & A WRONG

1. Password crackers differ as to when candidate digests are created.
2. Online brute force attacks are considered impractical.
3. An HMAC-based one-time password (HOTP) password is "event driven."

See Appendix B for the answer.

AUTHENTICATION SOLUTIONS

CERTIFICATION

2.4 Summarize authentication and authorization design concepts.

2.8 Summarize the basics of cryptographic concepts.

3.2 Given a scenario, implement host or application security solutions.

3.5 Given a scenario, implement secure mobile solutions.

3.7 Given a scenario, implement identity and account management controls.

3.8 Given a scenario, implement authentication and authorization solutions.

There are several solutions for securing authentication. These include security surrounding passwords and secure authentication technologies.

NOTE 26

Solutions for protecting authentication services in the cloud are similar to protecting other cloud services and are covered in Module 10. The solutions here are primarily on-prem protections.

Password Security

Because passwords are so widely used—and attacked—much attention is focused on securing passwords. This includes protecting password digest files and helping users manage their passwords.

Protecting Password Digests

Besides securing servers so that the password digest files cannot be stolen, additional steps can be taken to protect the contents of the digests. These include using salts and key stretching.

Salts One means for an enterprise to protect stored digests is to add a **salt**, which consists of a random string that is used in hash algorithms. Passwords can be protected by adding this random string to the user's plaintext password before it is hashed. Salts make dictionary attacks and brute force attacks for cracking large number of passwords much more difficult and limit the impact of rainbow tables. Another benefit of a salt is that two users choosing the same password does not help the attacker. Without salts, an attacker who can crack User #1's password would also immediately know User #2's password without performing any computations. By adding salts, however, each password digest is different.

CAUTION Salts should be random (never sequential like *0001, 0002,* etc.) and unique for each user.

Applying salts is not just limited to protected stored password digests. Salts can also be applied to sensitive information contained in a database. Database data can be further protected by hashing data and using tokenization.

NOTE 27

Tokenization is covered in Module 9.

Key Stretching Using general-purpose hash algorithms such as MD5 and SHA is not considered secure for creating digests because these hashing algorithms are designed to create a digest as quickly as possible. The speed of general-purpose hash algorithms works in an attacker's favor. When an attacker is creating candidate digests, a general-purpose hashing algorithm can rapidly create a large number of passwords for matching purposes.

A more secure approach for creating password digests is to use a specialized password hash algorithm that is intentionally designed to be slower. This would then limit the ability of an attacker to crack passwords because it requires significantly more time to create each candidate digest, thus slowing down the entire cracking process. This is called **key stretching**. Two popular key stretching password hash algorithms are bcrypt and PBKDF2. These can be configured to require more time to create a digest. A network administrator can specify the number of iterations (*rounds*), which sets how "expensive" (in terms of computer time and/or resources) the password hash function will be. Whereas the increased time is a minor inconvenience when one user logs in and waits for the password digest to be generated, it can significantly reduce attackers' speed of generating candidates.

NOTE 28

Using a general password algorithm, an attacker could generate about 95^8 candidate passwords in 5.5 hours. However, using bcrypt, only 71,000 candidate passwords could be generated in that same amount of time.

However, the problem with key stretching is that CPUs continue to process faster and faster, so yesterday's key stretching algorithms may become too fast with tomorrow's processors. The original standards written in 2000 for key stretching recommended at least 1,000 iterations. Today, iterations of 100,000 are not uncommon. To address this, a competition was initiated to develop an even stronger key stretching algorithm. After working through 24 proposals, a winner was announced: *Argon2*. Argon2 can be configured based on several different parameters: adding a salt (which must be between 8 and 16 characters), the number of iterations (default of three), and the memory usage (default parameter of 12).

Managing Passwords

While password digest files must be secured, it is likewise important that individual user passwords be kept safe. The most critical factor in a strong password is not complexity but length: a longer password is always more secure than a shorter password. This is because the longer a password is, the more attempts an attacker must make to break it. The formula for determining the number of possible passwords requires knowing only two items: the character set being used and the password length. Since the character set of most passwords is equal to the number of keys on a keyboard that can be used, the formula is *Number of Keyboard Keys ^ Password Length = Total Number of Possible Passwords*. Table 12-4 illustrates the number of possible passwords for different password lengths using a standard 95-key keyboard, along with the average attempts needed to break a password. Obviously, a longer password takes significantly more time to attempt to break than a short password.

Table 12-4 Number of possible passwords

Keyboard keys	Password length	Number of possible passwords	Average attempts to break password
95	2	9,025	4,513
95	3	857,375	428,688
95	4	81,450,625	40,725,313
95	5	7,737,809,375	3,868,904,688
95	6	735,091,890,625	367,545,945,313

NOTE 29

The average attempts to break a password is calculated as one-half of the total number of possible passwords. That is because an attack could break the password on the first attempt or on the very last attempt.

However, due to the limitations of human memory, it is virtually impossible for users to memorize long, complex, and unique passwords for all accounts. Instead of relying on human memory for passwords, security experts universally recommend using technology to store and manage passwords. The technology used for securing passwords includes using password vaults, password keys, and hardware modules.

Password Vaults As its name implies, a **password vault** is a secure repository in which users can store their passwords. Also known as a *password manager*, there are three basic types:

- *Password generators.* These are web browser extensions that generate passwords. The user enters a master password and the password generator creates a password based on the master password and the website's URL "on the fly." The disadvantage of password generators is that the browser extension must be installed on each computer and web browser.
- *Online vaults.* An online vault also uses a web browser extension, but instead of creating the user's password each time, it retrieves the password from a central online repository. The disadvantage is that online sites storing the passwords are vulnerable to attackers.
- *Password management applications.* A password management application is a program installed on a computer through which the user can create and store multiple strong passwords in a single user "vault" file that is protected by one strong master password. Users can retrieve individual passwords as needed by opening the user file, thus freeing the user from need to memorize multiple passwords. The disadvantage is that the program must be carried with the user or installed on multiple computers.

NOTE 30

A password management application is recognized as having the highest level of security. However, these applications are more than a password-protected list of passwords: they typically include drag-and-drop capabilities, enhanced encryption, in-memory protection that prevents the OS cache from being exposed to reveal retrieved passwords, and timed clipboard clearing. Some password management applications can even require that a secret key file be present when entering the master password to open the vault so that even if the vault file was stolen, it still could not be opened. The value of using a password management application is that long, complex, and unique strong passwords can be easily created and used for all accounts.

Password Keys A weakness of vaults is that they are software-based, making them susceptible to malware. More secure hardware-based solutions are also available in which to store passwords. They are called **password keys**. Just as a security key can be used by itself for MFA, a password key can also be used as a separate storage facility for passwords. Figure 12-12 illustrates a password key. Password keys often serve as a hardware-based password manager, two-factor security key, and file encryption device.

Source: OnlyKey

Figure 12-12 Password key

Hardware Modules Comprehensive cryptographic hardware modules can also facilitate password management. A hardware security module (HSM) is a removable external cryptographic device. An HSM can be a USB device, an expansion card, a device that connects directly to a computer through a port, or a secure network server. An HSM includes an onboard random number generator and key storage facility, as well as accelerated symmetric and asymmetric encryption, and can even back up sensitive material in encrypted form.

An example of an HSM in a small consumer-oriented form factor is a **MicroSD HSM**. A *Secure Digital (SD)* card is a small form factor storage media and has evolved from its inception in 1999 from a single card type and size to a variety of different types and sizes. The SD format includes four card "families" available in three form factors with different speed ratings. Currently, there are three sizes of SD cards: *full SD*, *miniSD*, and *microSD*. Full SD memory cards are typically used in personal computers, video cameras, digital cameras, and other large consumer electronics devices. MicroSD and miniSD cards are commonly used in smaller electronic devices like smartphones and tablets.

In addition to the HSM, the Trusted Platform Module (TPM) is a chip on the motherboard of the computer that provides cryptographic services. For example, TPM includes a true random number generator instead of a PRNG as well as full support for asymmetric encryption and can even generate public and private keys.

NOTE 31

HSM and TPM are covered in Module 6.

Secure Authentication Technologies

Several technologies can enhance secure authentication. These include single sign-on and authentication services.

Single Sign-On

One of the problems facing users today is the fact that they have many accounts across multiple platforms that each should use a unique username and password. Because managing different authentication credentials is difficult, users frequently compromise by selecting the least burdensome password and then use it for all accounts. A solution to this problem is to have one username and password to gain access to all accounts so that the user has only one username and password to remember.

This is the idea behind *identity management*, which is using a single authentication credential that is shared across multiple networks. When those networks are owned by different organizations, it is called **federation** (sometimes called *federated identity management* or *FIM*). One application of federation is **single sign-on (SSO)** or using one authentication credential to access multiple accounts or applications. SSO holds the promise of reducing the number of usernames and passwords that users must memorize (potentially, to just one).

NOTE 32

Several large Internet providers support SSO, but only for their own suite of services and applications. For example, a Google user can access all of Google's features—such as Gmail, Google Docs and Spreadsheets, Calendar, and Photos—by entering a single Google account username and password. Microsoft offers a similar service through its Microsoft Account. An advantage besides only using a single username and password is that settings made on one device are automatically synced with all other devices. However, these SSOs are proprietary and restricted to Google or Microsoft applications and are not "federated" with other organizations.

There are several current technologies for federation systems. These are listed in Table 12-5.

Table 12-5 Federation systems technologies

Name	Description	Explanation
OAuth (Open Authorization)	Open source federation framework	OAuth 2.0 is a framework to support the development of authorization protocols.
Open ID	Open standard decentralized authentication protocol	Authentication protocol that can be used in OAuth 2.0 as a standard means to obtain user identity.
Shibboleth	Open source software package for designing SSO	Uses federation standards to provide SSO and exchanging attributes.

NOTE 33

OAuth relies upon token credentials. Users send their authentication credentials to a server (such as a web application server) and authorize the server to issue token credentials to a third-party server. These token credentials are used in place of transferring the user's username and password. The tokens are not generic but are for specific resources on a site for a limited period.

Authentication Services

A user accessing a computer system must present authentication credentials or identification when logging in to the system. Different services can be used to provide authentication. These include RADIUS, Kerberos, Terminal Access Control Access Control Systems, directory services, Security Assertion Markup Language, and authentication framework protocols.

RADIUS **RADIUS**, or **Remote Authentication Dial-In User Service**, was developed in 1992 and quickly became the industry standard with widespread support across nearly all vendors of networking equipment. RADIUS was originally designed for remote dial-in access to a corporate network. However, the word *remote* in the name RADIUS is now almost a misnomer because RADIUS authentication is used for more than connecting to remote networks. With the development of IEEE 802.1x port security for both wired and wireless LANs, RADIUS has seen even greater usage.

NOTE 34

IEEE 802.1x is covered in Module 11.

A RADIUS client is not the device requesting authentication, such as a desktop system or wireless laptop computer. Instead, a RADIUS client is typically a device such as a wireless access point (AP) or dial-up server that is responsible for sending user credentials and connection parameters in the form of a RADIUS message to a RADIUS server. The RADIUS server authenticates and authorizes the RADIUS client request and sends back a RADIUS message response. RADIUS clients also send RADIUS accounting messages to RADIUS servers. The strength of RADIUS is that messages are never sent directly between the wireless device and the RADIUS server. This prevents an attacker from penetrating the RADIUS server and compromising security.

The detailed steps for RADIUS authentication with a wireless device in an IEEE 802.1x network, which are illustrated in Figure 12-13, are as follows:

1. A wireless device, called the *supplicant* (it makes an "appeal" for access), sends a request to an access point (AP) requesting permission to join the wireless LAN (WLAN). The AP prompts the user for the user ID and password.
2. The AP, serving as the *authenticator* that will accept or reject the wireless device, creates a data packet from this information called the *authentication request*. This packet includes information such as identification of the specific AP that is sending the authentication request and the user name and password. For protection from eavesdropping, the AP (acting as a RADIUS client) encrypts the password before it is sent to the RADIUS server. The authentication request is sent over the network from the AP to the RADIUS server. This communication can be done over either a local area network or a wide area network. This allows the RADIUS clients to be remotely located from the RADIUS server. If the RADIUS server cannot be reached, the AP can usually route the request to an alternate server.
3. When an authentication request is received, the RADIUS server validates that the request is from an approved AP and then decrypts the data packet to access the username and password information. This information is passed on to the appropriate security user database. This could be a text file, UNIX password file, a commercially available security system, or a custom database.
4. If the username and password are correct, the RADIUS server sends an authentication acknowledgment that includes information on the user's network system and service requirements. For example, the RADIUS server may tell the AP that the user needs TCP/IP. The acknowledgment can even contain filtering information to limit a user's access to specific resources on the network. If the username and password are not correct, the RADIUS server sends an authentication reject message to the AP and the user is denied access to the network. To ensure that requests are not responded to by unauthorized persons or devices on the network, the RADIUS server sends an authentication key, or signature, identifying itself to the RADIUS client.
5. If accounting is also supported by the RADIUS server, an entry is started in the accounting database.
6. Once the server information is received and verified by the AP, it enables the necessary configuration to deliver the wireless services to the user.

RADIUS allows an organization to maintain user profiles in a central database that all remote servers can share. Doing so increases security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it is easier to track usage for billing and for keeping network statistics.

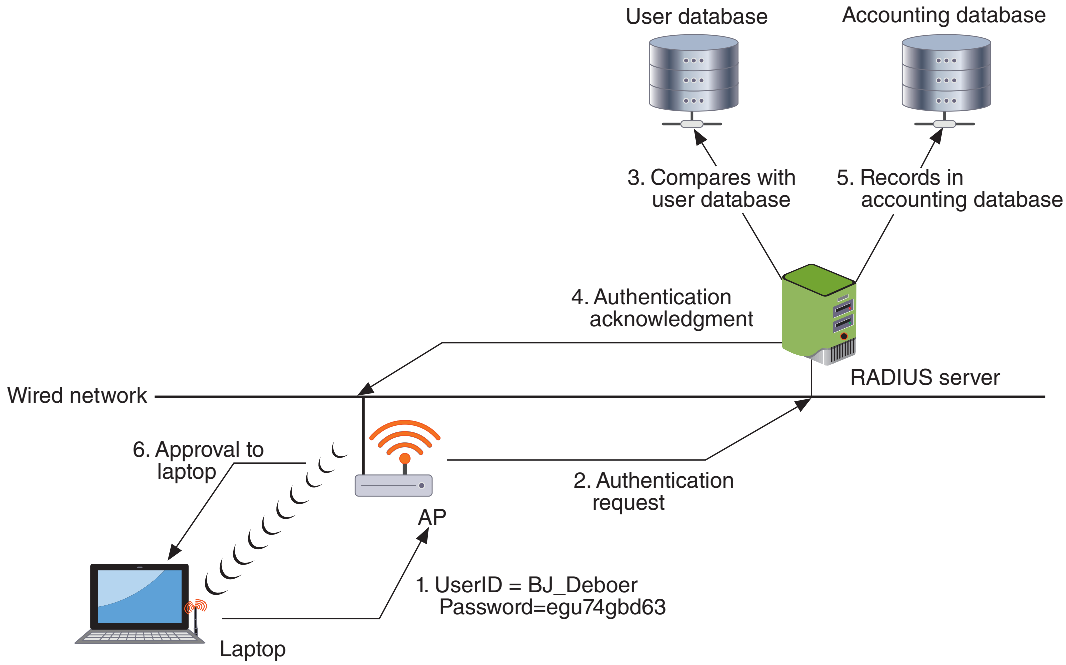


Figure 12-13 RADIUS authentication

Kerberos **Kerberos** is an authentication system developed by the Massachusetts Institute of Technology (MIT) in the 1980s and used to verify the identity of networked users. Named after a three-headed dog in Greek mythology that guarded the gates of Hades, Kerberos uses encryption and authentication for security. Kerberos will function under Windows, macOS, and Linux.

Kerberos has often been compared to using a driver's license to cash a check. A state agency, such as the Department of Motor Vehicles (DMV), issues a driver's license that has these characteristics:

- It is difficult to copy.
- It contains specific information (name, address, weight, height, etc.).
- It lists restrictions (must wear corrective lenses, etc.).
- It will expire at some future date.

Kerberos, which works in a similar fashion, is typically used when a user attempts to access a network service and that service requires authentication. The user is provided a ticket that is issued by the Kerberos authentication server, much as a driver's license is issued by the DMV. This ticket contains information linking it to the user. The user presents this ticket to the network for a service. The service then examines the ticket to verify the identity of the user. If the user is verified, he is then accepted. Kerberos tickets share some of the same characteristics as a driver's license: tickets are difficult to copy (because they are encrypted), they contain specific user information, they restrict what a user can do, and they expire after a few hours or a day. Issuing and submitting tickets in a Kerberos system is handled internally and is transparent to the user.

Terminal Access Control Access Control System+ (TACACS+) Similar to RADIUS, *Terminal Access Control Access Control System (TACACS)* is an authentication service commonly used on UNIX devices that communicates by forwarding user authentication information to a centralized server. The centralized server can be either a TACACS database or a database such as a Linux or UNIX password file with TACACS protocol support. The first version was simply called TACACS, while a later version introduced in 1990 was known as *Extended TACACS (XTACACS)*. The current version is **TACACS+**.

NOTE 35

TACACS is a proprietary system developed by Cisco Systems.

There are several differences between TACACS+ and RADIUS. These are summarized in Table 12-6.

Table 12-6 Comparison of RADIUS and TACACS+

Feature	RADIUS	TACACS+
Transport protocol	User Datagram Protocol (UDP)	Transmission Control Protocol (TCP)
Authentication and authorization	Combined	Separate
Communication	Unencrypted	Encrypted
Interacts with Kerberos	No	Yes
Can authenticate network devices	No	Yes

Directory Service A **directory service** is a database stored on the network itself that contains information about users and network devices. It contains information such as the user's name, telephone extension, email address, login name, and other facts. The directory service also keeps track of all the resources on the network and a user's privileges to those resources and grants or denies access based on the directory service information. Directory services make it much easier to grant privileges or permissions to network users and provide authentication.

Security Assertion Markup Language (SAML) **Security Assertion Markup Language (SAML)** is an XML standard that allows secure web domains to exchange user authentication and authorization data. This allows a user's login credentials to be stored with a single identity provider instead of being stored on each web service provider's server. SAML is used extensively for online e-commerce business-to-business (B2B) and business-to-consumer (B2C) transactions. The steps of a SAML transaction, which are illustrated in Figure 12-14, are as follows:

1. The user attempts to reach a website of a service provider that requires a username and password.
2. The service provider generates a SAML authentication request that is then encoded and embedded into a URL.
3. The service provider sends a redirect URL to the user's browser that includes the encoded SAML authentication request, which is then sent to the identity provider.

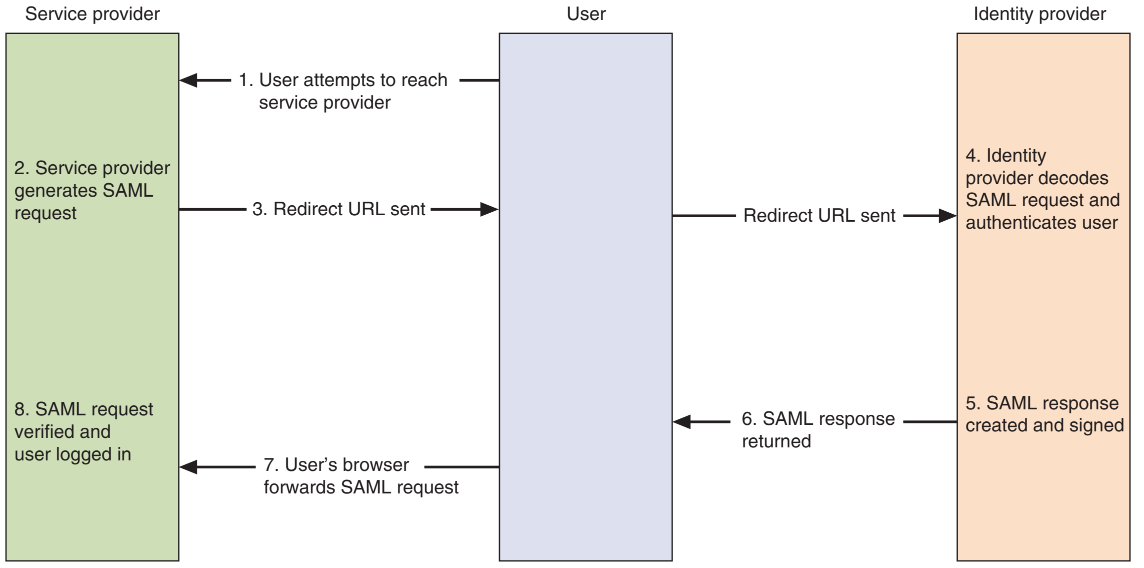


Figure 12-14 SAML transaction

4. The identity provider decodes the SAML request and extracts the embedded URL. The identity provider then attempts to authenticate the user either by asking for login credentials or by checking for valid session cookies.
5. The identity provider generates a SAML response that contains the authenticated user's username, which is then digitally signed using asymmetric cryptography.
6. The identity partner encodes the SAML response and returns that information to the user's browser.
7. Within the SAML response, there is a mechanism so that the user’s browser can forward that information back to the service provider, either by displaying a form that requires the user to click a *Submit* button or by automatically sending to the service provider.
8. The service provider verifies the SAML response by using the identity provider’s public key. If the response is successfully verified, the user is logged in.

NOTE 36

SAML works with multiple protocols including Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), and File Transfer Protocol (FTP).

Authentication Framework Protocols In an IEEE 802.1x configuration, communication between the supplicant, authenticator, and authentication server must be secure. A framework for transporting the authentication protocols is known as the *Extensible Authentication Protocol (EAP)*. EAP was created as a more secure alternative than the weak **Challenge-Handshake Authentication Protocol (CHAP)**, the Microsoft version of CHAP (**MS-CHAP**), and **Password Authentication Protocol (PAP)**. Despite its name, EAP is a *framework* for transporting authentication protocols instead of the authentication protocol itself. EAP essentially defines the format of the messages and uses four types of packets: *request*, *response*, *success*, and *failure*. Request packets are issued by the authenticator and ask for a response packet from the supplicant. Any number of request-response exchanges may be used to complete the authentication. If the authentication is successful, a success packet is sent to the supplicant; if not, a failure packet is sent.

NOTE 37

An EAP packet contains a field that indicates the function of the packet (such as response or request) and an identifier field used to match requests and responses. Response and request packets also have a field that indicates the type of data being transported (such as an authentication protocol) along with the data itself.

TWO RIGHTS & A WRONG

1. A salt is a random string that is used in hash algorithms.
2. Two popular key stretching password hash algorithms are bcrypt and PBKDF2.
3. A complex password (*xi8s7$t#6%)* is more secure than a long password (*thisisalongpassword)*.

See Appendix B for the answer.

VM LAB You’re now ready to complete the live, virtual machine labs for this module. The labs can be found in the Practice It folder in each MindTap module.

SUMMARY

- Authentication is proof of genuineness. Three authentication elements (something you know, something you have, and something you are) are called factors while the remaining four (somewhere you are, something you can do, something you exhibit, and someone you know) are called attributes. In information technology (IT), these types of elements are known as authentication credentials and are presented to an IT system to verify the genuineness of the user. Although any of these elements can be used as an authentication credential, the most common in IT are something you know, something you have, something you are, and something you can do.
- The most common "something you know" type of authentication (and any type of authentication) is a password. A password is a secret combination of letters, numbers, and/or characters that only the user should have knowledge of. Passwords provide a weak degree of protection because they rely on human memory. Human beings have a finite limit to the number of items that they can memorize. Because of the burdens that passwords place on human memory, users often take shortcuts to help them recall their passwords.
- While some attacks on passwords involve the attacker entering a password "guess" at a login prompt, these have a low rate of success. Instead, attackers use a different technique that generates a high success rate. Attackers steal the file of password digests and then load that file onto their own computers so they can attempt to discover the passwords through password cracking software. These programs create known digests (called candidates) and then compare them against the stolen digests. When a match occurs, then the attacker knows the underlying password. Password crackers differ as to how these candidates are created.
- One password attack that does not attempt to steal a file of password digests instead uses a type of "targeted guessing." A password spraying attack uses one or a small number of commonly used passwords and then uses this same password when trying to login to several different user accounts. Unlike a password spraying attack in which one password is used on multiple accounts, in an online brute force attack, the attacker continuously attacks the same account by entering different passwords. However, a password spraying attack is not considered to be practical.
- An offline brute force attack begins with a stolen digest file. An attacker loads this file onto their computer and then uses password cracking software to create candidate digests of every possible combination of letters, numbers, and characters. These are then matched against those in a stolen digest file looking for a match. A rule attack conducts a statistical analysis on the stolen passwords. The result of this analysis is then used to create a mask of the format of the candidate password. A dictionary attack begins with the attacker creating digests of common dictionary words as candidates and then comparing them against those in a stolen digest file. Dictionary attacks are successful because users often create passwords from simple dictionary words. Rainbow tables make password attacks easier by creating a large pregenerated data set of candidate digests. A rainbow table is a compressed representation of passwords that are related and organized in a sequence (called a chain). Using stolen password collections as candidate passwords is the foundation of password cracking today. Websites host lists of these leaked passwords that attackers can download along with important statistics and masks for a rule attack.
- Another type of authentication credential is based on approved users having a specific item in their possession (something you have). Such items are often used along with passwords, and because this involves more than one type of authentication credential, this is called multifactor authentication (MFA). Two specialized devices provide authentication based on something you have. A smart card is a credit-card-sized plastic card that can hold information to be used as part of the authentication process. Smart cards used for authentication generally require that the card be inserted into a card reader that is connected to the computer, although some cards are contactless cards that only require it to be in very close proximity to the reader. A hardware windowed token is typically a small device with a window display. A windowed token does not display a value that never changes (static code); instead, the value dynamically changes. This value is a one-time password (OTP), which is an authentication code that can be used only once or for a limited period of time.
- Whereas smart cards and windowed tokens are specialized devices, using a smartphone for authentication is considered a more practical approach. Authentication through using a smartphone can be accomplished by an automated phone call, an SMS text message, or through an authentication app using push notification. A more secure option that is gaining acceptance is using a dedicated token key, more commonly called a security

key. A security key is a dongle that is inserted into the computer's port or held near the endpoint (such as a smartphone using near field communication or NFC). It contains all the necessary cryptographic information to authenticate the user.

- The features and characteristics of the individual (something you are) can serve as authentication. Physiological biometrics uses a person's unique physical characteristics for authentication. This includes fingerprints, retinas, voice, iris, facial recognition, veins, and gait. There are disadvantages to biometrics. Cognitive biometrics is related to the perception, thought process, and understanding of the user. Cognitive biometrics is considered to be much easier for the user because it is based on the user's life experiences, which also makes it difficult for an attacker to imitate. Behavioral biometrics, or something you do, authenticates by normal actions that the user performs. Behavioral biometric technologies include keystroke dynamics.
- There are several solutions for securing authentication. One means for an enterprise to protect stored digests is to add a salt, which consists of a random string that is used in hash algorithms. Passwords can be protected by adding this random string to the user's plaintext password before it is hashed. Using general-purpose hash algorithms is not considered secure for creating digests because these hashing algorithms are designed to create a digest as quickly as possible. The speed of general-purpose hash algorithms works in an attacker's favor. A more secure approach for creating password digests is to use a specialized password hash algorithm that is intentionally designed to be slower. This would then limit the ability of an attacker to crack passwords because it requires significantly more time to create each candidate digest, thus slowing down the entire cracking process. This is called key stretching.
- While password digest files must be secured, it is likewise important that individual user passwords be kept safe. The most critical factor in a strong password is not complexity but length: a longer password is always more secure than a shorter password. This is because the longer a password is, the more attempts an attacker must make to break it. A password vault, also known as a password manager, is a secure repository in which users can store their passwords. A hardware-based password key can also be used as a separate storage facility for passwords. Comprehensive cryptographic hardware modules can also facilitate password management.
- Identity management is using a single authentication credential that is shared across multiple networks. When those networks are owned by different organizations, it is called federation. One application of federation is single sign-on (SSO), or using one authentication credential to access multiple accounts or applications. A user accessing a computer system must present authentication credentials or identification when logging in to the system. Different services can be used to provide authentication. RADIUS authentication is used for both wired and wireless LANs. Kerberos is an authentication system used to verify the identity of networked users. Terminal Access Control Access Control System (TACACS) is an authentication service commonly used on UNIX devices that communicates by forwarding user authentication information to a centralized server. A directory service is a database stored on the network itself that contains information about users and network devices. Directory services make it much easier to grant privileges or permissions to network users and provide authentication. A framework for transporting the authentication protocols is known as the Extensible Authentication Protocol (EAP). EAP was created as a more secure alternative than the weak Challenge-Handshake Authentication Protocol (CHAP), the Microsoft version of CHAP (MS-CHAP), and Password Authentication Protocol (PAP).

Key Terms

attestation
authentication
authentication app
brute force attack
card cloning
Challenge-Handshake Authentication Protocol (CHAP)
crossover error rate (CER)
dictionary attack
directory service
efficacy rate
facial recognition
false acceptance rate (FAR)
false rejection rate (FRR)
federation
fingerprint
gait
HMAC-based one-time password (HOTP)
iris
Kerberos
key stretching
knowledge-based authentication
MicroSD HSM
MS-CHAP
multifactor authentication (MFA)
OAuth (Open Authorization)
offline brute force attack
online brute force attack
Open ID

pass the hash
password
Password Authentication Protocol (PAP)
password crackers
password keys
password spraying
password vault
phone call
push notification
RADIUS (Remote Authentication Dial-In User Service)
rainbow tables
retina
salt
Security Assertion Markup Language (SAML)
security key
single sign-on (SSO)
skimming
smart card
someone you know
something you are
something you can do
something you exhibit
something you have
something you know
somewhere you are
static code
TACACS+
time-based one-time password (TOTP)
token
token key
vein
voice

Review Questions

1. **How is the Security Assertion Markup Language (SAML) used?**
   a. It serves as a backup to a RADIUS server.
   b. It allows secure web domains to exchange user authentication and authorization data.
   c. It is an authenticator in IEEE 802.1x.
   d. It is no longer used because it has been replaced by LDAP.
2. **Which of the following is the Microsoft version of EAP?**
   a. EAP-MS
   b. AD-EAP
   c. PAP-Microsoft
   d. MS-CHAP
3. **Which of the following is NOT used for authentication?**
   a. Somewhere you are
   b. Something you exhibit
   c. Something you can do
   d. Something you can find
4. **Ilya has been asked to recommend a federation system technology that is an open source federation framework that can support the development of authorization protocols. Which of these technologies would he recommend?**
   a. OAuth
   b. Open ID
   c. Shibboleth
   d. NTLM
5. **How is key stretching effective in resisting password attacks?**
   a. It takes more time to generate candidate password digests.
   b. It requires the use of GPUs.
   c. It does not require the use of salts.
   d. The license fees are very expensive to purchase and use it.
6. **Which of these is NOT a reason that users create weak passwords?**
   a. A lengthy and complex password can be difficult to memorize.
   b. A security policy requires a password to be changed regularly.
   c. Having multiple passwords makes it hard to remember all of them.
   d. The length and complexity required force users to circumvent creating strong passwords.
7. **Fernando is explaining to a colleague how a password cracker works. Which of the following is a valid statement about password crackers?**
   a. Most states prohibit password crackers unless they are used to retrieve a lost password.
   b. Due to their advanced capabilities, they require only a small amount of computing power.
   c. A password cracker attempts to uncover the type of hash algorithm that created the digest because once it is known, the password is broken.
   d. Password crackers differ as to how candidates are created.
8. **Which attack uses one or a small number of commonly used passwords to attempt to log in to several different user accounts?**
   a. Online brute force attack
   b. Offline brute force attack
   c. Password spraying attack
   d. Role attack

9. Why are dictionary attacks successful?
- **a.** Password crackers using a dictionary attack require less RAM than other types of password crackers.
- **b.** They link known words together in a "string" for faster processing.
- **c.** Users often create passwords from dictionary words.
- **d.** They use pregenerated rules to speed up the processing.

10. Which of these attacks is the last-resort effort in cracking a stolen password digest file?
- **a.** Hybrid
- **b.** Mask
- **c.** Rule list
- **d.** Brute force

11. Which of the following should NOT be stored in a secure password database?
- **a.** Iterations
- **b.** Password digest
- **c.** Salt
- **d.** Plaintext password

12. Which of the following is NOT an MFA using a smartphone?
- **a.** Authentication app
- **b.** Biometric gait analysis
- **c.** SMS text message
- **d.** Automated phone call

13. Timur was making a presentation regarding how attackers break passwords. His presentation demonstrated the attack technique that is the slowest yet most thorough attack that is used against passwords. Which of these password attacks did he demonstrate?
- **a.** Dictionary attack
- **b.** Hybrid attack
- **c.** Custom attack
- **d.** Brute force attack

14. Which human characteristic is NOT used for biometric identification?
- **a.** Retina
- **b.** Iris
- **c.** Height
- **d.** Fingerprint

15. ________________ biometrics is related to the perception, thought processes, and understanding of the user.
- **a.** Cognitive
- **b.** Standard
- **c.** Intelligent
- **d.** Behavioral

16. Which of the following is an authentication credential used to access multiple accounts or applications?
- **a.** Single sign-on
- **b.** Credentialization
- **c.** Identification authentication
- **d.** Federal login

17. What is a disadvantage of biometric readers?
- **a.** Speed
- **b.** Cost
- **c.** Weight
- **d.** Standards

18. Which of these creates a format of the candidate password to significantly reduce the time needed to crack a password?
- **a.** Rainbow
- **b.** Mask
- **c.** Rule
- **d.** Pass the hash

19. Pablo has been asked to look into security keys that have a feature of a key pair that is "burned" into the security key during manufacturing time and is specific to a device model. What feature is this?
- **a.** Authorization
- **b.** Authentication
- **c.** Attestation
- **d.** Accountability

20. Which one-time password is event driven?
- **a.** HOTP
- **b.** TOTP
- **c.** ROTP
- **d.** POTP

Hands-On Projects

CAUTION If you are concerned about installing any of the software in these projects on your regular computer, you can instead use the Windows Sandbox or install the software in the Windows virtual machine created in the Module 1 Hands-On Projects. Software installed within the virtual machine will not impact the host computer.

Project 12-1: Using an Online Password Cracker

Time Required: 20 minutes

Objective: 4.1 Given a scenario, use the appropriate tool to assess organizational security.

- Password crackers

Description: In this project, you create a hash on a password and then crack it through an online dictionary attack to demonstrate the speed of cracking passwords that use dictionary words.

1. The first step is to use a general-purpose hash algorithm to create a password hash. Use your web browser to go to **www.fileformat.info/tool/hash.htm**. (The location of content on the Internet may change without warning; if you are no longer able to access the program through this URL, use a search engine and search for "Fileformat.info.")
2. Under **String hash**, enter the simple password **apple123** in the **Text** box.
3. Click **Hash**.
4. Scroll down the page and copy the MD5 hash of this password to your Clipboard by selecting the text, right-clicking it, and choosing **Copy**.
5. Open a new tab on your web browser.
6. Go to **https://crackstation.net/**.
7. Paste the MD5 hash of *apple123* into the text box below **Enter up to 20 non-salted hashes, one per line**.
8. Follow the directions to affirm that you are not an automated device.
9. Click **Crack Hashes**.
10. How long did it take to crack this hash?
11. Click the browser tab to return to FileFormat.Info.
12. Under **String hash**, enter the longer password **applesauce1234** in the **Text** box.
13. Click **Hash**.
14. Scroll down the page and copy the MD5 hash of this password to your Clipboard.
15. Click the browser tab to return to the CrackStation site.
16. Paste the MD5 hash of *applesauce1234* into the text box below **Enter up to 20 non-salted hashes, one per line**.
17. Follow the directions to affirm that you are not an automated device, and then click **Crack Hashes**.
18. How long did it take this online rainbow table to crack the stronger password hash?
19. Click the browser tab to return to FileFormat.Info and experiment by entering new passwords, computing their hash, and testing them in the CrackStation site. If you are bold, enter a string hash that is similar to a real password that you use.
20. What does this tell you about the speed of password cracking tools? What does it tell you about how easy it is for attackers to crack weak passwords?
21. Close all windows.

Project 12-2: Using Facial Recognition Software with Federation Technology

Time Required: 25 minutes

Objective: 2.4 Summarize authentication and authorization design concepts.

- Biometrics

Description: Facial recognition is a biometric authentication that is becoming increasingly popular on smartphones. In this project, you download and use a facial recognition app that supports the federation technologies OAuth running on OpenID Connect and uses multifactor authentication. You need either an Apple iOS or Android device for this project.

1. On your mobile device, launch either the Apple App Store or Android Play Store app.
2. Search for **BioID Facial Recognition Authenticator**.

3. Download and install this app on your mobile device.
4. Click **Open**.
5. Use your web browser to go to **mobile.bioid.com**. (If you are no longer able to access the program through this URL, use a search engine and search for "BioID Facial Recognition.")
6. Follow the instructions to create an account.
7. Return to your mobile device, sign in to BioID, and then click **Register**.
8. Click **Yes**.
9. Click **Allow**.
10. Follow the instructions to take four sets of pictures.
11. Click **Verify**. You are now logged in using BioID. Close this app and log in again using different positions of your face. How easy is this to use? How accurate is it?
12. Open a web browser and enter the URL **playground.bioid.com**.
13. Click **Sign in or register**.
14. Click your user name to view your account information.
15. Click **Biometrics** in the left pane.
16. Under **Biometric template**, click **Examine** and then **Face** to display the photos. Read through the information and delete any photos that would not be helpful in recognizing your face. Be sure to keep at least four photos.
17. Return to the **My BioID profile** page.
18. Under **Challenge-response**, click **Enable** and read through the information. What additional degree of protection would this give you? Close the pop-up window.
19. Click **Multi-factor** in the left pane.
20. Under **Time-based one-time password (TOTP)**, click **Synchronize**. Read this information. What additional degree of protection would this give you? Click the browser's back button.
21. Under **Multi-factor authentication**, click **Configure**. Read this information. What additional degree of protection would this give you? Click the browser's back button.
22. How much would you trust this application for your authentication? Would you use it to replace your passwords? Why or why not?
23. Close all windows.

Project 12-3: Practicing Keystroke Dynamics

Time Required: 25 minutes

Objective: 2.4 Summarize authentication and authorization design concepts.

- Biometrics

Description: One type of behavioral biometrics is keystroke dynamics, which attempts to recognize a user's unique typing rhythm. In this project, you will use an online site that illustrates keystroke dynamics.

1. Use your web browser to go to **typingdna.com**. (If you are no longer able to access the program through this URL, use a search engine and search for "Typingdna.")
2. Click **Quick demo**.
3. Under **Login authentication**, click **Start demo**.
4. Enter your email and a fictitious password. Note that as you type, your information is being recorded.
5. Click **Start demo**.
6. Review and accept the terms.
7. Click **Start demo**.
8. Click **Try authentication**.
9. Enter your email and password again and log in. What percentage did you achieve?
10. Click **Try again** and this time try to alter your typing cadence. Were you able to make the program think that you are not authentic?
11. Now ask a friend to enter your email and password information. What was the result?
12. Under **Try other demos**, select one or two different demos, and determine the results. If possible, have your friend register and try to imitate their typing cadence.
13. How reliable would you consider this technology to be? How useful could it be?
14. Close all windows.

Project 12-4: Installing a Password Vault

Time Required: 25 minutes

Objective: 3.8 Given a scenario, implement authentication and authorization solutions.

- Password vaults

Description: The drawback to using strong passwords is that they can be very difficult to remember, particularly when a unique password is used for each account that a user has. As another option, password management programs allow users to store account information such as a username and password. These programs are themselves protected by a single strong password. One example of a password storage program is KeePass Password Safe, which is an open source product. In this project, you download and install KeePass.

1. Use your web browser to go to **keepass.info** and then click **Downloads**. (If you are no longer able to access the program through this URL, use a search engine and search for "KeePass.")
2. Locate the most recent portable version of KeePass and click it to download the application. Save this file in a location such as your desktop, a folder designated by your instructor, or your portable USB flash drive. When the file finishes downloading, extract and then install the program. Accept the installation defaults.

NOTE 38

Because this is the portable version of KeePass, it does not install under Windows. To use it after installation, you must double-click the filename KeePass.exe.

3. Launch KeePass to display the opening screen.
4. Click **File** and then **New** to start a password database. Enter a strong master password for the database to protect all the passwords in it.
5. Click **Entry** and then **Add Entry**. You will enter information about an online account that has a password that you already use.
6. Create a group by clicking **Group** and then **Add Group**. Enter **Websites** and then click **OK**.
7. Select the **Websites** group in the left pane, click **Entry**, and then click **Add Entry**.
8. Enter a title for your website (such as *Google Gmail*) under **Title**.
9. Under **User name**, enter the username that you use to log in to this account.
10. Delete the entries under **Password** and **Repeat** and enter the password that you use for this account and confirm it.
11. Enter the URL for this account under **URL**.
12. Click **OK**.
13. Click **File** and then **Save**. Enter your last name as the file name and then click **Save**.
14. Exit KeePass.
15. If necessary, navigate to the location of KeePass and double-click the file **KeePass.exe** to launch the application.
16. Enter your master password to open your password file.
17. If necessary, click the group to locate the account you just entered; it will be displayed in the right pane.
18. Click under **URL** to go to that website.
19. Click KeePass in the taskbar so that the window is now on top of your browser window.
20. Drag and drop your username from KeePass into the login username box for this account in your web browser.
21. Drag and drop your password from KeePass for this account.
22. Click the button on your browser to log in to this account.
23. Because you can drag and drop your account information from KeePass, you do not have to memorize any account passwords and can instead create strong passwords for each account. Is this an application that would help users create and use strong passwords? What are the strengths of such password programs? What are the weaknesses? Would you use KeePass?
24. Close all windows.

Project 12-5: Using Cognitive Biometrics

Time Required: 20 minutes

Objective: 2.4 Summarize authentication and authorization design concepts.

- Biometrics

Description: Cognitive biometrics holds great promise for adding two-factor authentication without placing a tremendous burden on the user. In this project, you participate in a demonstration of Passfaces.

1. Use your web browser to go to **www.passfaces.com/demo**. (If you are no longer able to access the program through this URL, use a search engine and search for "Passfaces demo.")
2. Under **First Time Users**, enter the requested information and then click **START THE DEMO**.
3. Click **Start the Demo**.
4. If you are prompted, accept **demo** as the name, and then click **OK**.
5. When asked, click **NEXT** to enroll now.
6. When the **Enroll in Passfaces** dialog box is displayed, click **NEXT**.
7. Look closely at the three faces you are presented with. After you are familiar with the faces, click **NEXT**.
8. You will then be asked to think of associations with the first face (who it looks like or who it reminds you of). Follow each step with the faces and then click **NEXT** after each face.
9. When the **STEP 2 Practice Using Passfaces** dialog box is displayed, click **NEXT**.
10. You will then select your faces from three separate screens, each of which has nine total faces. Click the face (which is also moving as a hint).
11. You can practice one more time. Click **NEXT**.
12. When the **STEP 3 Try Logging On with Passfaces** dialog box is displayed, click **NEXT**. Identify your faces, and click **NEXT**.
13. Click **DONE** and click **OK**.
14. Click **Try Passfaces** and then click **Logon**.
15. Click **OK** under the username and identify your faces.
16. Is this type of cognitive biometrics effective? If you came back to this site tomorrow, would you remember the three faces?
17. Close all windows.

Project 12-6: Using Windows Picture Password

Time Required: 25 minutes

Objective: 2.4 Summarize authentication and authorization design concepts.

- Biometrics

Description: In this project, you use another cognitive biometrics tool, Windows Picture Password.

1. Select a photo or other image that you want to use as a picture password. Be sure the image is clear enough so that you can create lines, dots, or circles easily and distinctively.
2. Click **Start**, then **Settings**, then **Accounts**, and finally **Sign-in options**.
3. In the right pane, scroll down and click **Picture Password**.
4. Click **Add**.
5. Enter your password when requested, and click **OK**.
6. Windows displays a generic image along with details. Click **Choose Picture**.
7. Navigate to the location of the picture that you want to use.
8. Double-click that picture.
9. Click **Use this picture**.
10. You will now create three gestures for this photo. They can be any combinations of circles, lines, and taps. On the initial screen use your mouse, stylus, or finger to draw a circle, line, or dot on the screen.
11. Windows will then prompt you to add two more gestures.
12. Windows displays an outline of the gestures for your review. You can either click **Start over** or accept these gestures.
13. Be sure to remember each gesture in sequence and where they occur on the photo. When requested, draw them again for confirmation.
14. Close all windows.
15. Now try your picture password. Click **Start** and **Sign out**.
16. Press any key when the lock screen appears to display the sign-in options along with your picture.
17. Draw the gestures to sign in. If you are unable to recreate them, click **Sign-in options** to enter your password.
18. How easy is picture password to use? How difficult? Would you consider it more or less secure than a password? Why?

Case Projects

Case Project 12-1: Testing Password Strength

How strong are your passwords? Various online tools can provide information on password strength, but not all feedback is the same. First, assign the numbers 1 through 3 to three passwords that are very similar (but not identical) to passwords you are currently using, and write down the number (not the password) on a piece of paper. Then, enter those passwords into these three online password testing services:

- How Secure Is My Password (*howsecureismypassword.net/*)
- Password Checker Online (*password-checker.online-domain-tools.com*)
- Password Meter (*www.passwordmeter.com/*)

Record next to each number the strength of that password as indicated by these three online tools. Then use each online password tester to modify the password by adding more random numbers or letters to increase its strength. How secure are your passwords? Would any of these tools encourage someone to create a stronger password? Which provided the best information? Create a one-paragraph summary of your findings.

Case Project 12-2: Password Management Applications

Research at least four password vaults, more commonly known as password management applications, one of which is a stand-alone application and another of which is a browser-based application. Create a table that lists and compares their features. Which would you recommend? Why? Create a report on your findings.

Case Project 12-3: Create Your Own Cognitive Biometric Memorable Event

What type of cognitive biometric "memorable event" do you think would be effective? Design your own example that is different from those given in the module. There should be five steps, and each step should have at least seven options. The final step should be a fill-in-the-blank user response. Compare your steps with those of other learners. Which do you think would be the easiest for users?

Case Project 12-4: Biometric Analysis

Use the Internet and other sources to research the two disadvantages of standard biometrics: cost and error rates. Select one biometric technique (fingerprint, palm print, iris, facial features, etc.) and research the costs for having biometric readers for that technique located at two separate entrances into a building. Next, research ways in which attackers attempt to defeat this particular standard biometric technique. Finally, how often will this technique reject authorized users while accepting unauthorized users compared to other standard biometric techniques? Based on your research, would you recommend this technique? Why or why not? Write a one-page paper on your findings.

Case Project 12-5: Password Requirements

Visit the website Passwords Requirements Shaming (**password-shaming.tumblr.com**), which is a list of password requirements for different websites that are considered weak. Read through several of the submissions. Select three that you consider the most egregious. Why are they the worst? Next, indicate what you would suggest to make the requirement stronger, while maintaining a requirement that most users could meet. Write a one-paragraph summary.

Case Project 12-6: Security Assertion Markup Language (SAML)

Use the Internet to research SAML. What are its features? How is it being used? What are its advantages and disadvantages? Write a one-page paper on your research.

Case Project 12-7: Log In With Other Sites

When logging in to an online account sometimes the option is provided for the user to log in using a different set of authentication credentials, such as “Log in With Facebook” in which the user’s Facebook username and password is used instead. Research the rewards and risks of logging in using authentication credentials from other sites. Is this like SSO? What are the advantages? What are the disadvantages? Is this safe? Would you recommend it? Write a one-page paper on your research.

Case Project 12-8: Biometric Laws

Several states now have biometric laws, and others are considering similar legislation. Research these laws that are currently in place from three states. Compare the laws. Are they sufficient? What are their weaknesses? Finally, create your own law that you believe would protect the biometric data of users. Write a one-page paper on your research.

Case Project 12-9: North Ridge Security

North Ridge Security provides security consulting and assurance services. You have recently been hired as an intern to assist them.

You have been asked to make a presentation for a local community group about password security.

1. Create a PowerPoint presentation for the group about the risks of weak passwords and how to create strong passwords. Include information about security keys and how smartphones can be used for MFA. Your presentation should contain at least 10 slides.
2. After the presentation, the community group has asked for your recommendation on security vaults and keys. Use the Internet to identify two of each type that you would recommend and create a memo to the group that includes why you see these as being strong choices.

Case Project 12-10: Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. Go to **community.cengage.com/infosec2** and click the *Join or Sign in* icon to log in, using your login name and password that you created in Module 1. Click **Forums (Discussion)** and click on **Security+ Case Projects (7th edition)**. Read the following case study.

Should facial recognition be limited for identification? What are the risks of having public cameras attempt to identify known criminals? Does that outweigh the potential benefits of being able to find a kidnapped child? Should there be restrictions on facial recognition? If so, what should they be? Record your thoughts on the Community Site discussion board.

References

1. Lady, Kyle, “A security analysis of over 500 million usernames and passwords,” *Duo Labs*, May 11, 2017, retrieved Jul. 27, 2020, https://duo.com/blog/a-security-analysis-of-over-500-million-usernames-and-passwords.
2. Schneier, Bruce, *Secrets and Lies: Digital Security in a Networked World* (New York: Wiley Computer Publishing), 2004.

MODULE 13

INCIDENT PREPARATION, RESPONSE, AND INVESTIGATION

After completing this module, you should be able to do the following:

1. Explain the steps in preparing for a cybersecurity incident
2. Describe how to respond in an incident
3. List the steps in an incident investigation

Front-Page Cybersecurity

Suppose that in your house or apartment you have something very valuable (a rare gemstone, a roll of cash, or a famous painting, for example). Unfortunately, a burglar finds out about it and wants to steal it. He waits until you are away from home one night and decides that now is his chance. He tries to open the front door and finds that it is securely locked. Would he then just walk away?

Probably not. Instead, he would look for a different entry point. He might check the windows in the garage, and if he finds that one of them is easy to force open, he enters the garage. He then works on the door in the garage that leads to the kitchen and opens it. He moves through the house until he finally arrives at the room where your valuable is hidden. He grabs it and disappears.

How this fictitious burglar works is how a cybersecurity attacker works. All the efforts focus on a single word: pivot. Synonyms of pivot are rotate, turn, revolve, spin, swivel, twirl, whirl, and wheel about. That's how burglars and cybersecurity attackers work today; they swiftly move from the initial entry point to other locations until they find what they are seeking.

Security researchers spend long hours analyzing how a successful cybersecurity incident occurs. This analysis helps to provide information about how threat actors can successfully compromise a system, information the victim can use to strengthen the system from future attacks. It also helps security personnel at other organizations understand how attacks take place and shore up their systems, too.

Analyzing successful cybersecurity incidents has resulted in a recipe that attackers generally follow in an attack. The steps are as follows:

1. The attackers first conduct reconnaissance against the systems, looking for vulnerabilities.
2. When a path to a vulnerability is exposed, they gain access to the system through the vulnerability.
3. Once access is gained, the attackers escalate that access to acquire more advanced privileges.
4. With the advanced privileges, they tunnel through the network looking for additional systems they can access from their elevated position.
5. Attackers install tools on the compromised systems to gain even deeper access to the network.

6. Attackers may install a backdoor that allows them repeated and long-term access to the system. The backdoors are not related to the initial vulnerability, so access remains even if the initial vulnerability is corrected.
7. Once the backdoor is installed, the attackers continue to probe until they find their ultimate target and perform their intended malicious action.

What lesson can be learned about pivoting? Think back to the burglar. Would a homeowner spend huge amounts of money on having a super-strong front door to prevent the burglar from entering the house—but not bother to even lock the garage windows? Of course not.

Yet that's what often happens when it comes to the thinking on cybersecurity. Many users, for example, decide that an email account does not need to have a strong password. Because almost all online accounts allow users to reset their password by sending a reset link to their email account, what would happen if an attacker could gain access to that email account? He could have password resets for all of the user's accounts sent to that single compromised email account, where he could then reset the password on these accounts to whatever he wanted. He could use those new passwords to enter these accounts and perform malicious actions like wiping out a bank account or gathering sensitive data.

Because cybersecurity attackers pivot like a burglar, there are no garage windows on our computers that can be left unlocked. Everything needs to be secured.

It is highly unlikely that any organization today would consider itself immune from a successful cybersecurity attack. Rather, virtually all organizations clearly understand that successful attacks are inevitable. That means that the sole focus of cybersecurity cannot be on trying to prevent an attack; rather, plans must be made for when a cybersecurity incident occurs.

The plans for preparing for an incident can be divided into three areas: incident preparation, incident response, and then a follow-up investigation as to how the incident occurred and how similar future events can be mitigated. In this module, you will study the three areas of incident preparation, response, and investigation.

INCIDENT PREPARATION

CERTIFICATION

2.1 Explain the importance of security concepts in an enterprise environment.

2.4 Summarize authentication and authorization design concepts.

3.5 Given a scenario, implement secure mobile solutions.

3.7 Given a scenario, implement identity and account management controls.

3.8 Given a scenario, implement authentication and authorization solutions.

4.2 Summarize the importance of policies, processes, and procedures for incident response.

4.1 Given a scenario, use the appropriate tool to assess organizational security.

5.5 Explain privacy and sensitive data concepts in relation to security.

Consider these two classical aphorisms: *Don't bury your head in the sand* and *An ounce of prevention is worth a pound of cure*. These pithy observations can directly apply to cybersecurity incident preparation. It is a major mistake to think that no attack could penetrate cybersecurity defenses, and being prepared for an incident significantly offsets the resources needed to recover from one if no preparations have been made. These **response and recovery controls**, or measures for identifying and counteracting security attacks, are essential.

Preparing for an incident first involves understanding the reasons such incidents are successful. This understanding can be useful in preparing for an incident.

Reasons for Cybersecurity Incidents

While there are any number of reasons a cybersecurity incident can occur, many can be classified into two broad areas. The first area is weak account types and the second is poor access control.

Weak Account Types

As outlined in the *Front-Page Cybersecurity* introduction to this module, once access is gained by threat actors, their next step is to pivot and then escalate that access to gain more advanced privileges. This is often achieved by looking for a **user account** (an approved identity between a user and an endpoint, network, or service) that has weak security and is associated with a high level of privileges. If this account can be compromised, the threat actors can imitate the owner of the account and use those privileges to access other protected systems, steal confidential data, or perform any number of nefarious activities.

Besides requiring strong authentication on user accounts, the accounts themselves should be routinely reviewed for security and, if necessary, be deleted or strengthened. For example, any **shared account** (an account used by more than one user), **generic account** (an account not tied to a specific person, such as *HelpDesk_1*), or **guest account** (given to temporary users) should be prohibited. These types of accounts that cannot be linked to a single authorized individual are common entry points threat actors compromise. In addition, a **service account**, which is a user account that is created explicitly to provide a security context for services running on a server, should be carefully configured so as not to provide more privileges than are absolutely necessary.

CAUTION Suspicious accounts that are identified should be disabled (made inactive) instead of immediately deleted. Disabling an account serves to create an audit trail to conform with compliance regulations and makes the reestablishment of an account easier if further investigation reveals that the account is valid.

Poor Access Control

As its name implies, *access control* is granting or denying approval to use specific resources; it is controlling access. While physical access control consists of fencing, hardware door locks, and mantraps to limit contact with devices, technical access control consists of technology restrictions that limit users on digital devices from accessing resources and data. Access control has a set of associated concepts and terminology used to describe its actions. Standard access control schemes and access control lists are also used to help enforce access control, though these have their own weaknesses.

NOTE 1

Most home users have full privileges on their personal computers so they can install programs, access files, or delete folders at will and give no thought to access control. In the enterprise, however, where multiple individuals could potentially have access to sensitive information, access control is essential.

Access Control Concepts Suppose that Gabe is babysitting his sister Mia one afternoon. Before leaving the house, his mother tells Gabe that a package delivery service is coming to pick up a box, which is inside the front door. Soon there is a knock at the door, and as Gabe looks out, he sees the delivery person standing on the porch. Gabe asks her to display her employee credentials, which the delivery person is pleased to do, and then he opens the door and allows her inside, but only to the area by the front door, to pick up the box. Gabe then signs the delivery person's tablet device so there is a confirmation record that the package was picked up.

This scenario illustrates the basic steps in limiting access. The package delivery person first presents an ID to Gabe to be reviewed. A user accessing a computer system would likewise present credentials or *identification*, such as a username, when logging in to the system. Identification is the process of recognizing and distinguishing the user from any other user. Checking the delivery person's credentials to be sure that they are authentic and not fabricated is *authentication*. Computer users, likewise, must have their credentials authenticated to ensure that they are who they claim to be, often by entering a password, fingerprint scan, or other means of authentication. **Authorization**, granting permission to take an action, is the next step. Gabe allowed the package delivery person to enter the house because she had been preapproved by Gabe's mother and her credentials were authentic. Likewise, once users have presented their identification and been authenticated, they can be authorized to log in to the system and access resources.

Gabe only allowed the package delivery person access to the area by the front door to retrieve the box; he did not allow her to go upstairs or into the kitchen. Likewise, computer users are granted access only to the specific services, devices, applications, and files needed to perform their job duties. Gabe signing on the tablet is akin to **accounting**, which is a record that is preserved of who accessed the network, what resources they accessed, and when they disconnected from the network. Accounting data can be used to provide an audit trail, and for billing, determining trends, identifying resource utilization, and future capacity planning. The basic steps in this access control process are summarized in Table 13-1.

NOTE 2

Authentication, authorization, and accounting are sometimes called AAA ("triple-A"), providing a framework for controlling access to computer resources.

Table 13-1 Basic steps in access control

Action	Description	Scenario example	Computer process
Identification	Review of credentials	Delivery person shows employee badge	User enters username
Authentication	Validate credentials as genuine	Gabe reads badge to determine it is real	User provides password
Authorization	Permission granted for admittance	Gabe opens door to allow delivery person in	User authorized to log in
Access	Right given to access specific resources	Delivery person can only retrieve box by door	User allowed to access only specific data
Accounting	Record of user actions	Gabe signs to confirm the package was picked up	Information recorded in log file

Other terminology describes how computer systems impose this technical access control:

- *Object*. An object is a specific resource, such as a file or a hardware device.
- *Subject*. A subject is a user or a process functioning on behalf of the user that attempts to access an object.
- *Operation*. The action that is taken by the subject over the object is called an operation. For example, a user (subject) may attempt to delete (operation) a file (object).

Individuals are given different roles in relationship to access control objects or resources. These roles are summarized in Table 13-2.

Figure 13-1 illustrates selected technical access control roles and terminology.

Access Control Schemes Consider a system administrator who needs to act as an access control data custodian/steward. One afternoon she must give a new employee access to specific servers and files. With hundreds of thousands of files scattered across a multitude of different servers, and with the new employee being given different access privileges to each file (for example, he can view one file but not edit it, but for a different file he can edit but not delete), controlling access could prove to be a daunting task.

Table 13-2 Roles in access control

Role	Description	Duties	Example
Data privacy officer (DPO)	Manager who oversees data privacy compliance and manages data risk	Ensures the enterprise complies with data privacy laws and its own privacy policies	Decides that users can have permission to access SALARY.XLSX
Data custodian/steward	Individual to whom day-to-day actions have been assigned by the owner	Periodically reviews security settings and maintains records of access by end-users	Sets and reviews security settings on SALARY.XLSX
Data owner	Person responsible for the data	Determines the level of security needed for the data and delegates security duties as required	Determines that the file SALARY.XLSX can be read only by department managers
Data controller	Principal party for collecting the data	Acquire user's consent, store the data, and manage consent or revoking access	Gathers data for SALARY.XLSX and identifies where it is stored
Data processor	Proxy who acts on behalf of data controller	Person or agency that holds and processes personal data for a third party but does not make decisions about using the data and is not responsible for the data	Manages SALARY.XLSX file on behalf of data controller

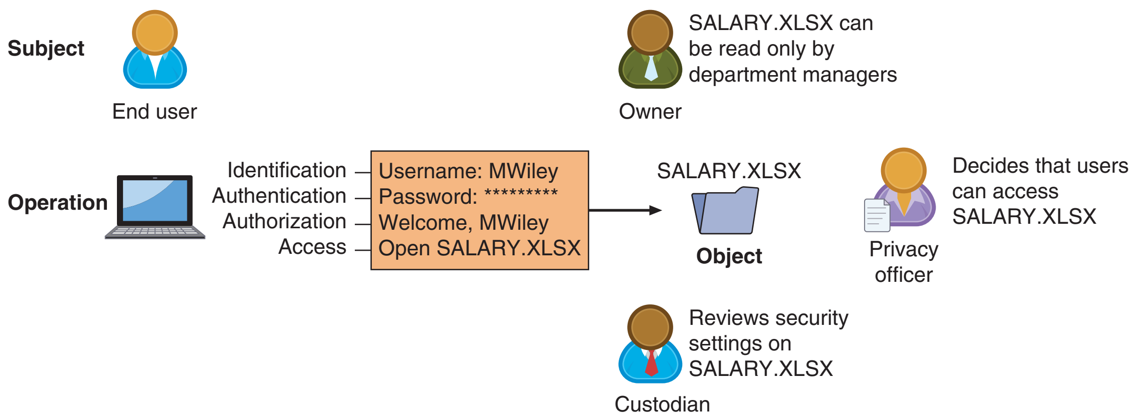


Figure 13-1 Technical access control roles and terminology

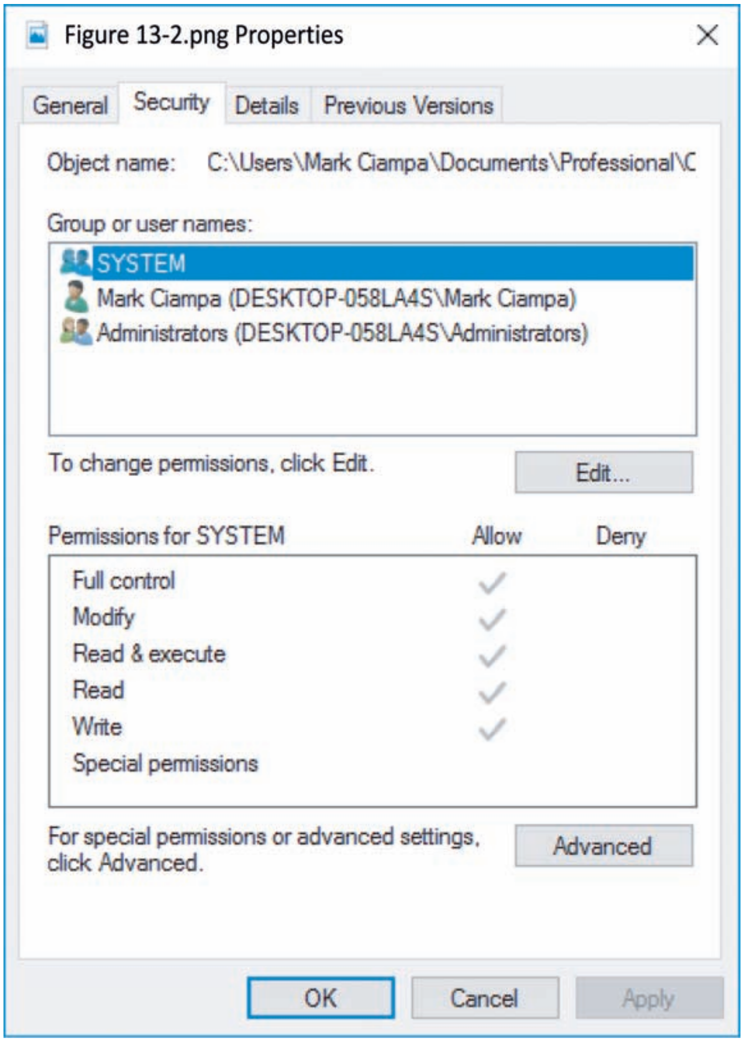
However, this job is made easier by the fact that the hardware and software have a predefined framework that the custodian can use for controlling access. This framework, called an **access control scheme**, is embedded in the software and hardware. The custodian/steward can use the appropriate scheme to configure the necessary level of control. Using these schemes is part of **privileged access management**, which is the technologies and strategies for controlling elevated (privileged) access and permissions.

NOTE 3

Access control schemes are variously referred to as access control models, methods, modes, techniques, or types. They are used by data custodians/stewards for access control but are neither created nor installed by them. Instead, these schemes are already part of the software and hardware.

There are five major access control schemes: Discretionary Access Control, Mandatory Access Control, Role-Based Access Control, Rule-Based Access Control, and Attribute-Based Access Control. Although the schemes can be used to help mitigate a threat actor's attempts at privilege elevation, they still have weaknesses and often result in cybersecurity incidences.

Discretionary Access Control (DAC) The **Discretionary Access Control (DAC)** scheme is the least restrictive. With the DAC scheme, every object has an owner, who has total control over that object. Most importantly, the owner has discretion (the choice) as to who can access the owner's objects and can grant permissions to other subjects over these objects. DAC is used on major operating systems (OSs). Figure 13-2 illustrates the DAC that a Microsoft Windows owner has over an object. These controls can be configured so that another user can have full or limited access over a file, printer, or other object.



Used with permissions from Microsoft

Figure 13-2 Windows Discretionary Access Control (DAC)

DAC has two significant weaknesses. First, although it gives a degree of freedom to the subject, DAC poses risks in that it relies on decisions made by the user to set the proper level of security. As a result, incorrect permissions might be granted to a subject or permissions might be given to an unauthorized subject. A second weakness is that a subject's permissions will be "inherited" by any programs that the subject executes. Threat actors often take advantage of this inheritance because users frequently have a high level of privileges. Malware downloaded onto a user's computer that uses the DAC scheme would then run at the same high level as the user's privileges.

Mandatory Access Control (MAC) The opposite of DAC is the most restrictive access control scheme, **Mandatory Access Control (MAC)**. MAC assigns users' access controls strictly according to the custodian's desires. This is considered the most restrictive access control scheme because the user has no freedom to set any controls or distribute access to other subjects. **SEAndroid**, which is a security-enhanced version of the Android operating system, uses MAC.

There are two key elements to MAC:

- *Labels*. In a system using MAC, every entity is an object (laptops, files, projects, and so on) and is assigned a classification label. These labels represent the relative importance of the object, such as *confidential, secret*, and *top secret*. Subjects (users, processes, and so on) are assigned a privilege label (sometimes called a *clearance*).
- *Levels*. A hierarchy based on the labels is also used, both for objects and subjects. *Top secret* has a higher level than *secret*, which has a higher level than *confidential*.

MAC grants permissions by matching object labels with subject labels based on their respective levels. To determine if a file can be opened by a user, the object and subject labels are compared. The subject must have an equal or greater level than the object in order to be granted access. For example, if the object label is *top secret*, yet the subject has only a lower *secret* clearance, access is denied. Subjects cannot change the labels of objects or other subjects to modify the security settings.

NOTE 4

In the original MAC scheme, all objects and subjects were assigned a numeric access level and the access level of the subject had to be higher than that of the object for access to be granted. For example, if EMPLOYEES.XLSX was assigned Level 500 while SALARIES.XLSX was assigned level 700, then a user with an assigned level of 600 could access EMPLOYEES.XLSX (Level 500) but not SALARIES.XLSX (Level 700). This scheme was later modified to use labels instead of numbers.

Microsoft Windows uses a MAC implementation called *Mandatory Integrity Control (MIC)* that ensures data integrity by controlling access to securable objects. A *security identifier (SID)* is a unique number issued to the user, group, or session. Each time a user logs in, the system retrieves the SID for that user from the database and then uses that SID to identify the user in all subsequent interactions with Windows security. Windows links the SID to an *integrity level.* Objects such as files, processes, services, and devices are assigned integrity levels—*low*, *medium*, *high*, and *system*—that determine their levels of protection or access. To write to or delete an object, the integrity level of the subject must be equal to or greater than the object's level. This ensures that processes running with a low integrity level cannot write to an object with a medium integrity level. MIC works in addition to Windows DAC: Windows first checks any requests against MIC, and if they pass, it checks DAC.

This can be seen in practice through a Windows feature known as *User Account Control (UAC)*. The standard user (lower level) who attempts to install software (higher level) is first required by UAC to enter the higher-level administrative password before being allowed to proceed (which elevates the action to the higher level). As an additional check, an administrative user also must confirm the action (yet does not need to enter the administrative password). In this way, UAC attempts to match the subject's privilege level with that of the object.

NOTE 5

By default, Windows switches to "Secure Desktop mode" when the UAC prompt appears. Secure Desktop mode allows only trusted processes with the integrity level *System* to run, which prevents malware from "spoofing" what appears on the screen to trick users. Secure Desktop mode is similar to what appears when a Windows login screen appears or the keystroke combination Ctrl+Alt+Delete is pressed. In Secure Desktop mode, users cannot click any icon other than the Windows prompt.

Role-Based Access Control The third access control scheme is **Role-Based Access Control (RBAC)**, sometimes called *Non-Discretionary Access Control*. RBAC is considered a more "real-world" access control than the other schemes because the access under RBAC is based on a user's job function within an organization. Instead of setting permissions for each user or group, the RBAC scheme assigns permissions to particular roles in the organization and then assigns users to those roles. Objects are set to be a certain type, to which subjects with that particular role have access. For example, instead of creating a user account for Ahmed and assigning specific privileges to that account, the role

Business_Manager can be created based on the privileges an individual in that job function should have. Ahmed and all other business managers in the organization can then be assigned to that role. The users and objects inherit all the permissions for the role.

Rule-Based Access Control The **Rule-Based Access Control** scheme, also called the *Rule-Based Role-Based Access Control (RB-RBAC)* scheme or *automated provisioning*, can dynamically assign roles to subjects based on a set of rules defined by a custodian (called **conditional access**). Each resource object contains a set of access properties based on the rules. When a user attempts to access that resource, the system checks the rules contained in that object to determine if the access is permissible.

Rule-Based Access Control is often used for managing user access to one or more systems, where business changes may trigger the application of the rules that specify access changes. For example, a subject on Network A wants to access objects on Network B, which is located on the other side of a router. This router contains the set of access control rules and can assign a certain role to the user, based on the network address or protocol, which will then determine whether the user will be granted access. Similar to MAC, Rule-Based Access Control cannot be changed by users. All access permissions are controlled based on rules established by the custodian or system administrator.

Attribute-Based Access Control While the Rule-Based Access Control scheme uses predefined rules, **Attribute-Based Access Control (ABAC)** uses more flexible policies that can combine attributes. These policies can take advantage of many types of attributes, such as object attributes, subject attributes, and environment attributes. ABAC rules can be formatted using an *If-Then-Else* structure, so that a policy can be created such as *If this subject has the role of manager, then grant access; else deny access.*

NOTE 6

ABAC systems can also enforce both DAC and MAC schemes.

Table 13-3 summarizes the features of the five access control schemes.

Table 13-3 Access control schemes

Name	Explanation	Description
Mandatory Access Control (MAC)	End-user cannot set controls	Most restrictive scheme
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive scheme
Role-Based Access Control (RBAC)	Assigns permissions to particular roles in the organization and then users are assigned to roles	Considered a more "real-world" approach
Rule-Based Access Control	Dynamically assigns roles to subjects based on a set of rules defined by a custodian	Used for managing user access to one or more systems
Attribute-Based Access Control (ABAC)	Uses policies that can combine attributes	Most flexible scheme

Access Control Lists (ACLs) An **access control list (ACL)** is a set of permissions that is attached to an object. This list specifies which subjects are allowed to access the object and what operations they can perform on it. When a subject requests permission to perform an operation on an object, the system checks the ACL for an approved entry in order to decide if the operation is allowed.

Although ACLs can be associated with any type of object, these lists are most often viewed in relation to files maintained by the OS. All OSs use a *filesystem*, which is a method for storing and organizing computer files to facilitate access. ACLs provide **filesystem permissions** for protecting files managed by the OS. ACLs have also been ported to SQL and relational database systems so that ACLs can provide database security as well.

NOTE 7

ACLs are the oldest and most basic form of access control. These became popular in the 1970s with the growth of multiuser systems, particularly UNIX systems, when it became necessary to limit access to files and data on shared systems. Later, as multiuser operating systems for personal use became popular, the concept of ACLs was added to them. Today all major OS make use of ACLs at some level.

Although widely used, ACLs have limitations. First, using ACLs is not efficient. The ACL for each file, process, or resource must be checked every time the resource is accessed. ACLs control not only user access to system resources but also application and system access. This means that in a typical computing session, ACLs are checked whenever a user accesses files, when applications are opened (along with the files and applications those applications open and modify), when the operating system performs certain functions, and so on. A second limitation to ACLs is that they can be difficult to manage in an enterprise setting where many users need to have different levels of access to many different resources. Selectively adding, deleting, and changing ACLs on individual files, or even groups of files, can be time consuming and open to errors, particularly if changes must be made frequently.

Preparing for an Incident

Due to weak account types, poor access control, and other vulnerabilities that lead to successful attacks, it is important to prepare in advance for an incident. The steps to take in preparation are creating an incident response plan, performing exercises, and studying attack frameworks.

Creating an Incident Response Plan

System weaknesses that lead to successful attacks mean that a formal plan of action is essential. An **incident response plan** is a set of written instructions for reacting to a security incident. Without such a plan, enterprises are at risk of being unable to quickly identify the attack, contain its spread, recover, and learn from the attack to improve defenses.

The six action steps to be taken when an incident occurs, called the **incident response process**, also make up the six elements of an incident response plan. These are listed in Table 13-4.

Table 13-4 Incident response process

Action step	Description
Preparation	Equipping IT staff, management, and users to handle potential incidents when they arise
Identification	Determining whether an event is actually a security incident
Containment	Limiting the damage of the incident and isolating those systems that are impacted to prevent further damage
Eradication	Finding the cause of the incident and temporarily removing any systems that may be causing damage
Recovery	After ensuring no threat remains, permitting affected systems to return to normal operation
Lessons learned	Completing incident documentation, performing detailed analysis to increase security and improve future response efforts

At a minimum, an incident response plan should contain the following information:

- *Documented incident definitions*. The plan should provide clear descriptions of the types and categories of documented incident definitions, which outline in detail what is—and is not—an incident that requires a response.
- *Incident response teams*. An **incident response team** is responsible for responding to security incidents. In addition to technical specialists who can address specific threats, it should also include members who are public relations employees and managers who can guide enterprise executives on appropriate communication. Each member should have clearly designated duties, roles, and responsibilities in the team.

- *Reporting requirements/escalation*. The reporting requirements/escalation indicates to whom information should be distributed and at what point the security event has escalated to the degree that specific actions should be implemented.
- *Retention policy*. A **retention policy** as part of an incident response plan outlines how long the evidence of the incident should be retained. This policy should also consider the costs associated with the retention.
- *Stakeholder management*. An incident response plan must identify the relevant stakeholders within the organization who need to be initially informed of an incident and then kept up to date. Known as **stakeholder management**, it includes areas such as operations, legal, technical, finance, and even human resources.
- *Communication plan*. A **communication plan** outlines the internal and external constituents who need to be informed of an incident, how they should be informed, and when communication should take place. Depending upon the size of the organization, the communications staff may be charged with this task, but the details should be contained in the communication plan. Because the communications staff are professionals in this area, using the staff instead of members of the incident response team helps to ensure consistent messaging that complies with business requirements, including with respect to the public, investors, affected individuals or customers, and employee communications within the organization.

NOTE 8

A communication plan will usually require coordination with the legal team to ensure that the communications comply with all applicable legal requirements.

Performing Exercises

An incident response plan must be tested by conducting simulated **exercises** to make necessary adjustments. The types of exercises are summarized in Table 13-5.

Table 13-5 Incident response exercises

Exercise Name	Description	Example
Tabletop	A monthly 30-minute discussion of a scenario conducted in an informal and stress-free environment.	This scenario is presented: An employee casually remarks about how generous it is of a vendor to provide the box of USB drives on the conference room table, embossed with the company logo. After making some inquiries, you find the vendor did not provide USB drives to employees. What do we now do?
Walkthrough	A review by IT personnel of the steps of the plan by paying particular attention to the IT systems and services that may be targeted in an attack.	A technician with knowledge of the current system will walk through the proposed recovery procedures to determine if there are omissions, gaps, errors, or false assumptions.
Simulation	A hands-on simulation exercise using a realistic scenario to thoroughly test each step of the plan.	A simulation of a senior vice president who opens a malicious attachment and introduces malware into the network is presented.

NOTE 9

During the first few months of the COVID-19 pandemic, many medical professionals around the world who were active in combating the disease participated online in a tabletop game called Pandemic. The players collaborated (not competed) to contain outbreaks around the world and search for cures. Each player chose a role like scientist, researcher, or medic, each with unique abilities, and had to work together to develop cures before the diseases overwhelmed them. Many medical professions reported that playing the game was therapeutic and a boost to morale.

Studying Attack Frameworks

Just as a cybersecurity framework, or series of documented processes, can be used to define policies and procedures for implementing and managing security controls in an enterprise environment, frameworks about how attacks occur can also be studied. These **exploitation frameworks** serve as models of the thinking and actions of today's threat actors.

NOTE 10

Frameworks are covered in Module 2.

Three common attack frameworks include the following:

- *MITRE ATT&CK*. **MITRE ATT&CK** is a knowledge base of attacker techniques that have been broken down and classified in detail. The attacks are offensively oriented actions that can be used against particular platforms. The focus of ATT&CK is not on the tools and malware that attackers use but on how they interact with systems during an operation. These techniques are arranged into a set of tactics to help explain and provide context for the technique. Figure 13-3 displays a sample of the ATT&CK framework.

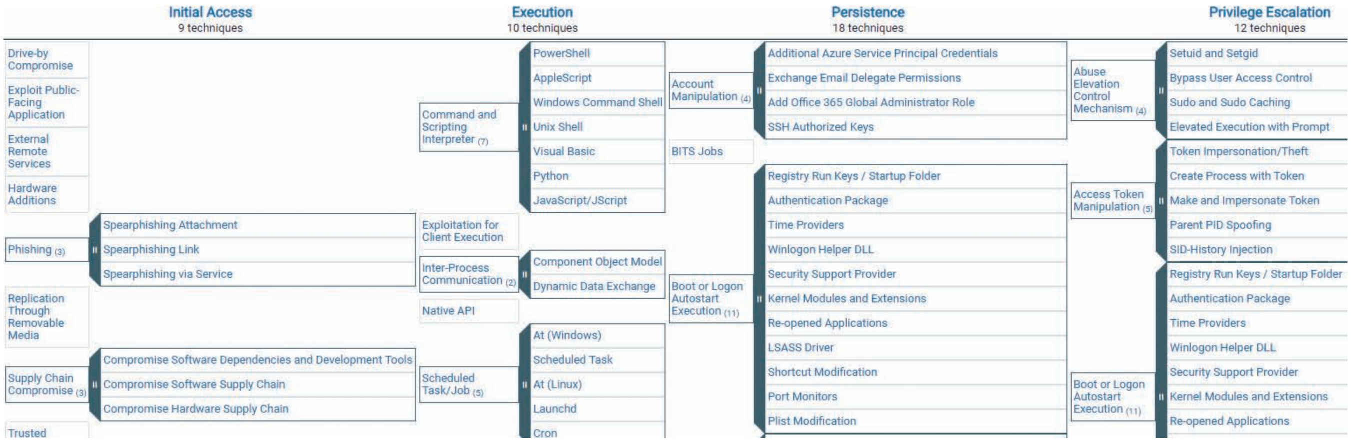
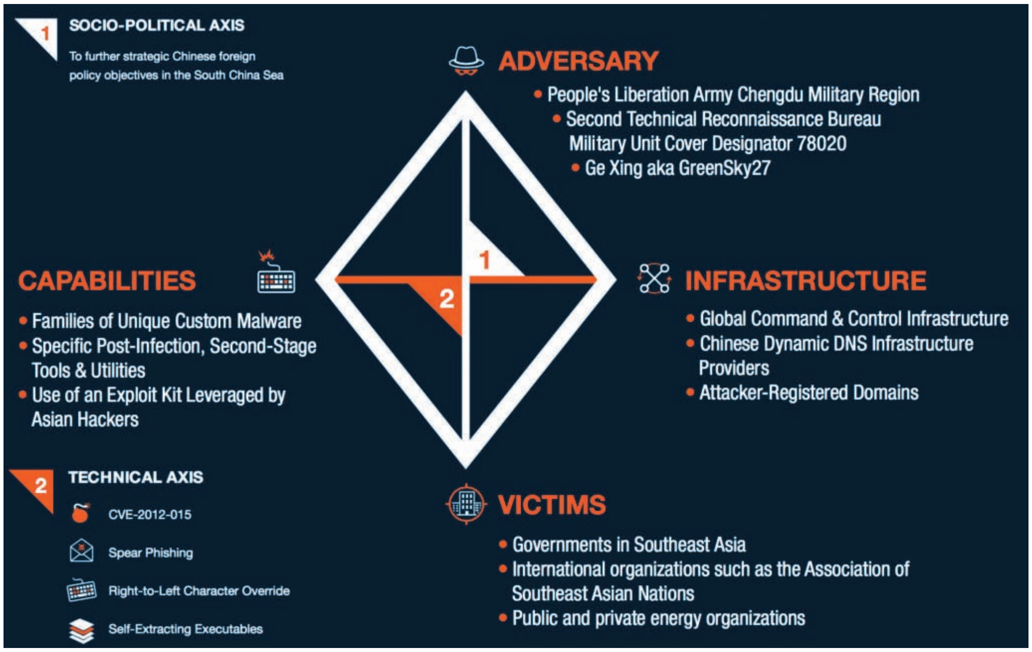


Figure 13-3 MITRE ATT&CK framework

Source: The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation

- *The Diamond Model of Intrusion Analysis*. The **Diamond Model of Intrusion Analysis** is a framework for examining network intrusion events. This framework derives its name and shape from the four core interconnected elements that comprise any event: adversary, infrastructure, capability, and victim. Analyzing security incidents involves piecing together the Diamond using information collected about these four facets to understand the threat in its full context. Figure 13-4 illustrates the Diamond Model.



Source: ThreatConnect, Inc

Figure 13-4 Diamond Model of Intrusion Analysis

- *Cyber Kill Chain*. A *kill chain* is a military term used to describe the systematic process to target and engage an enemy. An attacker who attempts to break into a web server or computer network actually follows these same steps. Known as the **Cyber Kill Chain**, it outlines the steps of an attack. Figure 13-5 shows the Cyber Kill Chain. The underlying purpose of the Cyber Kill Chain is to illustrate that attacks are an integrated and end-to-end process like a "chain." Disrupting any one of the steps will interrupt the entire attack process, but the ability to disrupt the early steps of the chain is the most effective and least costly.

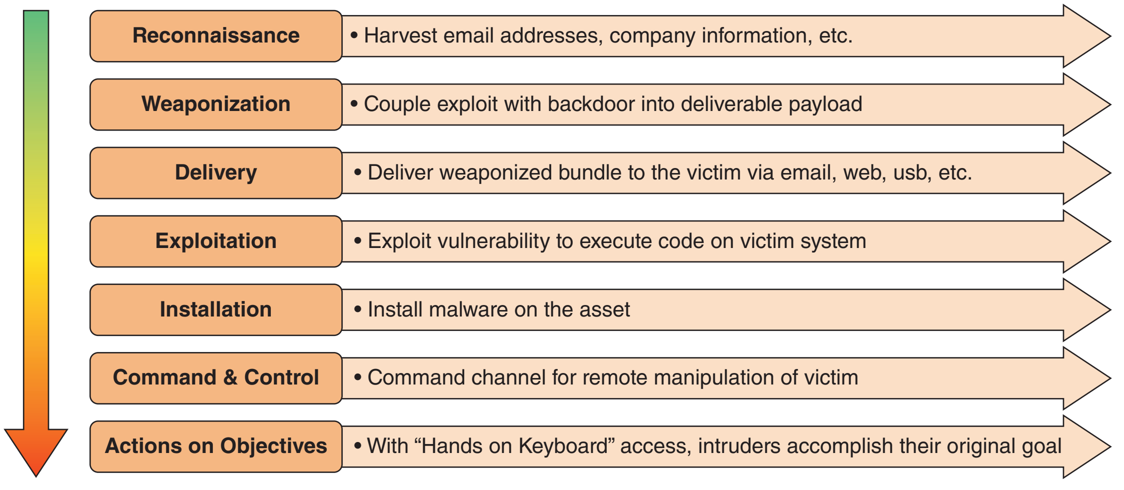


Figure 13-5 Cyber Kill Chain

NOTE 11

The Cyber Kill Chain was first introduced by researchers at Lockheed Martin in 2011, which later trademarked the term, "Cyber Kill Chain."

TWO RIGHTS & A WRONG

1. Any shared account (an account used by more than one user), generic account (an account not tied to a specific person), or guest account (given to temporary users) should be prohibited.
2. A data privacy officer (DPO) is someone to whom day-to-day actions have been assigned by the owner.
3. An access control scheme is embedded in the software and hardware.

See Appendix B for the answer.

INCIDENT RESPONSE

CERTIFICATION

2.1 Explain the importance of security concepts in an enterprise environment.

4.4 Given an incident, apply mitigation techniques or controls to secure an environment.

Several important steps should be taken when responding to an incident in order to recover from it (called **response and recovery controls**). In general, these steps include taking advantage of SOAR runbooks and playbooks, performing containment, and making configuration changes.

Use SOAR Runbooks and Playbooks

A Security Orchestration, Automation, and Response (SOAR) product can help security teams manage and respond to security warnings and alarms. By combining more comprehensive data gathering and analytics to automate incident response, a SOAR allows a security team to automate incident responses.

NOTE 12

SOARs are covered in Module 2.

Two elements that are closely associated with using SOARs are a SOAR playbook and a runbook. A **playbook** is a linear-style checklist of required steps and actions needed to successfully respond to specific incident types and threats. These playbooks give a top-down step-by-step approach to incident response by establishing formalized incident response processes and procedures. A playbook can help ensure that required steps are systematically followed, particularly when it is necessary to comply with regulatory frameworks. Although playbooks support both human tasks and automated actions, most organizations use playbooks to document processes and procedures that rely heavily on manual tasks, such as breach notification or malware reverse engineering.

A **runbook** is a series of automated conditional steps (like threat containment) that are part of an incident response procedure. Whereas a playbook focuses more on manual steps to be performed, a runbook is usually actions that are performed automatically. These automated responses can help to speed up the assessment and containment of incidences. While runbooks can also include human decision making as required, generally, however, most runbooks are automated action-based steps.

CAUTION Playbooks are not exclusively manual procedures, nor are runbooks exclusively automated procedures. However, playbooks are predominantly manual while runbooks are mostly automated.

Most SOAR platforms have different pre-configured “out-of-the-box” playbooks that are based on industry best practices and recognized standards. These playbooks identify and automate responses to frequent enterprise incidents, including phishing, compromised accounts, and malware. Organizations can craft their own customized playbooks, which are more simplified or advanced than pre-configured playbooks. This gives the organization freedom to react to an incident that is in accordance with regulations or compliance measures that more directly apply to them.

NOTE 13

Playbooks can be customized to enforce role-based security requirements that require authorization for containment.

Used together, runbooks and playbooks provide organizations with streamlined methods for orchestrating incident response and to document different security processes. Multiple runbooks and playbooks can even be assigned to a single incident so that the correct type and level of automation and orchestration can be delivered.

Perform Containment

One of the most critical steps in incident response is limiting the spread of the attack (containment). However, containment can be most effective when the network has been properly designed. A secure network design takes advantage of network *segmentation* based upon the principle of zero trust, which is a strategic initiative about secure network design. Network segments (sometimes called IP ranges, security groups, subnets, or network zones) can be created based on business units, locations, or the level of sensitivity of the network data. Network administrators can use access controls to configure services that are allowed between different zones.

NOTE 14

Network segmentation and zero trust are covered in Module 9.

Although important, network segmentation only restricts attackers by limiting access to other parts of the network. When an incident occurs, **isolation** is then used to segregate both the attacker and the infected systems from reaching other devices. During isolation, the compromised systems are either disconnected or disabled until the incident is resolved.

Make Configuration Changes

To neutralize the attacker, limit the spread of the attack, and prevent additional successful incidents, it may be necessary to make configuration changes to devices and processes. Configuration changes may need to be applied to the following:

- Firewall rules
- Content/URL filters
- Digital certificates
- Data loss prevention settings
- Mobile device management settings

TWO RIGHTS & A WRONG

1. A runbook is a linear-style checklist of required steps and actions required to successfully respond to specific incident types and threats.
2. SOAR platforms have different pre-configured playbooks that are based on industry best practices and recognized standards.
3. When an incident occurs, isolation is then used to segregate both the attacker and the infected systems from reaching other devices.

See Appendix B for the answer.

INCIDENT INVESTIGATION

CERTIFICATION

4.1 Given a scenario, use the appropriate tool to assess organizational security.

4.3 Given an incident, utilize appropriate data sources to support an investigation.

4.5 Explain the key aspects of digital forensics.

Following a cybersecurity incident, it must be fully investigated. The investigation is to not only pinpoint how it occurred so that future incidents can be prevented but also for regulatory compliance reporting. Incident investigation involves analyzing data sources and performing a digital forensics investigation.

Data Sources

Several sources of data can provide helpful clues in uncovering how an incident occurred. These data sources include log files and data from other sources.

Log Files

Using data from log files involves identifying log file sources, collecting data, and analyzing data.

Types of Logs A **log** is a record of events that occur. Security logs are particularly important for an incident investigation because they can reveal the type of attack that was directed at the network and how it successfully circumvented existing security defenses. Network-based device logs that provide the most beneficial security data for an investigation, in order of importance, are listed in Table 13-6.

Table 13-6 Network device log sources

Device	Explanation
Firewalls	Firewall logs can be used to determine whether new IP addresses are attempting to probe the network and if stronger firewall rules are necessary to block them. Outgoing connections, incoming connections, denied traffic, and permitted traffic should all be recorded.
Network intrusion detection systems (NIDS) and network intrusion prevention systems (NIPS)	Intrusion detection and intrusion prevention systems record detailed security log information on suspicious behavior as well as any attacks that are detected. In addition, these logs also record any actions NIPS used to stop the attacks.
Web servers	Web servers are usually the primary target of attackers. These logs can provide valuable information about the type of attack that can help in configuring good security on the server.
DHCP servers	DHCP server logs can identify new systems that mysteriously appear and then disappear as part of the network. They can also show what hardware device had which IP address at a specific time.
VPN concentrators	VPN logs can be monitored for attempted unauthorized access to the network.
Proxies	As intermediate hosts access websites, these devices keep a log of all URLs that are accessed through them. This information can be useful when determining if a zombie is "calling home."
Domain Name System (DNS)	A DNS log can create entries in a log for all queries that are received. Some DNS servers also can create logs for error and alert messages.
Email servers	Email servers can show the latest malware attacks that are being launched through the use of attachments.
Routers and switches	Router and switch logs provide general information about network traffic.

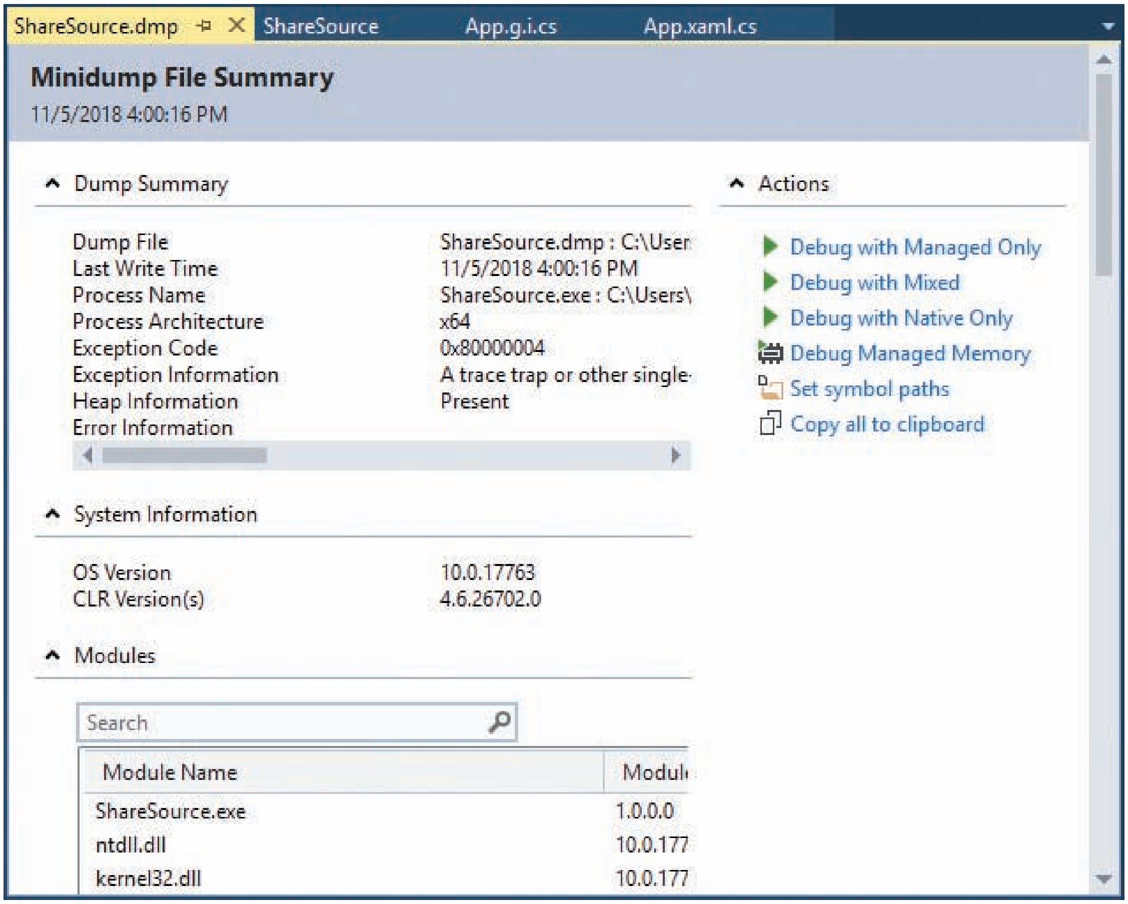
Different system log files should also be investigated. Particular interest should be directed at **authentication servers** that facilitate authentication of an entity that attempts to access a network, such as a user or another server. Authentication servers provide valuable information about failed authentication attempts and brute force attacks.

In addition, application log files can give information about attacks focused on different applications. If an application log identifies an app that has been the source of a compromise, software can be used to create a **dump file**, which is a snapshot of the process that was executing and any modules that were loaded for an app at a specific point in time. Dump file output is seen in Figure 13-6.

Log files that relate to voice and video communication should not be overlooked. Vulnerabilities in these services are often compromised to allow attackers to pivot to other resources. **Session Initiation Protocol (SIP)** is a signaling protocol used to create "sessions" between multiple participants and is widely found in voice telephony products. A **call manager** is a platform used to provide telephony, video, and web conferences. Voice over IP (VoIP) is the convergence of voice and data traffic over a single Internet Protocol (IP) network. Each of these produces valuable log files.

NOTE 15

VoIP is covered in Module 5.



Source: ShareSource

Figure 13-6 Dump file output

Collection and Analysis Several problems are associated with *log management*—or transmitting, collecting, analyzing, and disposing of log data. This is due to the following:

- *Multiple devices generating logs*. As noted, virtually every network device, both standard network devices and network security devices, can create logs. Each device may interpret an event in a different context, so that a router looks at a single event differently than a firewall does. This can create a confusing mix of log data.
- *Very large volume of data*. Because each device generates its own data, a very large amount of data can accumulate in a very short period of time. In addition, many devices record all events, even those that are not security related, which increases the amount of data that is generated. Filtering through this large volume of data can be overwhelming.
- *Different log formats*. Perhaps the biggest obstacle to log management is that different devices record log information in different formats and even capture different data. Combining multiple logs, each with a different format, can be a major challenge.

There are different solutions to these problems. These are listed in Table 13-7.

Table 13-7 Log management tools

Solution	Description
syslog	syslog (system logging protocol) is a standard to send system log or event messages to a server.
nxlog	nxlog is a multi-platform log management tool and supports various platforms, log sources, and formats.
rsyslog	rsyslog (rocket-fast system for log processing) is an open source utility for forwarding log messages in an IP network on UNIX devices.
syslog-ng	syslog-ng is an open source utility for UNIX devices that includes content filtering.
journalctl	journalctl is a Linux utility for querying and displaying log files.

NOTE 16

The question of how long a log file should be retained depends on several different factors, including regulatory compliance and organizational policy. Generally, logs that provide evidence of an incident should be retained for at least one year.

Other Data Sources

Data accumulated from various other sources can also provide useful information. These include the following:

- *IP monitors*. Various IP software monitors can provide insight into an incident. **NetFlow** is a session sampling protocol feature on Cisco routers that collects IP network traffic as it enters or exits an interface and uses TCP/IP Internet Control Message Protocol (ICMP) **Echo** request packets, while **sFlow** is a packet sampling protocol that gives a statistical sampling instead of the actual flow of packets. **IPFIX (IP Flow Information Export)** is similar to NetFlow but with additional capabilities, such as integrating Simple Network Management Protocol (SNMP) information directly into the IPFIX information so that all the information is available instead of requiring separate queries to the SNMP server.
- *Metadata*. **Metadata** is "data about data," or data that describes information about other data. Analyzing file, web, mobile, and email metadata can give clues regarding an attack.
- *Analyzers*. Other types of monitors and analyzers that provide useful information are bandwidth monitors and protocol analyzers.
- *Vulnerability scans*. Data from a vulnerability scan and Security Information and Event Management (SIEM) products that consolidate real-time security monitoring and management of security information with analysis and reporting of security events is useful. A SIEM dashboard can provide information collected from its sensors. This information includes alerts, trends, sensitivity, and correlation data.

NOTE 17

Vulnerability scans and SIEMs are covered in Module 2.

Digital Forensics

Digital forensics is an important element in incident investigation. In fact, many users equate incident investigation with digital forensics, although they are not exactly the same: forensics is one important part of incident investigation. Understanding digital forensics involves knowing what it is, the procedures for forensics, tools that are used, and the difference between on-prem and cloud forensics.

What Is Forensics?

Forensics, also known as *forensic science*, is the application of science to questions that are of interest to the legal profession. While most users associate forensics with analyzing evidence from a murder scene, it also can be applied to technology. Digital forensics uses technology to search for evidence pertaining to a cybercrime or damage that occurred during a cyber incident. Digital evidence can be retrieved from computers, mobile devices, cell phones, digital cameras, and virtually any device that has a processor, memory, or storage.

Forensics Procedures

When responding to an incident that requires an examination using computer forensics, five basic steps are followed, which are similar to those of standard forensics. The steps are secure the crime scene, preserve the evidence, document the chain of custody, examine the evidence, and enable recovery.

Secure the Scene When an on-prem illegal or unauthorized incident occurs that involves technology, action must be taken immediately. A delay of even a few minutes can allow digital evidence to be overwritten in the normal function of the device, become contaminated by other users, or give the perpetrator time to destroy the evidence.

When an incident occurs, those individuals in the immediate vicinity should perform *damage control*, which is the effort to minimize any loss of evidence. The steps in damage control include contacting the incident response team, securing and then quarantining the electronic equipment involved, and, if necessary, reporting the incident to the appropriate external authorities.

Once the incident response team arrives, its first job is to secure the scene, which includes the following actions:

- The physical surroundings of the device computer should be clearly documented. Many forensics experts use a video camera to capture video of all the work performed by the incident response team to demonstrate that proper procedures were followed.
- Photographs of the area should be taken before anything is touched to help document that the computer was working prior to the attack. (Some defense attorneys have argued that a computer was not functioning properly, and, thus, the attacker could not be held responsible for any damages.) The device should be photographed from several angles, including the images displayed on the screen. Because digital pictures can be altered, some security professionals recommend that photographs be taken with a standard camera using film.
- Any cables connected to a device should be labeled to document the hardware components and how they are connected.
- The team should take custody of the device along with any peripherals. In addition, USB flash drives and any other media must be secured.
- The team must speak with those present to perform witness interviews and everyone who had access to the system and document their findings, including what those people were doing with the system, what its intended functions were, and how it has been affected by the unauthorized actions.

Preserve the Evidence The next task is **preservation of the evidence**, or ensuring that important proof is not corrupted or even destroyed. Preserving evidence can also help mitigate *nonrepudiation*, or a denial by the perpetrators that they were involved or did anything wrong.

Evidence from a suspected device should be placed in bags that have **tags** or identifying labels that have a description of the item, a numeric identifier, date, collection location, and other relevant information. These bags should then be sealed to serve as protection against evidence being altered. Two types of seals are commonly used. A tamper-evident seal is a seal or tape that cannot be removed and reapplied without leaving obvious visual evidence. If the seal or tape is lifted or removed, a clearly visible *OPENED* message appears on the packaging. For additional traceability and security, the tape is often labeled with a unique sequential number every 9 inches (22 centimeters). Tamper-evident tape is shown in Figure 13-7. A tamper-resistant seal is designed to deter tampering with the bag. However, it does not necessarily produce visual evidence if tampering has occurred: If the sticker is removed carefully, it can be reapplied with no visual evidence of tampering.

Source: American Casting MFG

Figure 13-7 Tamper-evident tape

Depending upon the type and severity of the incident, it may be necessary to immediately involve the judicial system to help collect and preserve the digital evidence. This ensures that the integrity of the evidence is maintained and can hold up in a court of law (**admissibility**). One of the first steps is **e-discovery**, which is identifying, collecting, and producing electronically stored information (ESI) in response to a request in an investigation or lawsuit. Once data has been identified, it can be placed under a **legal hold**, meaning that it cannot be modified, deleted, erased, or otherwise destroyed.

CAUTION There is a tendency to issue legal holds that are too broad in scope. For example, to place a legal hold on all email correspondence may result in retaining thousands or millions of unneeded messages and associated attachments, while placing a legal hold on all portable devices requiring them to be locked away makes them useless to the organization. Instead, appropriate filters should be used to capture only data that is relevant.

Document Chain of Custody As soon as the team begins its work, it must start and maintain a strict chain of custody. Documenting the evidence from the very beginning is called **provenance**. The **chain of custody** documents that the evidence was always under strict control and no unauthorized person was given the opportunity to corrupt the evidence. A chain of custody includes documenting all the serial numbers of the systems involved, who handled and had custody of the systems and for what length of time, how the computer was shipped, and any other steps in the process. In short, a chain of custody is a detailed document describing where the evidence was at all times from the beginning of the investigation.

CAUTION Gaps in a chain of custody can result in severe legal consequences. Courts have dismissed cases involving computer forensics because a secure chain of custody could not be verified.

A chain of custody form helps to document that evidence was under strict control at all times and no unauthorized person was given the opportunity to corrupt it, as shown in Figure 13-8.

Examine for Evidence When examining technology devices that may contain evidence, called **artifacts**, it is critical to follow a specific order. This is because different data sources have different degrees of preservation. An **order of volatility** must be followed to preserve the most fragile data first. Table 13-8 lists the order of volatility.

Table 13-8 Order of volatility

Order	Examples	Description
1	Registers and CPU cache	Registers and the CPU cache are extremely volatile and change constantly.
2	Routing tables, ARP cache, process table, kernel statistics, RAM	The network routing and process tables have data located on network devices that can change quickly while the system is in operation, and kernel statistics are moving between cache and main memory, which make them highly volatile. RAM information can be lost if power is lost.
3	Temporary filesystems	Temporary filesystems are not subject to the degree of rapid changes as the prior elements.
4	Hard drive	Hard drive data is relatively stable.
5	Remote logging and monitoring data	Although remote logging and monitoring is more volatile than hard drive data, the data on a hard drive is considered more valuable and should be preserved first.
6	Physical configuration and network topology	These items are not considered volatile and do not have a significant impact on an investigation.
7	Archival media	Data that has been preserved in archival form is not volatile.

Property Record Number: ______________

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: ______________ Offense: ______________
Submitting Official: (Name/ID#) ______________
Date/Time Seized: ______________ Location of Seizure: ______________

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

Final Disposal Authority

Item(s) #: ________ on this document pertaining to (suspect): ______________
is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)
☐ Return to Owner ☐ Auction/Destroy/Divert
Name & ID# of Authorizing Official: ______________ Signature: ______________ Date: ________

Witness to Destruction of Evidence

Item(s) #: ________ on this document were destroyed by Evidence Custodian ______________ ID#:_____
in my presence on (date) ______________.
Name & ID# of Witness to destruction: ______________ Signature: ______________ Date: ________

Release to Lawful Owner

Item(s) #: ________ on this document was/were released by Evidence Custodian
______________ ID#:________ to
Name ______________
Address: ______________ City: ______________ State: ______ Zip Code:
____
Telephone Number: (_____) ______________
Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: ______________ Date: ______________

Copy of Government-issued photo identification is attached. ☐ Yes ☐ No

This Evidence Chain-of-Custody form is to be retained as a permanent record.

Figure 13-8 Chain of custody form

The first two levels are considered the most volatile because they can change very quickly. A **cache** is a type of high-speed memory that stores recently used information so that it can be quickly accessed again at a later time. Both the CPU and ARP caches can easily change and should be captured immediately. To facilitate this, there are tools that allow capturing the system image, or a **snapshot** of the current state of these elements that contains all current settings and data. On the other hand, data that is stored in a less volatile state, such as **OS event logs** that document incorrect login attempts, system setting modifications, application or system failures, and other events can be retrieved after the most volatile data is secured.

After retrieving the volatile data, the team next focuses on the hard drive. A *mirror image backup*, also called a *bit-stream backup*, is an evidence-grade backup because its accuracy meets evidence standards. A mirror image backup is not the same as a normal copy of the data. Standard file copies or backups include only files. Mirror image backups replicate all sectors of a computer hard drive, including all files and any hidden data storage areas. Using a standard copy procedure can miss significant data and can taint the evidence. For example, copying a file may change file date information on the source drive, which is information that is often critical in a computer forensic investigation.

To guarantee the integrity of the data, mirror image backup programs rely upon *hashing algorithms* as part of the validation process. The digest of the original source data is compared against the digest of the copied data to help create a snapshot of the current system based on the contents of the drives. This is done to document that any retrieved evidence came from the system and was not "planted" there.

CAUTION Many resources that describe forensic hashing call it "creating a checksum." A hash and a checksum are very different and have different purposes, as explained in Module 6.

Two elements are frequently overlooked when performing a forensics investigation. A mirror image backup will capture the **swap file** or **pagefile** that contains data that has been moved from RAM to the hard drive due to a lack of RAM space, and this should be examined for evidence. A second element is **firmware**, or software in hardware. It is not uncommon for a threat actor to infect unprotected firmware as an entry point into a system.

Often clues are not obvious and must be mined and exposed. One source of hidden data is called *slack*. Windows computers use two types of slack. The first is RAM slack. Windows stores files on a hard drive in 512-byte blocks called sectors, and multiple sectors are used to make up a cluster. Clusters are made up of blocks of sectors. When a file that is being saved is not large enough to fill up the last sector on a disk (a common occurrence because a file size only rarely matches the sector size), Windows pads the remaining cluster space with data that is currently stored in RAM. This padding creates *RAM slack*, which can contain any information that has been created, viewed, modified, downloaded, or copied since the computer was last booted. Thus, if the computer has not been shut down for several days, the data stored in RAM slack can come from activity that occurred during that time. RAM slack is illustrated in Figure 13-9.

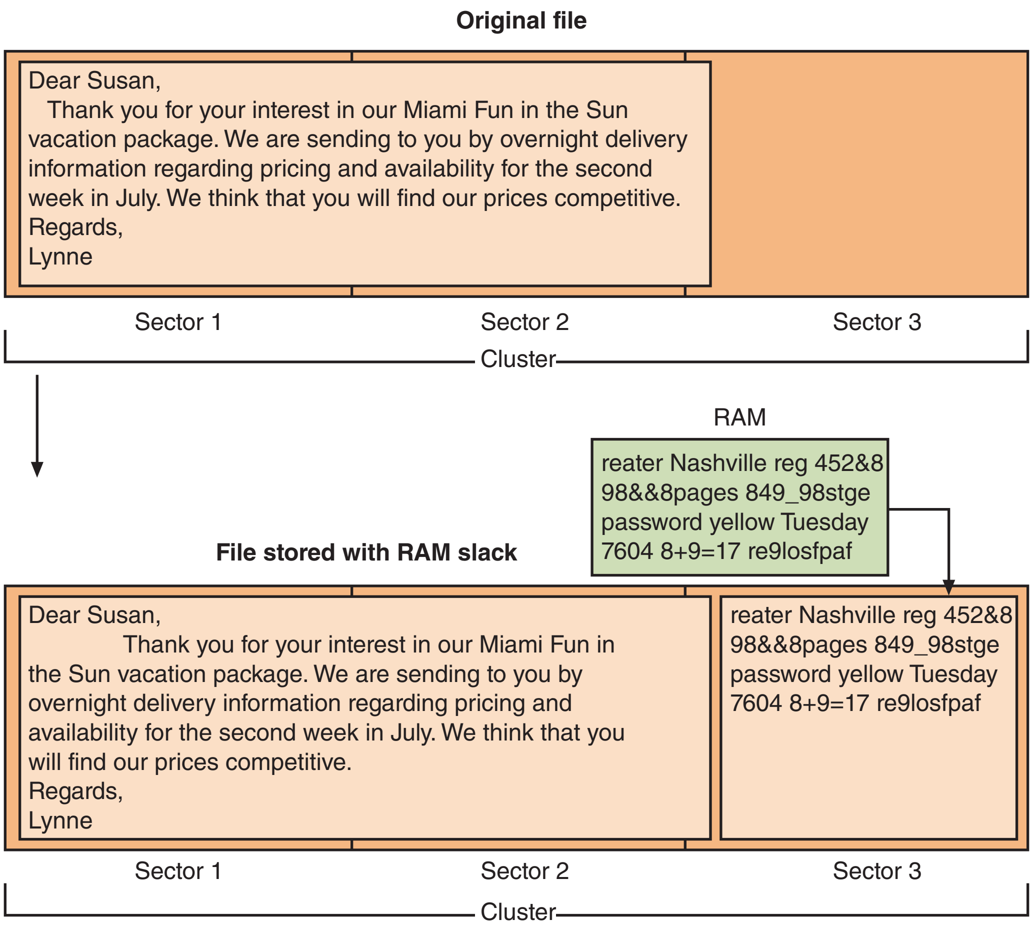


Figure 13-9 RAM slack

RAM slack pertains only to the last sector of a file. If additional sectors are needed to round out the block size for the last cluster assigned to the file, then a different type of slack is created. This is known as *drive file slack* (sometimes called *drive slack*) because the padded data that Windows uses comes from data stored on the hard drive. Such data could contain remnants of previously deleted files or data from the format pattern associated with disk storage space that has yet to be used by the computer. Drive file slack is illustrated in Figure 13-10. Both RAM slack and drive slack can hold valuable evidence.

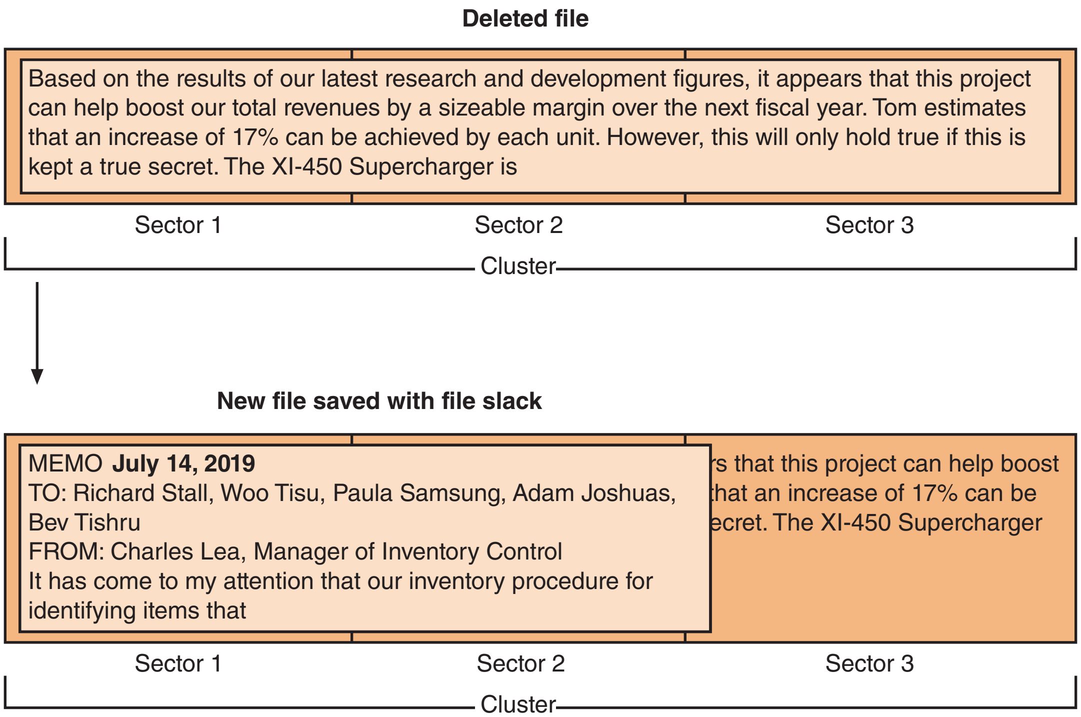


Figure 13-10 Drive file slack

An additional source of hidden clues can be gleaned from metadata. Some electronic files may contain hundreds of pieces of such information. Examples of metadata include the file type, authorship, and edit history. Another example of metadata is the date and time that a file was created or accessed. A **time stamp** is the recorded time that an event took place irrespective of the location of the endpoint. The **time offset** is the amount of time added to or subtracted from Coordinated Universal Time (UTC) to arrive at the current "actual" (called *civil*) time, which may be affected by daylight savings time and different regional time zones. However, different operating systems store time values differently. Microsoft Windows uses a 64-bit time stamp that counts the number of 100 nanosecond intervals that have occurred since January 1, 1601, at 00:00:00 Greenwich Mean Time (GMT). The Linux operating system uses a 32-bit time stamp that recognizes the number of seconds that have occurred since January 1, 1970, at 00:00:00 GMT. It is important when examining evidence to be aware of how the particular operating system stores time and record its time offset.

Upon completion of the examination, a detailed report is required that lists the steps that were taken and any evidence that was uncovered in the forensic investigation.

Enable Recovery A final analysis looks at recovering the data from the security event and the lessons that can be learned from it. The forensics procedures have gathered **strategic intelligence**, or the collection, processing, analysis, and dissemination of intelligence for forming policy changes. A more in-depth application of strategic intelligence is **strategic counterintelligence**, which involves gaining information about the attacker's intelligence collection capabilities.

Forensics Tools

There are different software and hardware forensics tools available for analysis.

Forensics Software Tools An *imaging utility* is used for generating a physical copy. A utility named **dd**, sometimes called GNU dd, is the oldest imaging tool still in use, primarily because it requires only minimal resources to run and generates raw image files that can be read by many other programs. However, dd is a command-line program and lacks some of the useful features found in more modern imagers, such as metadata gathering, error correction, and a user-friendly interface.

> **CAUTION** Because dd is a command-line program, it requires several ambiguous command-line arguments (*switches* or *flags*) to tailor the imaging command. Some of these arguments are similar and easily confused and can even result in destroying the source media being duplicated. Users should exercise extreme caution when using the dd utility.

Other popular forensics software tools are **memdump**, a Linux utility that "dumps" system memory; **WinHex**, a hexadecimal editor that can be used for forensics; and **Autopsy**, a digital forensics platform.

Products are available that package multiple tools into a single *suite* that has a common user interface and can more easily exchange information among the different tools. Two of the most common forensic suites are EnCase (shown in Figure 13–11) and **FTK Imager**.

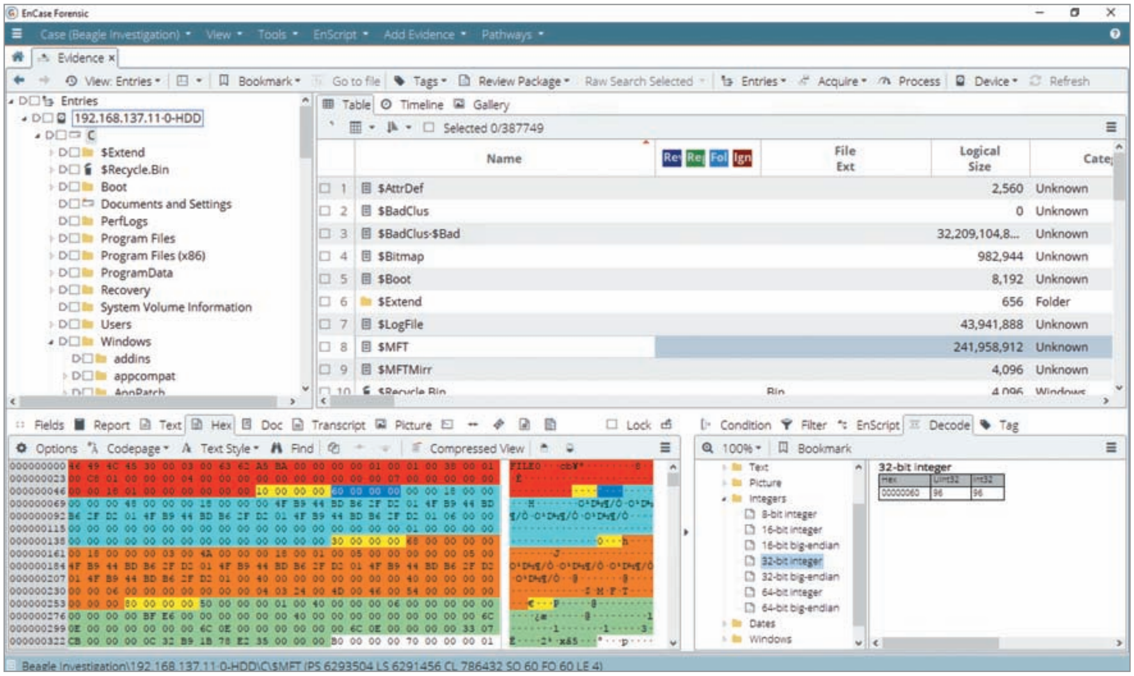


Figure 13-11 EnCase software

Source: Opentext

Forensics Hardware Tools Instead of gathering different forensics software tools, a digital forensic workstation, which is a computer that is specially configured to perform forensics activities, can be used instead. A digital forensic workstation is shown in Figure 13-12.

Digital forensic workstations are typically configured with the latest computer hardware, such as multiple gigabit network ports and USB ports, along with up to 10 drive "hot swap" bays to hold as many as eight drives. The two additional empty bays can be used for backups or additional processing, such as copying data directly to a network attached storage (NAS) device. These workstations also are configured with eight or more 6 TB hard drives configured in RAID 5 for redundancy, and they have 1000-watt power supply units, multiple fans for cooling, and the latest high-end CPUs.

NOTE 18

Digital forensic workstations are expensive. Depending on the options installed, such a workstation might cost more than $20,000.

Source: Teel Technologies

Figure 13-12 Digital forensics workstation

There are also specialized hardware tools for a forensics investigation. For example, a mobile device forensics tool is designed to perform forensics on smartphones, tablets, and other similar devices. Although mobile devices are sometimes characterized merely as "portable computers," they actually contain a broader wealth of information than a desktop or laptop computer. Mobile devices are almost continually in a user's possession, unlike a standard computer, and, thus, can more accurately reveal the user's actions. Forensic information that can be uniquely extracted from a mobile device includes the following:

- *Call detail records*. This information can reveal the date and time a telephone call was started and ended, the terminating and originating cell phone towers that were used, whether the call was outgoing or incoming, the call's duration, who was called, and who made the call.
- *Global Positioning System (GPS) data*. GPS data can accurately pinpoint the location of a user and what activities he was performing in a specific location.
- *App data*. Many apps store and access data such as media files, contact lists, and a gallery of all the photos on the device.
- *Short Message Service (SMS) texts*. Text messaging is a popular means of communication. It leaves electronic records of dialogue that can be used as evidence.
- *Photos and videos*. Media recorded as photos and videos on a mobile device can often contain incriminating evidence.

Cloud Forensics

If the incident is the result of a breach of cloud-based resources, it is not possible to secure the scene as in an on-prem incident. When dealing with a cloud incident, the following should be considered:

- A primary concern is to ensure that the digital evidence has not been tampered with by third parties so it can be admissible in a court of law. In Software as a Service (SaaS) and Platform as a Service (PaaS) models, because customers do not have control of the hardware, they must depend on the cloud service providers to accumulate log data. A **right to audit clause** in a cloud contract gives the customer the legal right to review the logs, and these should also be negotiated in advance.
- When a cloud customer is notified by its cloud service provider that an incident occurred, the immediate response from the customer's in-house legal and IT teams will be to ask for details about the scope of the

impact. However, unless they are contractually obligated, the cloud provider may take weeks or even months to provide its client with details as they perform an investigation. However, once the cloud customer has been notified, the "clock has started ticking" regarding **data breach notification law** deadlines. This can place the cloud customer in an awkward situation.

- The legal **regulatory/jurisdiction** laws that govern the site in which the cloud data resides may present difficulties. For example, a court order issued in a jurisdiction where the cloud data center is located will likely not be applicable to another jurisdiction in another country.

CAUTION When creating a cloud platform, the customer can often choose the region in which the data will reside. It is at this time that issues regarding jurisdiction should be considered and the region chosen carefully.

TWO RIGHTS & A WRONG

1. A DNS service is the most important network-based device log to examine.
2. A multi-platform log management tool that supports various platforms, log sources, and formats is nxlog.
3. IPFIX (IP Flow Information Export) is similar to NetFlow but with additional capabilities, such as integrating Simple Network Management Protocol (SNMP) information directly into the IPFIX information.

See Appendix B for the answer.

VM LAB You're now ready to complete the live, virtual machine labs for this module. The labs can be found in the Practice It folder in each MindTap module.

SUMMARY

- Access control is granting or denying approval to use specific resources; it is controlling access. Authentication, authorization, and accounting, sometimes called AAA, provide a framework for controlling access to computer resources. Individuals are given different roles in relationship to access control objects or resources. These include data privacy officer, data custodian/steward, data owner, data controller, and data processor. Hardware and software have a predefined framework that the custodian can use for controlling access. This framework, called an access control scheme, can be used by a custodian/steward to configure the necessary level of control. Using these schemes is part of privileged access management, which is the technologies and strategies for controlling elevated (privileged) access. There are five major access control schemes: Discretionary Access Control, Mandatory Access Control, Role-Based Access Control, Rule-Based Access Control, and Attribute-Based Access Control.
- An access control list (ACL) is a set of permissions that is attached to an object. This list specifies which subjects are allowed to access the object and what operations they can perform on it. Although ACLs can be associated with any type of object, these lists are most often viewed in relation to files maintained by the OS. Although widely used, ACLs have limitations. First, using ACLs is not efficient. A second limitation to ACLs is that they can be difficult to manage in an enterprise setting where many users need to have different levels of access to many different resources.
- An incident response plan is a set of written instructions for reacting to a security incident. An incident response team is responsible for responding to security incidents. In addition to technical specialists who can address specific threats, it should also include members who are public relations employees and managers who can guide enterprise executives on appropriate communication. It is important for an incident response plan to identify the relevant stakeholders within the organization who need to be initially informed of an incident and then kept up to date. Known as stakeholder management, it includes areas such as operations, legal, technical, finance, and human resources.

- It is important to test an incident response plan by conducting simulated exercises to make necessary adjustments. The different types of exercises are tabletop, walkthrough, and simulation. Just as a cybersecurity framework, or series of documented processes, can be used to define policies and procedures for implementing and managing security controls in an enterprise environment, frameworks about how attacks occur can also be studied. These exploitation frameworks serve as models of the thinking and actions of threat actors. Common attack frameworks are MITRE ATT&CK, the Diamond Model of Intrusion Analysis, and Cyber Kill Chain.
- Two elements that are closely associated with using SOARs are a SOAR playbook and a runbook. A playbook is a linear-style checklist of required steps and actions needed to successfully respond to specific incident types and threats. A runbook is a series of automated conditional steps (like threat containment) that are part of an incident response procedure. Whereas a playbook focuses more on manual steps to be performed, a runbook is usually actions that are performed automatically. One of the most critical steps in incident response is limiting the spread of the attack (containment). However, containment can be most effective when the network has been properly designed. In order to neutralize the attacker, limit the spread of the attack, and prevent additional successful incidents, it may be necessary to make configuration changes to devices and processes.
- Following a cybersecurity incident, it must be fully investigated. This is to not only pinpoint how it occurred so that future incidents can be prevented but also for regulatory compliance reporting. There are several sources of data that can provide helpful clues in uncovering how an incident occurred. A log is a record of events that occur. Security logs are particularly important as they relate to incident investigation because they can reveal the type of attack that was directed at the network and how it successfully circumvented existing security defenses. Application log files can give information about attacks focused on different applications. If an application log identifies an app that has been the source of a compromise, software can be used to create a dump file, which is a snapshot of the process that was executing and any modules that were loaded for an app at a specific point in time. There are several problems associated with log management—or transmitting, collecting, analyzing, and disposing of log data. There are different solutions to these problems, such as syslog, nxlog, rsyslog, syslog-ng, and journalctl.
- IP software monitors can provide insight into an incident. NetFlow is a session sampling protocol feature on Cisco routers that collects IP network traffic as it enters or exits an interface and uses ICMP Echo request packets. The tool sFlow is a packet sampling protocol that gives a statistical sampling instead of the actual flow of packets. IPFIX (IP Flow Information Export) is similar to NetFlow but adds additional capabilities, such as integrating SNMP information directly into the IPFIX information. Metadata is data that describes information about other data. Analyzing file, web, mobile, and email metadata can give clues regarding an attack. Data from a vulnerability scan and SIEM products that consolidate real-time security monitoring and management of security information with analysis and reporting of security events is useful.
- Forensics is the application of science to questions that are of interest to the legal profession. Digital forensics uses technology to search for evidence pertaining to a cybercrime or damage that occurred during a cyber incident. When an on-prem illegal or unauthorized incident occurs that involves technology, action must be taken immediately. A delay of even a few minutes can allow digital evidence to be overwritten in the normal function of the device, become contaminated by other users, or give the perpetrator time to destroy the evidence. Preservation of evidence, or ensuring that important proof is not corrupted or even destroyed, is also critical. Preserving evidence can also help mitigate nonrepudiation, or a denial by the perpetrators that they were involved or did anything wrong.
- As soon as the incident response team begins its work, it must start and maintain a strict chain of custody. The chain of custody documents that the evidence was always under strict control and no unauthorized person was given the opportunity to corrupt the evidence. When examining technology devices that may contain evidence, called artifacts, it is critical to follow a specific order. This is because different data sources have different degrees of preservation. An order of volatility must be followed to preserve the most fragile data first. A final analysis looks at recovering the data from the security event and what lessons can be learned from it. The forensics procedures have gathered strategic intelligence—or the collection, processing, analysis, and dissemination of intelligence for forming policy changes. A more in-depth application of strategic intelligence is strategic counterintelligence, which involves gaining information about the attacker's intelligence collection capabilities.
- There are different software and hardware forensics tools available for analysis. Instead of using individual software tools for a forensics investigation, products are available that package multiple tools into a single suite that has a common user interface and can more easily exchange information among the different tools. A digital forensic workstation is a computer that is specially configured to perform forensics activities. If

an incident is the result of a breach of cloud-based resources, it is not possible to secure the scene as in an on-prem incident. When dealing with a cloud incident, there are different procedures that must be followed.

Key Terms

access control list (ACL)
access control scheme
accounting
admissibility
artifacts
Attribute-Based Access Control (ABAC)
authentication servers
authorization
Autopsy
cache
call manager
chain of custody
communication plan
conditional access
containment
Cyber Kill Chain
data breach notification law
data controller
data custodian/steward
data owner
data privacy officer (DPO)
data processor
dd
Diamond Model of Intrusion Analysis
Discretionary Access Control (DAC)
dump file
Echo
e-discovery
eradication
exercises
exploitation frameworks
filesystem permissions
firmware
forensics
FTK Imager
generic account
guest account
identification
incident response plan
incident response process
incident response team
IPFIX (IP Flow Information Export)
isolation
journalctl
legal hold
lessons learned
log
Mandatory Access Control (MAC)
memdump
metadata
MITRE ATT&CK
NetFlow
nxlog
order of volatility
OS event logs
pagefile
playbook
preparation
preservation of the evidence
privileged access management
provenance
recovery
regulatory/jurisdiction
response and recovery controls
retention policy
right to audit clause
Role-Based Access Control
rsyslog
Rule-Based Access Control
runbook
SEAndroid
service account
Session Initiation Protocol (SIP)
sFlow
shared account
simulation
snapshot
stakeholder management
strategic counterintelligence
strategic intelligence
swap file
syslog
syslog-ng
tabletop
tags
time offset
time stamp
user account
walkthrough
WinHex

Review Questions

1. Which of the following is NOT part of the AAA framework?
    - **a.** Authentication
    - **b.** Access
    - **c.** Authorization
    - **d.** Accounting
2. Raul has been asked to serve as the individual to whom day-to-day actions have been assigned by the owner. What role is Raul taking?
    - **a.** Data custodian/steward
    - **b.** Data privacy officer
    - **c.** Data controller
    - **d.** Data processor
3. Which access control scheme is the most restrictive?
    - **a.** Role-Based Access Control
    - **b.** DAC
    - **c.** Rule-Based Access Control
    - **d.** MAC
4. Which type of access control scheme uses predefined rules that makes it the most flexible scheme?
    - **a.** ABAC
    - **b.** DAC
    - **c.** MAC
    - **d.** NAC

5. Which statement about Rule-Based Access Control is true?
   a. It requires that a custodian set all rules.
   b. It is no longer considered secure.
   c. It dynamically assigns roles to subjects based on rules.
   d. It is considered a real-world approach by linking a user's job function with security.
6. Which of these is a set of permissions that is attached to an object?
   a. ACL
   b. SRE
   c. Object modifier
   d. Entity attribute (EnATT)
7. What can be used to provide both filesystem security and database security?
   a. RBASEs
   b. LDAPs
   c. CHAPs
   d. ACLs
8. What is the amount of time added to or subtracted from Coordinated Universal Time to determine local time?
   a. Greenwich Mean Time (GMT)
   b. Civil time
   c. Daylight savings time
   d. Time offset
9. Cheryl has been asked to set up a user account explicitly to provide a security context for services running on a server. What type of account will she create?
   a. Generic account
   b. Service account
   c. User account
   d. Privilege account
10. Which of these is NOT an incident response process step?
    a. Recovery
    b. Reporting
    c. Eradication
    d. Lessons learned
11. Which of the following is typically a monthly discussion of a scenario conducted in an informal and stress-free environment to evaluate an incident response plan?
    a. Walkthrough
    b. Simulation
    c. Tabletop
    d. Incident Response Plan Evaluation (IRP-E)
12. Ella wants to research an attack framework that incorporates adversary, infrastructure, capability, and victim. Which of the following would she choose?
    a. Diamond Model of Intrusion Analysis
    b. Cyber Kill Chain
    c. Mitre ATT&CK
    d. Basic-Advanced Incident (BAI) Framework
13. Blaise needs to create a document that is a linear-style checklist of required manual steps and actions needed to successfully respond to a specific type of incident. What does she need to create?
    a. Playbook
    b. Runbook
    c. SIEM-book
    d. ARC Codebook
14. Which of the following should be performed in advance of an incident?
    a. Containment
    b. Segmentation
    c. Isolation
    d. Capture
15. What is a platform used to provide telephony, video, and web conferences that can serve as an entry point to a threat actor?
    a. SIP
    b. VoIP
    c. Call manager
    d. IP voice
16. Which of the following is NOT a problem associated with log management?
    a. Multiple devices generating logs
    b. Large volume of log data
    c. Different log formats
    d. Time-stamped log data
17. Which tool is an open source utility for UNIX devices that includes content filtering?
    a. syslog
    b. nxlog
    c. rsyslog
    d. syslog-ng
18. Which of the following is a packet sampling protocol that gives a statistical sample instead of the actual flow of packets?
    a. NetFlow
    b. sFlow
    c. IPFIX
    d. journalctl

19. Which of the following is the most fragile and should be captured first in a forensics investigation?
- **a.** ARP cache
- **b.** Kernel statistics
- **c.** CPU cache
- **d.** RAM

20. Which of the following is a Linux utility that displays the contents of system memory?
- **a.** Autopsy
- **b.** WinHex
- **c.** dd
- **d.** memdump

Hands-On Projects

CAUTION If you are concerned about installing any of the software in these projects on your regular computer, you can instead use the Windows Sandbox or install the software in the Windows virtual machine created in the Module 1 Hands-On Projects. Software installed within the virtual machine will not impact the host computer.

Project 13-1: Entering and Viewing Metadata

Time Required: 25 minutes

Objective: 4.5 Explain the key aspects of digital forensics.
- Data recovery

Description: Although most file metadata is not accessible to users, they can enter and change some types of metadata. In this project, you view and enter metadata in a Microsoft Word document.

1. Use Microsoft Word to create a document containing your name. Save the document as **Metadata1.docx**.
2. Click the **File** tab on the Ribbon, and then click **Info**.
3. Click the **Properties** arrow and then click **Advanced Properties**.
4. Enter the following information in the Advanced Properties dialog box:
   - Title—**Project 13-1**
   - Author—Your name
   - Category—**Computer Forensics**
   - Comments—**Viewing metadata in Microsoft Word**
5. Click **OK**.
6. Save **Metadata1.docx**.
7. Click the **File** tab on the Ribbon, and then click **Info**.
8. Click the **Properties** arrow and then click **Advanced Properties**.
9. Click the **Statistics** tab in the Properties dialog box and view the information it contains. How could a computer forensics specialist use this metadata when examining this file?
10. Click the **Custom** tab. Notice that it includes several predefined fields that can contain metadata.
11. In the Name box, enter **Editor**.
12. Be sure the Type is set to **Text**.
13. Enter your name in the **Value** field, and then press **Enter**.
14. Select three predefined fields and enter values for each field. Click **OK**. Save your document when you are finished.
15. Click the **Back** button to return to **Metadata1.docx.**
16. Delete your name from **Metadata1.docx** so you have a blank document. However, this file still has the metadata. Enter today's date and save this as **Metadata2.docx**.
17. Close **Metadata2.docx**.
18. Reopen **Metadata2.docx**.
19. Click the **File** tab on the Ribbon, and then click **Info**.
20. Click to **Properties** arrow and then click **Advanced Properties**.
21. What properties carried over to **Metadata2.docx** from **Metadata1.docx**, even though the content of the file was erased? Why did this happen? Could a computer forensics specialist use this technique to examine metadata, even if the contents of the document were deleted?
22. Close all windows.

Project 13-2: Viewing Windows Slack and Hidden Data

Time Required: 20 minutes

Objective: 4.5 Explain the key aspects of digital forensics.

- Data recovery

Description: RAM slack, drive slack, and other hidden data can be helpful to a computer forensics investigator. In this project, you download and use a program to search for hidden data.

1. Use your web browser to go to **www.briggsoft.com**. (The location of content on the Internet may change without warning. If you are no longer able to access the program through the above URL, use a search engine and search for "Directory Snoop.")
2. Scroll down to the current version of **Directory Snoop** and click **Download** above **Free Trial**.
3. Follow the default installation procedures to install Directory Snoop.
4. Launch Directory Snoop.
5. Depending on the filesystem on your computer, click **FAT Module** or **NTFS Module**.
6. Under Select Drive, click **C:** or the drive letter of your hard drive. If the RawDisk Driver dialog box appears, click **Install Driver**, click **OK**, and then select the appropriate drive again.
7. Click to select a file and display its contents, preferably a user-created document (such as a Microsoft Word file). Scroll down under **Text data** to view the contents that you can read.
8. Select other files to look for hidden data. Did you discover anything that might be useful to a computer forensics specialist?
9. To create a text document using Notepad, click the **Start** button, enter **Notepad** in the Search box, and then click the app.
10. Enter the text **Now is the time for all good men to come to the aid of their country.**
11. Save the document on your desktop as **Country.txt**.
12. Exit Notepad.
13. Right-click **Start**, click **File Explorer**, and then navigate to **Country.txt**.
14. Right-click **Country.txt** and then click **Delete** to delete the file.
15. Search for information contained in the file you just deleted. Return to **Directory Snoop**, click the top-level node for the **C:** drive, and then click the **Search** icon.
16. Click **Files**.
17. Enter **country** as the item that you are searching for.
18. Click **Search in slack area also**.
19. Click **OK**. Did the program find this data? Why or why not?
20. Close all windows.

Project 13-3: Using Discretionary Access Control to Share Files in Windows

NOTE 19

You should have a standard user named "Abby Lomax" created in Windows and a Notepad document Sample.txt created by an administrative user to complete this assignment.

Time Required: 25 minutes

Objective: 3.8 Given a scenario, implement authentication and authorization solutions.

- Access control schemes

Description: Discretionary Access Control can be applied in Microsoft Windows. In this project, you set up file sharing with other users.

1. Right-click the file **Sample.txt**.
2. To see the current permissions on this file, click **Properties**, and then click the **Security** tab.
3. Click your username and then click **Edit**.
4. Click your username again (if necessary), and then, under **Permissions for [user]**, click **Deny** for the **Read** attribute.
5. Click **Apply** and then click **Yes** at the warning dialog box.
6. Click **OK** in the Properties dialog box and then click **OK** in the Sample.txt dialog box.
7. Double-click the file **Sample.txt** to open it. What happens?

8. Give permission to Abby Lomax to open the file. Click the file **Sample.txt**.
9. Click the **Share** tab and then click **Specific people**.
10. Click the arrow and select **Abby Lomax**. Click **Add**.
11. Click **Share**.
12. Click **Done** when the sharing process is completed.
13. Click **Start**, click your account name or picture, and then click **Switch User**.
14. Log in as Abby Lomax.
15. Right-click **Start** and then click **File Explorer**.
16. Navigate to your account name and locate the file Sample.txt.
17. Double-click **Sample.txt** to open the file. Using DAC, permissions have been granted to another user.
18. Close all windows.

Project 13-4: Exploring User Account Control (UAC)

Time Required: 20 minutes

Objective: 3.8 Given a scenario, implement authentication and authorization solutions.

- Access control schemes

Description: Microsoft Windows provides several options with user account control (UAC). In this project, you configure and test UAC settings. Note that during this project, the UAC dialog box may appear after specific steps. Be sure to always confirm the selection by clicking **OK** or **Yes**.

1. First ensure that UAC is set at its highest level. Enter **UAC** in the search box, and then press **Enter**.
2. The User Account Control Settings dialog box is displayed. If necessary, move the slider up to the higher level of **Always notify**.
3. Click **OK**.
4. Type **mmc** in the search box, and then press **Enter**.
5. The UAC confirmation box is displayed. Click **No**.
6. Enter **UAC** in the search box, and then press **Enter**.
7. The User Account Control settings dialog box is displayed. Move the slider down to the lowest level of **Never notify me when**.
8. Click **OK**.
9. Type **mmc** in the search box, and then press **Enter**. What happens?
10. Enter **UAC** in the search box, and then press **Enter**.
11. Change the account settings to **Notify me only when apps try to make changes to my computer (default)** and click **OK**.
12. Type **mmc** in the search box, and then press **Enter**. What happens? Close the Console1 dialog box.
13. Enter **UAC** in the search box, and then press **Enter**.
14. Change the account settings to **Notify me only when apps try to make changes to my computer (do not dim my desktop)** and click **OK**.
15. Type **mmc** in the search box, and then press **Enter**. What happens?
16. Enter **UAC** in the search box, and then press **Enter**.
17. The User Account Control Settings dialog box is displayed. Move the slider up to the higher level of **Always notify**.
18. Click **OK**.
19. Next, change the settings to disable secure desktop mode in UAC. Enter **gpedit.msc** in the search box, and then press **Enter**.
20. If necessary, click **Computer Configuration**.
21. Expand **Windows Settings**.
22. Expand **Security Settings**.
23. Expand **Local Policies**.
24. Expand **Security Options**.
25. Navigate to **User Account Control: Switch to the secure desktop when prompting for elevation** and double-click it.
26. Change **Enabled** to **Disabled**.
27. Click **Apply** and then click **OK**.

28. Enter **UAC** in the search box, and then press **Enter**.
29. What is different about your desktop now?
30. Return to the Security Options in gpedit.msc.
31. Review the other UAC options available.
32. Navigate to **User Account Control: Switch to the secure desktop when prompting for elevation** and double-click it.
33. Change **Disabled** to **Enabled**.
34. Click **Apply** and then **OK**.
35. Close all windows.

Case Projects

Case Project 13-1: Forensics Tools

Search the Internet for websites that advertise computer forensic tools. Locate reviews of four tools. Create a chart that lists the tool, the type of data that it searches for, its features, the cost, etc. Which would you recommend if you could purchase only one tool and budget were not a concern?

Case Project 13-2: Diamond Model of Intrusion Analysis

The Diamond Model of Intrusion Analysis is a framework for examining network intrusion events. Use the Internet to research this model. Identify how it is used, its strengths and weaknesses, and how widely implemented it is. What is your conclusion about this framework? How useful does it appear to be to you? Write a one-page analysis of your research.

Case Project 13-3: SOAR Runbooks and Playbooks

Research SOAR runbooks and playbooks. If possible, locate an example and read through each type. What are their advantages? What are their disadvantages? How are they used? Write a one-page paper on your research.

Case Project 13-4: Sources of Forensics Data

IP software monitors can provide insight into an incident for a forensics evaluation. Use the Internet to research NetFlow, sFlow, and IPFIX. How are they used? What are their differences? What are their similarities? Create a table that lists the strengths and weaknesses of each.

Case Project 13-5: Log Collection and Analysis Tools

Research the log tools syslog, nxlog, rsyslog, syslog-ng, and journalctl. Create a table that compares each of them, and list how they are used. Include a detailed description of the strengths and weaknesses of each tool. Write a one-page paper on your research.

Case Project 13-6: Cloud Forensics

Use the Internet to research cloud forensics. What can a cloud provider customer do when they are alerted to a cloud security breach? What are the responsibilities of the cloud provider when this occurs? What are the responsibilities of the customer? How can customers insulate themselves from damages? If you were a cloud customer, what would you require of the cloud provider? Write a one-page paper on your research.

Case Project 13-7: North Ridge Security

North Ridge Security provides security consulting and assurance services. You have recently been hired as an intern to assist them.

Impact Industries is a new client of North Ridge and wants an update on forensics investigations. You have been asked to make a presentation to them.

1. Create a PowerPoint presentation for Impact Industries about forensics, including the procedures for conducting an investigation and the tools that can be used. Your presentation should contain at least 10 slides.
2. After the presentation, Impact Industries has asked about how a forensic examination would be performed on the data stored by their cloud provider. Use the Internet to research cloud forensics and then create a memo about your findings and recommendations.

Case Project 13-8: Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. Go to **community.cengage.com/infosec2** and click the *Join or Sign in* icon to log in, using your login name and password that you created in Module 1. Click **Forums (Discussion)** and click on **Security+ Case Projects (7th edition)**. Read the following case study.

Although a data breach may require that an organization contact the affected parties, it is often less clear whether law enforcement agencies should be contacted after a cyber incident has occurred. One study revealed that only 28 percent of businesses in the United Kingdom (UK) reported a cybercrime to law enforcement agencies.[1] In the United States, the FBI estimates that only 15 percent of victims report cybercrimes against them.[2] The following reasons are often cited for the reluctance to report cyber incidents to law enforcement agencies:

- Identifying threat actors, especially when attacks come from abroad, is notoriously difficult for domestic law enforcement agencies and often leads to no arrests or convictions.
- While the interest of the organization is to resume operations as quickly as possible, the interest of law enforcement is to identify, track down, and prosecute the perpetrator. This may result in competing interests and could impede the organization from resuming normal operations as law enforcement seeks to retain evidence and launch its own investigation.
- Reporting an incident may make it public knowledge and harm the organization's reputation unnecessarily.

However, there are advantages to reporting a cyber incident:

- Law enforcement agencies can work with foreign counterparts to stop organized cybercrime gangs, which can help reduce the number of overall attacks on a business.
- Large federal law enforcement agencies have extensive resources and experience and can even make the company's own internal investigation easier by having experts at hand.
- Companies that report incidents to law enforcement can help provide information toward intelligence-sharing efforts.
- Many law enforcement agencies emphasize that a business might have the missing piece of a puzzle that can help capture repeat cyber criminals.

Would you contact law enforcement if there were a breach at your place of business? Take your side of this argument and post your opinions to on the Community Site discussion board.

References

1. "Cyber security underpinning the digital economy," *IoD*, March 3, 2016, retrieved Aug. 16, 2019, www.iod.com/cyber-security-for-your-business/articles/cyber-security-underpinning-the-digital-economy.
2. "2016 internet crime report," *IC3*, retrieved Aug. 16, 2019, https://pdf.ic3.gov/2016_IC3Report.pdf.

MODULE 14

CYBERSECURITY RESILIENCE

After completing this module, you should be able to do the following:

1. Define business continuity
2. Describe how to achieve resilience through redundancy
3. Explain what a policy is
4. Describe different types of security policies

Front-Page Cybersecurity

Ransomware continues to plague users and organizations of all types and sizes. However, the threat actors behind ransomware have not stood still. The most effective tool to combat ransomware—backups—is now under attack.

When ransomware first became widespread, users were reminded that their key defense was to make regular backups of their data. If ransomware locked a computer, the data backups could be used to restore a computer to its preransomware state. While it still essentially remains true that up-to-date backups are a good defense, threat actors have expanded their targets to include backups, too. Instead of ransomware encrypting only files on the user's local computer, the "next level" of ransomware will encrypt all files on any network or device connected to the local computer. This includes secondary hard disk drives, USB hard drives, network attached storage (NAS) devices, network servers, and even cloud-based data repositories.

How can users defend themselves against ransomware that may infect their data backups? How can users protect their files stored on a networked or attached device connected to the computer or even cloud storage repositories? If an endpoint becomes infected with ransomware, is there a way to protect remote backup files as well?

Users can apply two tests to determine if files other than those stored on the local hard drive are at risk from ransomware. First, if a remote storage device is "mounted" on the local computer and displays a drive letter (such as "D:"), then those files are at risk from a ransomware attack. Second, if a cloud storage repository is configured so that files automatically placed in a local folder are synchronized to the cloud storage, they too are at risk. This is because the ransomware can move encrypted files into the folder, where they will be replicated onto the cloud.

The defense against this next level of ransomware involves a different approach to storage devices and the cloud. Users should first think about having an "air gap," or physically isolating (putting distance between) the computer and the remote backup files. "Manual authentication" that requires the user to enter a username and password, not automatically applied authentication, can also mitigate this next level of ransomware. Some suggestions for devices include the following:

External USB storage device. Unplug the storage device from the computer when not using it.

Secondary hard disk drive. Unmount the drive when it is not needed and then mount it again when needed. (Unmounting the drive hides it from the computer but retains the data.) The command "mountvol D: /p" at the command line will unmount the drive, as will using the Windows Disk Management utility.

Network attached storage (NAS). Create a new share ("admin") and then create a new user account that is the only account with access to the share. Give this user account a strong username and password, and then log in to (and out of) that share as needed.

Cloud storage. Consider turning off automatic synchronization so that files placed in a local folder are not immediately synced to cloud storage. Instead, users should log in to their cloud storage provider through a web browser that requires entering a username and password to sync the files. If this is not feasible, users should check with their cloud storage provider. Many cloud providers have some type of short-term "versioning," meaning that older versions are retained online for a limited period of time (perhaps seven days but sometimes up to a month). If cloud storage files become locked with ransomware, it is possible to roll back to a previous version of unencrypted files.

Earthquakes, tsunamis, tornados, hurricanes, floods, wildfires—these and other natural disasters have a major impact on businesses around the world. The worldwide global economic loss due to natural disasters for 2019 was $232 billion dollars. Although this is a very high amount, it actually is the lowest over the last four years. (The amount fluctuates each year due to the number, type, and duration of natural disasters.) In 2017, this loss was more than double, at $475 billion dollars. Flooding generates the highest loss of both property and lives each year.[1] Natural disasters are virtually impossible to predict in time to make quick preparations.

Not all disasters, however, are acts of nature. Sabotage, terrorism, cyberattacks, and pandemics also can quickly bring a business to its knees—or put it out of operation entirely. The ability of an organization to maintain its operations and services in the face of catastrophe is crucial if it is to survive.

Although preparation for disasters is an essential task for organizations both large and small, it remains sadly lacking in practice. Many organizations are completely unprepared. It is estimated that four out of every 10 businesses do not reopen following a disaster, and another 25 percent fail within one year. Nine out of 10 businesses fail within two years of being struck by a disaster.[2] Of those organizations that do have plans on paper, most have never tested the plans to determine whether they would successfully bring the business through an unforeseen event.

One of the keys for an organization to continue to function following any type of disaster is *resilience*, which is defined as the capacity to recovery quickly from difficulties and spring back into shape. But resilience does not happen by accident: it requires planning and preparation.

In this module, you learn about applying resilience to keep an organization operational during and after a disaster. You first learn what business continuity is and why it is important. Next, you investigate how to prevent disruptions through redundancy. Finally, you see how business policies can help provide resilience to an organization.

BUSINESS CONTINUITY

CERTIFICATION

2.5 Given a scenario, implement cybersecurity resilience.

4.2 Summarize the importance of policies, processes, and procedures for incident response.

5.4 Summarize risk management processes and concepts.

This section explains what business continuity is and how it can be achieved through redundancy.

Introduction to Business Continuity

Defining business continuity can best be done by comparing similar but different types of processes and plans. A business impact analysis and a disaster recovery plan are closely associated with business continuity.

What Is Business Continuity?

Business continuity can be defined as the ability of an organization to maintain its operations and services in the face of a disruptive event or a major disaster. These disasters may be **environmental disasters** such as floods, hurricanes, and tornados, or **man-made disasters** such as industrial accidents, oil spills, terrorist attacks, and transportation accidents. Although most disasters to an organization are **external disasters** (such as environmental disasters), some are **internal disasters** (such as a fire in a data center).

A **business continuity plan (BCP)** is a strategic document that provides alternative modes of operation for business activities that, if interrupted, could result in a significant loss to the enterprise. Creating a BCP involves identifying exposure to threats, creating preventive and recovery procedures, and then testing them to determine if they are sufficient. In short, a BCP is designed to ensure that an organization can continue to function (*continuity of operations*) in the event of an environmental disaster or man-made disaster; it is *recovery planning*.

NOTE 1

BCP may also include succession planning, which is determining in advance who will be authorized to take over in the event of the incapacitation or death of key employees.

A BCP generally has three goals:

- *Business recovery planning*. This involves resuming critical business functions and processes that relate to and support the delivery of the core products or services to a customer.
- *Crisis management and communications*. Crisis management and communications is the process of giving an effective response to an event. It is intended to stabilize the situation through effective leadership communication.
- *Disaster recovery*. This element addresses the recovery of critical information technology (IT) assets, including systems, applications, databases, storage, and network assets.

A BCP may sometimes be confusing due to conflicting terminology. Because BCPs are used across a wide range of industries and by different regulatory groups and agencies, many of these use their own unique terminology that is similar to BCP but slightly different. Table 14-1 lists several of the terms that are similar to or related to a BCP but have different meanings.

Table 14-1 BCP terminology

Terminology	Definition	How it compares to BCP
Resumption planning	Used for the recovery of critical business functions separate from IT, such as resuming a critical manufacturing process	Part of the BCP process
Contingency actions	Tactical solutions addressing a core business resource or process, such as how to handle the loss of a specific vendor	Contingency planning is usually considered an isolated action and not part of an overall BCP
Emergency response	The immediate actions taken to preserve lives and safeguard property and assets, such as an evacuation plan	Emergency response is a subset of a BCP
Disaster recovery	The recovery and resumption of critical technology assets in the event of a disaster	Disaster recovery is a component of an overall BCP program

A BCP should include the following elements:

- *High availability*. A BCP should address **high availability**, which is the ability to withstand all outages—planned and unplanned outages, and environmental and internal disasters—while providing continuous processing for critical applications. For example, a high availability solution for critical e-commerce servers and databases would require a fully automated failover to a backup system so that sales can continue functioning without any disruption.

- *Scalability*. Organizations continue to grow and expand on a regular basis. A BCP that only looks at the organization as it stands today will find that the plan is out of date tomorrow. Instead, a BCP must have the capability to cover increased capacity; in other words, a BCP must have **scalability**.
- *Diversity*. Just as a BCP must have scalability as capacity increases, it must also include **diversity** as different technologies, third-party vendors, controls, and even cryptographic solutions are added.
- *On-prem and cloud*. As more and more resources are moved from on-premises to the cloud, a BCP should have the flexibility to address this movement without needing to continually rewrite the plan.

Similar to creating a BCP is **continuity of operation planning (COOP)**. This is a federal initiative that is intended to encourage organizations (and departments with an organization) to address how critical operations will continue under a broad range of negative circumstances. A COOP plan addresses emergencies from an "all-hazards approach" instead of focusing more narrowly on a specific event. It is designed to establish requirements for ensuring that critical functions continue and even includes how personnel and resources can be relocated in case of emergencies.

Business Impact Analysis (BIA)

One important tool for creating a BCP is a **business impact analysis (BIA)**. A BIA identifies business processes and functions and then quantifies the impact a loss of these functions may have on business operations. These impacts include the impact on property (tangible assets), impact on finance (monetary funding), impact on safety (physical protection), impact on reputation (status), and even the impact on life (well-being). By identifying the critical processes and functions through a **site risk assessment** (a detailed evaluation of the processes performed at a site and how they can be impacted), a BIA can then be the foundation for a **functional recovery plan** that addresses the steps to take to restore those processes, if necessary.

CAUTION

An organization with remote sites sometimes assumes that all sites perform essentially the same functions as the main headquarters. However, that is not always true. In one case, a third-party vendor was hired to perform a BIA but was told to only look at the headquarters. The vendor convinced the organization to examine all the sites. They found that the headquarters performed more than 80 functions, of which half were centrally managed and implemented. The other 40 functions could be performed at the satellite offices in various combinations, which would have been overlooked if the BIA were not conducted at each site.

A BIA is designed to identify those processes that are critically important to an enterprise. A BIA will help determine the **mission-essential function**, or the activity that serves as the core purpose of the enterprise. For example, a mission-essential function for a hospital could be to *deliver healthcare services to individuals and their families*, while a nonessential function is to *generate and distribute a monthly online newsletter*. In addition, a BIA can also help in the **identification of critical systems** that in turn support the mission-essential function. In a hospital setting, a critical system could be to *maintain an emergency room facility for the community*. Whereas this is a critical system, is not the core purpose of the hospital.

Identifying the **single point of failure**, which is a component or entity in a system that if it no longer functions will disable the entire system, is also a goal of a BIA. A patient information database in a hospital could be considered a single point of failure. Minimizing these single failure points results in a system that can function for an extended period with little downtime. This availability is often expressed as a percentage of uptime in a year. Table 14-2 lists the percentage availability and the corresponding downtimes.

Table 14-2 Percentage availability and downtimes

Percentage availability	Name	Weekly downtime	Monthly downtime	Yearly downtime
90%	One Nine	16.8 hours	72 hours	36.5 days
99%	Two Nines	1.68 hours	7.20 hours	3.65 days
99.9%	Three Nines	10.1 minutes	43.2 minutes	8.76 hours
99.99%	Four Nines	1.01 minutes	4.32 minutes	52.56 minutes
99.999%	Five Nines	6.05 seconds	25.9 seconds	5.26 minutes
99.9999%	Six Nines	0.605 second	2.59 seconds	31.5 seconds

NOTE 2

Because privacy of data is of high importance today, many BIAs also contain a privacy impact assessment, which is used to identify and mitigate privacy risks. This includes an examination of what personally identifiable information (PII) is being collected, the reasons it is collected, and the safeguards regarding how the data will be accessed, shared, and stored. A privacy threshold assessment can determine if a system contains PII, whether a privacy impact assessment is required, and if any other privacy requirements apply to the IT system.

Disaster Recovery Plan (DRP)

Whereas a BCP considers the needs of the business as a whole in recovering from a catastrophe, a subset of it focuses on continuity in the context of IT. This is called a **disaster recovery plan (DRP)**, which is involved with restoring IT functions and services. A DRP is a written document that details the process for restoring IT resources following an event that causes a significant disruption in service. Comprehensive in scope, a DRP is intended to be a detailed document that is updated regularly.

Most DRPs cover a standard set of topics. One common topic is the sequence in restoring systems. After a disaster has occurred, in what sequence should systems be reinstated (**restoration order**)? That is, which systems should have priority and be restored before other systems? Several factors may be considered. One factor is obvious dependencies: that is, the network must be restored before applications that rely on the network are restored. A second factor is the processes that are of fundamental importance to an enterprise: critical systems that support the mission-essential function and those systems that require high availability need to be restored before other systems. Another factor is the alternative business practices, or those "workaround" activities that can temporarily substitute for normal business activities. That is, how long can a manual workaround process meet the temporary needs without causing bigger problems such as unmanageable backlogs?

Resilience Through Redundancy

Adding cybersecurity resilience to promote business continuity is important to prevent certain events from crippling an enterprise. This is sometimes known as incorporating "fault tolerance" into IT systems. A "fault" is a malfunction or deviation from the systems' normal expected behavior, while "tolerance" is the capacity for enduring. Fault tolerance refers to a system's ability to deal with malfunctions.

NOTE 3

Fault tolerance is a realization that systems will always have faults or the potential for faults, so they must be designed in such a way that the system will be tolerant of those faults. The system should compensate for the faults yet continue to function.

Because no IT system can ever be completely free of faults, the solution to fault tolerance is to build in **redundancy**, or the use of duplicated equipment to improve the availability of the system. The goal of redundancy is to reduce a variable known as the **mean time to recovery (MTTR)**. Some systems are designed to have a MTTR of zero, which means they have redundant components that can take over the instant the primary component fails.

Redundancy planning can involve redundancy for endpoints, servers, disks, networks, power, sites, and data.

Endpoints

Although resilience through redundancy is critical for business continuity, not all systems may require it. For example, the downtime from a user's endpoint, such as a desktop computer, is not as critical as that for servers, disks, and networks. Also, a desktop or laptop computer is a ubiquitous commodity item today that, if necessary, can be quickly replaced in the event of a hardware component failure, and thus would not require hardware redundancy (such as two identical hard disks, two identical keyboards, and so on).

In the event of a software issue, such as a malware infection, many OSs have a feature known as **revert to known state** in which it is possible to "roll back the clock" on the OS and restore it to an earlier point prior to the problem. Versions of Microsoft Windows through Windows 7 had a **last known good configuration** option in which the OS could be rolled back to the last time the device properly booted. If the problem persisted, then **live boot media** (such as a USB device that contained a complete bootable OS) could be used as a recovery mechanism. Newer versions of Windows have comparable options.

To protect an endpoint from malware infections, programs are available that can "freeze" a computer to prevent it from accepting any changes from malware. This makes the computer **nonpersistent**. *Persistent* is to continue to exist, so a computer that is nonpersistent means that any changes or additions are not saved when the computer is rebooted and thus returns to its original state.

Servers

Because servers play such a key role in a network infrastructure, the loss of one or more servers that supports a critical application can have a significant impact. In the past, some organizations stockpiled spare parts to replace a part that failed (such as a server's power supply) or even had entire redundant servers as standbys. However, the time it takes to install a new part or add a new server to the network and then load software and backup data was sometimes longer than an organization could tolerate.

Another approach that some organizations take is to design the network infrastructure so that multiple servers are incorporated into the network yet appear to users and applications as a single computing resource. One method to do this is by *clustering* or combining two or more devices to appear as a single unit. A *server cluster* is the combination of two or more servers that are interconnected to appear as one, as shown in Figure 14-1. These servers are connected through both a *public cluster connection* so that clients see them as a single unit as well as a *private cluster connection* so that the servers can exchange data when necessary. There are two types of server clusters. In an *asymmetric server cluster*, a standby server exists only to take over for another server in the event of its failure. The standby server performs no useful work other than to be ready if it is needed. In a *symmetric server cluster*, every server in the cluster performs useful work. If one server fails, the remaining servers continue to perform their normal work as well as that of the failed server.

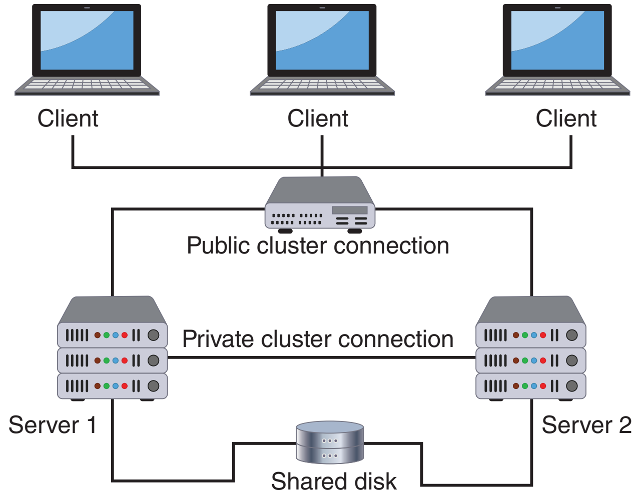


Figure 14-1 Server cluster

Today, however, just as virtualization has reduced the number of physical servers that are needed in a data center, so too has virtualization impacted the number of server clusters that are needed for server redundancy in disaster recovery. Because a virtualized image can be quickly moved to another physical server, the need for server clusters supporting large numbers of physical servers for disaster recovery has diminished. Tools are available so that as one virtual machine is shut down, a copy of that virtual machine is automatically launched (**replication**).

Disks

There are two hardware redundancies for disks that store data. These are RAID and SAN multipath.

RAID A trend in data storage technologies for computers today is to use solid state drives (SSDs), which essentially store data on chips instead of magnetic platters. Because SSDs lack spinning platters, actuator arms with read/write heads, and motors, they are more resistant to failure and are considered more reliable than traditional hard disk drives (HDDs). However, due primarily to lower cost, HDDs still serve as the backbone of data storage for servers.

Because HDDs are mechanical devices, they often are the first component of a system to fail. Some organizations maintain a stockpile of hard drives as spare parts to replace those that fail. Yet how many spare hard drives should an organization keep on hand?

A statistical value that is used to answer this question is **mean time between failures (MTBF)**. MTBF refers to the average (*mean*) amount of time until a component fails, cannot be repaired, and must be replaced. Calculating the MTBF involves taking the total time measured divided by the total number of failures observed. For example, if 15,400 hard drive units were run for 1,000 hours each and that resulted in 11 failures, the MTBF would be (15,400 × 1,000) hours/11, or 1.4 million hours. This MTBF rating can be used to determine the number of spare hard drives that should be available for a quick replacement. If an organization had 1,000 hard drives operating continuously with an MTBF rating of 1.4 million hours, it could be expected that one drive would fail every 58 days, or 19 failures over three years. This data can help an organization know how many spare hard drives are needed.

CAUTION The MTBF certainly does not mean that a single hard drive is expected to last 1.4 million hours (159 years)! MTBF is a statistical measure and, as such, cannot predict anything for a single unit.

Instead of waiting for a hard drive to fail, a more proactive approach can be used. A system of hard drives based on redundancy can be achieved through using a technology known as **RAID (Redundant Array of Independent Drives** or **Redundant Array of Inexpensive Disks)**, which uses multiple hard disk drives for increased reliability and performance. RAID can be implemented through either software or hardware. Software-based RAID is implemented at the operating system level, while hardware-based RAID requires a specialized hardware controller either on the client computer or on the array that holds the RAID drives.

CAUTION Although some motherboards have built-in RAID, this is simply BIOS-assisted software RAID and is usually proprietary and nonstandard. It is commonly known as "Fake RAID."

There are several standard RAID configurations (called *levels*). Additional levels include "nested" levels that often combine two other RAID levels. For example, RAID Level 10 is a combination of RAID Level 0 and Level 1. With nested RAID, the elements can be either individual disks or entire RAIDs.

The most common levels of RAID are Level 0, 1, 5, 6, and 10. Descriptions of several of these common levels include the following:

- *RAID Level 0 (striped disk array without fault tolerance).* RAID 0 technology is based on *striping*. Striping partitions divides the storage space of each hard drive into smaller sections (*stripes*), which can be as small as 512 bytes or as large as several megabytes. Data written to the stripes is alternated across the drives, as shown in Figure 14-2. Although RAID Level 0 uses multiple drives, it is not fault tolerant; if one of the drives fails, all the data on that drive is lost.

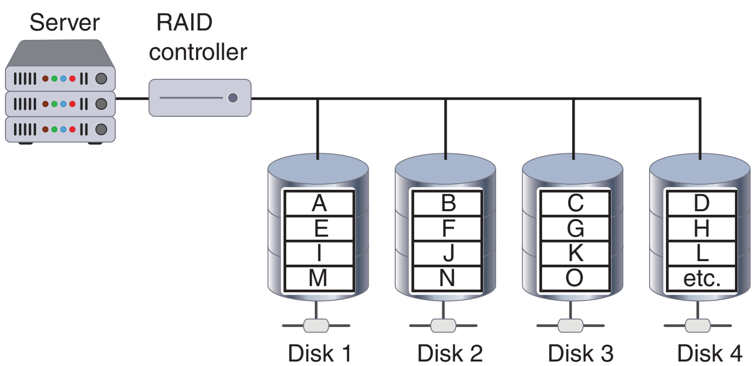


Figure 14-2 RAID Level 0

- *RAID Level 1 (mirroring).* RAID Level 1 uses *disk mirroring*. Disk mirroring involves connecting multiple drives in the server to the same disk controller card. When a request is made to write data to the drive, the controller sends that request to each drive; when a read action is required, the data is read twice, once from each drive. By "mirroring" the action on the primary drive, the other drives become exact duplicates. In case the primary drive fails, the other drives take over with no loss of data. This is shown in Figure 14-3. A variation of RAID Level 1 is to include *disk duplexing*. Instead of having a single disk controller card that is attached to all hard drives, disk duplexing has separate cards for each disk. A single controller card failure affects only one drive. This additional redundancy protects against controller card failures.

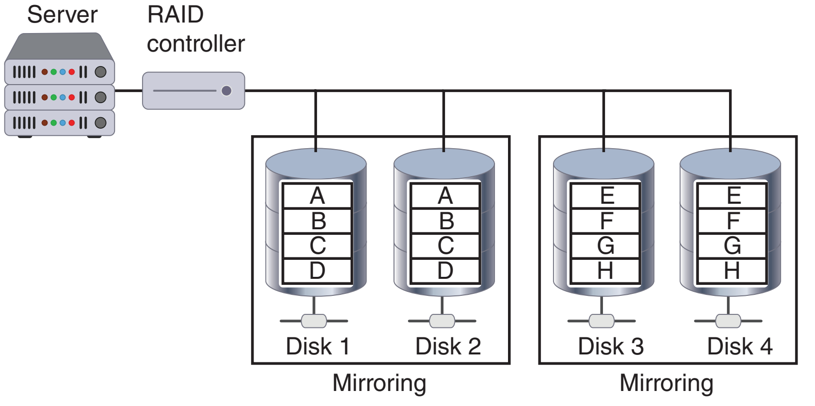


Figure 14-3 RAID Level 1

- *RAID 5 (independent disks with distributed parity).* RAID Level 5 distributes *parity* data (a type of error checking) across all drives instead of using a separate drive to hold the parity error checking information. Data is always stored on one drive while its parity information is stored on another drive, as shown in Figure 14-4. Distributing parity across other disks provides an additional degree of protection.

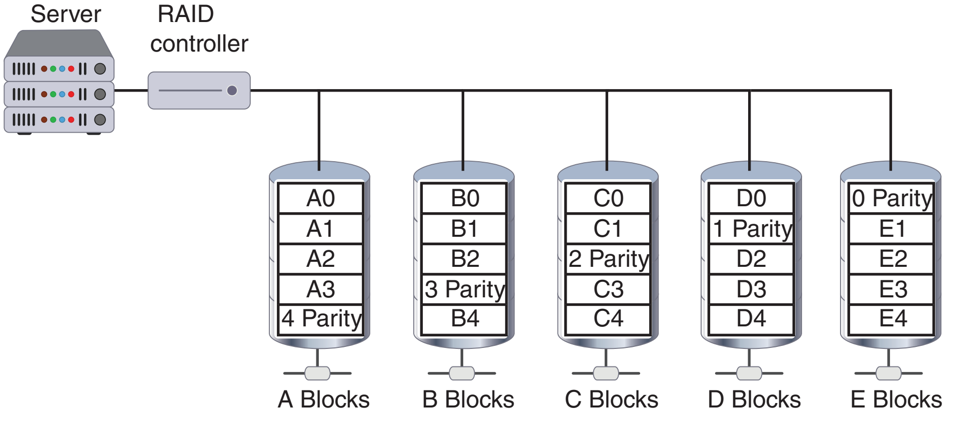


Figure 14-4 RAID Level 5

Different levels of RAID have different use cases. For example, RAID Level 0 is ideal for non-critical storage of data that must be read/written at a high speed, such as on an image retouching or video editing station. RAID Level 1 is best for mission-critical storage, such as for accounting systems. It is also suitable for small servers in which only two data drives will be used. RAID Level 5 is a good all-round system that combines efficient storage with excellent security and decent performance. It is best for file and application servers that have a limited number of data drives.

CAUTION Although all levels of RAID except Level 0 can offer protection from a single drive failure, RAID is not intended to replace data backups but only to provide increased reliability and performance.

SAN Multipath In the enterprise, the standard data storage facilities and networking protocols cannot always cope with the need to store and transmit large volumes of data. Most organizations have turned to using a **storage area network (SAN)**, which is a dedicated network storage facility that provides access to data storage over a high-speed network. SANs consolidate different storage facilities—disk arrays, tape libraries, and even "optical jukeboxes" that can load thousands of discs by robotic arms—so they are accessible to servers. The different storage facilities actually appear as a single pool of locally attached devices.

NOTE 4

SANs can also support SAN-to-SAN replication: a SAN at Site A can update a duplicate SAN at Site B to serve as a backup copy. This type of replication does not impact the performance of normal servers and thus is very efficient.

Multipath is a technique for creating more than one physical path between devices and a SAN. If one path is interrupted (due to a cable break or a technician unplugging the wrong cable) multipath would simply redirect the broken connection to another path. Multipath can also assist with increasing the speed of a SAN by spreading connections across multiple paths so that a "bottleneck" is not created.

Networks

Due to the critical nature of connectivity today, redundant networks also may be necessary. A redundant network waits in the background during normal operations and uses a replication scheme to keep its copy of the live network information current. If a disaster occurs, the redundant network automatically launches so that it is transparent to users. A redundant network ensures that network services are always accessible.

NOTE 5

Some enterprises contract with more than one Internet service provider (ISP) for remote site network connectivity. In case the primary ISP is no longer available, the secondary ISP will be used. Enterprises can elect to use redundant fiber-optic lines to the different ISPs, each of which takes a diverse path through an area.

Virtually all network hardware components can be duplicated to provide a redundant network. Some manufacturers offer switches and routers that have a primary active port as well as a standby failover network port for physical redundancy. If a special packet is not detected in a specific time frame on the primary port, the failover port automatically takes over. Load balancers can provide a degree of network redundancy by blocking traffic to servers that are not functioning. Also, multiple redundant switches and routers can be integrated into the network infrastructure. Virtual software-defined network (SDN) controllers can increase network reliability and may lessen the need for redundant equipment. One technique that an SDN controller can use to increase network reliability is to set up multiple paths between the origin and the destination so that the network is not impacted by the outage of a single link.

NOTE 6

Load balancers are covered in Module 9, and SDNs are covered in Module 10.

Another network hardware element that can be configured for redundancy is the network interface card (NIC) adapters. A server that performs a critical function can have up to 32 physical adapters installed and then configured into one or more software-based virtual network adapters. This is called **NIC teaming** and provides redundancy as well as faster performance.

Power

Maintaining electrical power is essential when planning for redundancy. Critical devices such as servers can be fitted with a **dual power supply** so that if one power supply fails, the other can take over. A dual power supply from Athena Power is shown in Figure 14-5. A managed **power distribution unit (PDU)** is a device fitted with multiple electrical outputs and is designed to distribute electric power, especially to racks of computers and networking equipment located within a data center.

Source: Athena Power

Figure 14-5 Dual power supply

An **uninterruptible power supply (UPS)** is a device that maintains power to equipment in case of an interruption in the primary electrical power source. A UPS is more than just a big battery, however. UPS systems also can communicate with the network operating system on a server to ensure that an orderly shutdown occurs. Specifically, if the power goes down, a UPS can complete the following tasks:

- Send a message to the network administrator's computer, or page or telephone the network manager, to indicate that the power has failed.
- Notify all users that they must finish their work immediately and log off.
- Prevent any new users from logging on.
- Disconnect users and shut down the server.

There are two primary types of UPSs. An *offline UPS* is considered the least expensive and simplest solution. During normal operation, the equipment being protected is served by the standard primary power source. The offline UPS battery charger is also connected to the primary power source to charge its battery. If power is interrupted, the UPS quickly (usually within a few milliseconds) begins supplying power to the equipment. When the primary power is restored, the UPS automatically switches back into standby mode. An *online UPS* is always running off its battery while the main power runs the battery charger. An advantage of an online UPS is that it is not affected by dips or sags in voltage. An online UPS can clean the electrical power before it reaches the server to ensure that a correct and constant level of power is delivered to the server. The online UPS also can serve as a surge protector, which keeps intense spikes of electrical current, common during thunderstorms, from reaching systems.

Because a UPS can supply power for a limited amount of time, some organizations turn to a backup **generator** to create power. Backup generators can be powered by diesel, natural gas, or propane gas to generate electricity. Unlike portable residential backup generators, commercial backup generators are permanently installed as part of the building's power infrastructure. They include automatic transfer switches that can, in less than one second, detect the loss of a building's primary power and switch to the backup generator.

Sites

Just as redundancy can be planned for servers, storage, networks, and power, it also can be planned for the entire site. A major disaster such as a flood or hurricane can inflict such extensive damage to a building that the organization must temporarily move to another location. Many organizations maintain redundant recovery sites in case this occurs. Three basic types of redundant sites are used: hot sites, cold sites, and warm sites.

- *Hot site*. A **hot site** is generally run by a commercial disaster recovery service that allows a business to continue computer and network operations to maintain business continuity. A hot site is essentially a duplicate of the production site and has all the equipment needed for an organization to continue running, including office space and furniture, telephone jacks, computer equipment, and a live telecommunications link. Data backups of information can be quickly moved to the hot site, and in some instances the production site automatically synchronizes all its data with the hot site so that all data is immediately accessible. If the organization's data processing center becomes inoperable, typically all data processing operations can be moved to a hot site within an hour.
- *Cold site*. A **cold site** provides office space, but the customer must provide and install all the equipment needed to continue operations. In addition, there are no backups of data immediately available at this site. A cold site is less expensive but requires more time to get an enterprise in full operation after a disaster.
- *Warm site*. A **warm site** has all the equipment installed but does not have active Internet or telecommunications facilities and does not have current backups of data. This type of site is much less expensive than constantly maintaining those connections as required for a hot site; however, the amount of time needed to turn on the connections and install the backups can be as much as half a day or more.

NOTE 7

Businesses usually have an annual contract with a company that offers hot and cold site services with a monthly service charge. Some services also offer data backup services so that all company data is available regardless of whether a hot site or cold site is used.

However, it is important when creating alternate sites to consider **geographic dispersal**. Instead of all sites being clustered in a limited geographic area, they should be distributed across a larger area to mitigate the impact of an environmental disasters (such as hurricanes and tornados) and man-made disasters (such as terrorist attacks and transport accidents). Geographic dispersal should also be considered when using cloud computing in conjunction with sites. Some organizations back up their applications and data to the cloud and then, if a disaster occurs, restore it to hardware in a hot, cold, or warm site. Other organizations also back up to the cloud but, instead of restoring to hardware at a site, they restore to virtual machines in the cloud, which then can be accessed from almost any location. This approach reduces or even eliminates the need for maintaining sites. When creating a cloud platform, the customer can often choose the region in which the data will reside.

Data

A **data backup** is copying information to a different medium and storing it so that it can be used in the event of a disaster. Backing up data involves data backup calculations, creating different types of data backups, and storing the backups.

Data Backup Calculations Two elements are used in the calculation of when backups should be performed. The first is known as the **recovery point objective (RPO)**, which is defined as the maximum length of time that an organization can tolerate between backups. Simply put, RPO is the "age" of the data that an organization wants the ability to restore in the event of a disaster. For example, if an RPO is six hours, this means that an organization wants to be able to restore systems back to the state they were in no longer than six hours ago. To achieve this, it is necessary to make backups at least every six hours; any data created or modified between backups will be lost.

Related to the RPO is the **recovery time objective (RTO)**. The RTO is the length of time it will take to recover the data that has been backed up. An RTO of two hours means that data can be restored within that time frame.

Types of Data Backups One of the keys to backing up files is knowing which files need to be backed up. Software that is used to create backups of files can internally designate which files have already been backed up by setting an archive bit in the properties of the file. A file with the archive bit cleared (set to 0) indicates that the file has been backed up. Any time the contents of that file are changed, the archive bit is set (to 1), meaning that this modified file now needs to be backed up. The archive bit is illustrated in Figure 14-6.

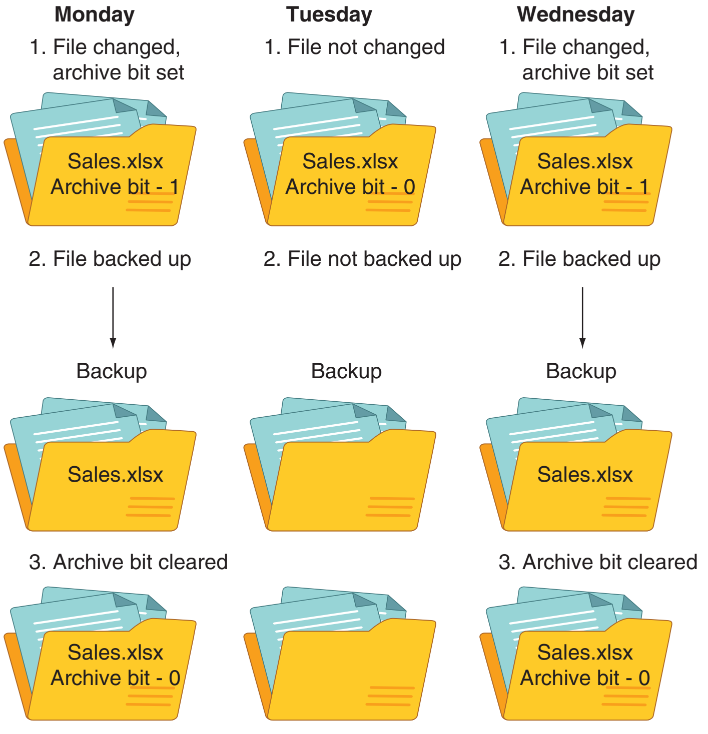


Figure 14-6 Archive bit

There are different types of backups, and three of the most common are summarized in Table 14-3. The archive bit is not always cleared after each type of backup; this provides additional flexibility regarding which files should be backed up.

Table 14-3 Types of data backups

Type of backup	How used	Archive bit after backup	Files needed for recovery
Full backup	Starting point for all backups	Cleared (set to 0)	The full backup is needed.
Differential backup	Backs up any data that has changed since last full backup	Not cleared (set to 1)	The full backup and only last differential backup are needed.
Incremental backup	Backs up any data that has changed since last full backup or last incremental backup	Cleared (set to 0)	The full backup and all incremental backups are needed.

The drawback to backing up only files (called a *file backup*) is that it does not provide the means to restore the apps that created the files or the operating system. An alternative is to perform an **image backup** that captures the entire contents of the disk. This enables an entire restoration of the contents of the disk to a new hard disk or computer. Image backups can also restore a single file or directory and can create an incremental image based on the previous image created.

A more comprehensive backup technology than file backups or image backups is known as *continuous data protection (CDP)*. As its name implies, CDP performs continuous data backups that can be restored immediately, thus providing excellent RPO and RTO times. CDP maintains a historical record of all changes made to data by constantly monitoring all writes to the hard drive. It does this by creating a **snapshot** of the data, which is essentially a series of "reference markers" of the data at a specific point in time.

NOTE 8

Many CDP products even let users restore their own documents. A user who accidentally deletes a file can search the CDP system by entering the name of the document and then view the results through an interface that looks like a web search engine. Clicking the desired file then restores it. For security purposes, users may search only for documents for which they have permissions.

Storing Backups A key consideration with backups is where they should be stored. It is not required that only the original backup be stored; instead, a **backup copy** (a copy of the original backup) can—and should—be made and stored in more than one location for additional protection. The options for storing backups are onsite, offsite, and the cloud.

Onsite Once a backup has been created, it is then stored locally onsite on media (local magnetic disk, optical disk, or magnetic tape) that is accessible. It can also be stored on a SAN or a **network-attached storage (NAS)** device. (A NAS is a single storage device that serves files over the network and is relatively inexpensive.) The advantage of storing the backup onsite is that it allows quick access to data (for example, to retrieve a file that was erroneously deleted by a user). Even if the backup is stored offline, it can quickly be made available. The disadvantages of storing a backup onsite are security (it may be vulnerable to theft) and damage (an environmental disaster or man-made disaster that impacts the data center will likewise impact the data backup).

Offsite In the past, offsite backups were typically stored in a secure location such as a local bank vault. Later services became available in which a courier would routinely visit the enterprise and pick up magnetic tapes or hard drives that contained the most recent backups and transport them to the vendor's secure site. However, the location selection of where the media should be stored was often an issue (called **distance considerations**) due to security concerns (transporting media over long distances increased the risk of accident or theft) or a delay in accessing the media in the event the data backup had to be quickly restored. This is because at offsite locations it was stored offline instead of online.

NOTE 9

One of the most secure offsite backup facilities is in a former salt mine facility in Kansas. It is 650 feet (198 meters) or about 45 stories beneath the surface. The facility is encased in solid stone and covers the equivalent of 35 football fields with more than 1.7 million square feet (0.52 million square meters) of storage space. The temperature and humidity levels remain constant year round. The site protects against natural disasters (tornado, hurricane, flooding, etc.) as well as man-made disasters (explosion, fire, civil unrest, etc.). It serves as the largest single storage facility for the movie and television film industry worldwide.

Cloud Today many organizations store their offsite backups using an online cloud repository. These online sites often use CDP to continually back up data and provide the highest degree of protection today to users. There are several Internet services available that provide similar features:

- *Automatic continuous backup*. Once the initial backup is completed, any new or modified files are also backed up. Usually the backup software "sleeps" while the computer is being used and performs backups only when there is no user activity. This helps to lessen any impact on the computer's performance or Internet speed.
- *Universal access*. Files backed up through online services can be made available to another computer.
- *Delayed deletion*. Files that are copied to the online server will remain accessible for up to 30 days before they are deleted. This allows a user to have a longer window of opportunity to restore a deleted file.
- *Online or media-based restore*. If a file or the entire computer must be restored, then this can be done online. Some services also provide the option of shipping backup files on a new media device such as an SSD or on optical media.

Most security experts recommend that at minimum, a *3-2-1 backup* plan should be used. This plan says that there should always be *three* different copies of backups (that does not count the original data itself) on at least *two* different types of storage media, and *one* of the backups should be stored at a different location such as the cloud or in a remote site.

NOTE 10

Home users should likewise follow the 3-2-1 backup plan by always maintaining *three* different copies of backups (that does not count the original data itself) by using at least *two* different types of media on which to store these backups (a separate hard drive, an external hard drive, a USB device, etc.) and storing *one* of the backups offsite.

TWO RIGHTS & A WRONG

1. A business continuity plan (BCP) is the development of a strategic document that provides alternative modes of operation for business activities that, if interrupted, could result in a significant loss to the enterprise.
2. Mean time to recovery (MTTR) is the average amount of time that it will take a device to recover from a failure that is not a terminal failure.
3. RAID can be implemented only through hardware.

See Appendix B for the answer.

POLICIES

CERTIFICATION

3.7 Given a scenario, implement identity and account management controls.

5.3 Explain the importance of policies to organizational security.

Another means of cybersecurity resilience is through a security policy. It is important to know the definition of a policy and the different types of policies that are used.

Definition of a Policy

Several terms describe the "rules" that a user follows in an organization. A *standard* is a collection of requirements specific to the system or a procedure that must be met by everyone. For example, a standard might describe how to secure a computer at home that remotely connects to the organization's network. Users must follow this standard if they want to be able to connect. A *guideline* is a collection of suggestions that should be implemented. These are not requirements to be met but are strongly recommended. A **policy** is a document that outlines specific requirements or rules that must be met. A policy is considered the correct tool for an organization to use when establishing security because a policy applies to a wide range of hardware or software (it is not a standard) and is required (it is not just a guideline).

NOTE 11

If the question "What is a security policy?" were posed to both a manager and a security technician, the answers would likely be different. A manager might say that a security policy is a set of management statements that defines an organization's philosophy of how to safeguard its information. A security technician might respond that a security policy is the cybersecurity configuration settings in a system. These two responses are not conflicting but are complementary: a written policy dictates what technology configuration settings should be used.

A policy generally has these characteristics:

- Communicates a consensus of judgment
- Defines appropriate behavior for users
- Identifies what tools and procedures are needed
- Provides directives for human resources action in response to inappropriate behavior
- May be helpful if it is necessary to prosecute violators

NOTE 12

The purpose of security policies is not to serve as a motivational tool to force users to practice safe security techniques. The results from research have indicated that the specific elements of a security policy do not have an impact on user behavior. Relying on a security policy as the exclusive defense mechanism will not provide adequate security for an organization.

Types of Security Policies

There are several types of security policies. These include account management policies, mobile device location-based policies, personnel policies, organizational policies, and data policies.

Account Management Policies

Account management involves the restrictions regarding user accounts. This includes not only who is authorized to access resources, but when, how, and from what location they can do so. Common account management "sub-policies" are **credential policies** that address requirements for authentication credentials, such as the length and complexity of passwords. Credential policies apply to all personnel (users, administrators, and third parties) but to also devices and service accounts.

Unlike most other written policies that an organization may have written, account management policies can be enforced through technology. There are different technologies that can be used to enforce these policies. In a Microsoft environment, these can be enforced through Windows Group Policy, Active Directory, and Cloud App Security.

Group Policy Managing login credentials such as passwords in user accounts (credential management) can be accomplished by setting technology restrictions regarding the creation and use of passwords. Although these restrictions can be performed on a user-by-user basis, this quickly becomes cumbersome and is a security risk: it is too easy to overlook one setting in one user account and create a security vulnerability.

A preferred approach is to assign privileges to a group of common users. In a Microsoft Windows environment, controls over user and computer accounts can be set through a feature known as Group Policy. Group Policy settings can be made on an individual computer (*Local Group Policy*) but will only apply to that computer, while settings applied to users in a domain will apply to all users (*Domain Group Policy*).

NOTE 13

If a Local Group Policy setting is different from a Domain Group Policy setting, the Domain Group Policy takes precedence.

Establishing controls on authentication credentials such as passwords and on the accounts can be configured by using Group Policy. Several of the common domain policy settings called Microsoft setting objects are listed in Table 14-4.

NOTE 14

Other common password parameters, such as length and expiration, can also be set through Group Policy.

Active Directory Microsoft's directory service manager, Active Directory, can also be used to enforce account management policies. An **access policy** allows a network administrator to create **account permissions** (the privileges that the user is given) and restrictions based on a role-based access control scheme.

Table 14-4 Windows Group Policy password settings

Setting name	Microsoft setting object	Description	Recommended setting
Password reuse	Enforce password history	Determines the number of unique new passwords a user must use before an old password can be reused (from 0 to 24).	24 new passwords
Password history	Minimum password age	Determines how many days a new password must be kept before the user can change it (from 0 to 999). This setting is designed to work with the Enforce password history setting so that users cannot quickly reset their passwords the required number of times and then change back to their old passwords.	1 day
Password complexity	Passwords must meet complexity requirements	Determines whether the following are used in creating a password: Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters; must contain characters from three of the following four categories—English uppercase characters (A through Z), English lowercase characters (a through z), digits (0 through 9), and nonalphabetic characters (!, $, #, %).	Enabled
Network Location	Network List Manager policies	Network type can be set as Not Configured, Public, or Private.	Private
Account Audits	Audit Logon Events and Audit Account Logon Events	Logon Events audits every user attempt to log on and off a computer, while Audit Accounts Logon Events logs every event generated on a computer.	Enabled

NOTE 15

Role-based access control is covered in Module 13.

Another setting is a **time-based login** based on **time of day** restrictions can be used to limit when a user can log in to their account to access resources. When setting these restrictions, a network administrator would typically indicate the times a user is restricted from accessing the system or resources. Figure 14-7 illustrates time-based login implemented by indicating the specific days and times.

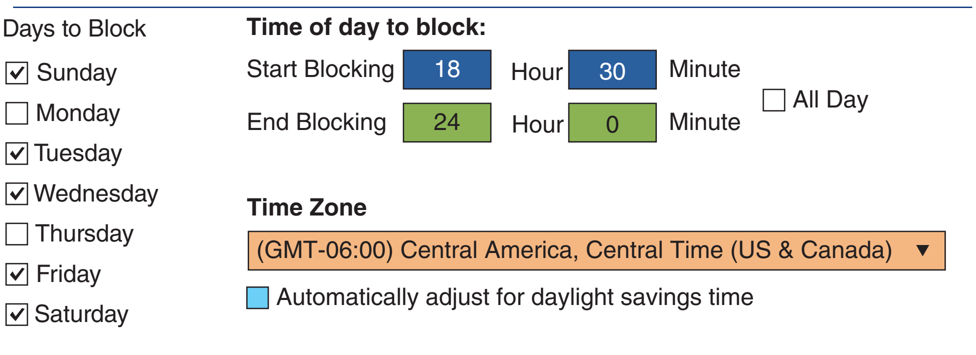


Figure 14-7 Time-based login

Cloud App Security A growing set of enforcement technologies is based on the accumulation and analysis of real-time data that is processed in the cloud. These give a higher level of protection over setting static policies found in Group Policy and Active Directory.

Suppose users access their online account from Nashville. However, 10 minutes later someone tries to access that same user account from Tampa or even Beijing. The Microsoft Cloud App Security feature **Impossible Travel** would deny the second login and generate a security alert because it is not possible for someone to travel that distance within that time. Another feature is **Risky IP address**, which examines the IP address that was used to attempt a login and compares it against a list of IP addresses involved in malicious activities.

NOTE 16

Other Cloud App Security features include Activity from Infrequent Country, Activity from Anonymous IP Address, Activity Performed by Terminated User, Suspicious Inbox Forwarding, Unusual Multiple File Download Activities, and Unusual File Share Activities.

If a suspicious login is trapped by Cloud App Security, generally an automatic and immediate **lockout** is placed on the account, meaning that the account cannot be accessed until a security administrator reviews the incident and removes the lockout. This is different from a **disablement** in which the account requires an administrator to suspend the account. A lockout occurs automatically while a disablement requires manual intervention.

NOTE 17

System administrators cannot perform a lockout but only a disablement.

Mobile Device Location-Based Policies

Policies can also enforce what mobile devices can access or perform based on the location of the device. The technologies for identification and enforcement include the following:

- *Geolocation*. Mobile devices typically support geolocation, or identifying the geographical location of the device. When finding a person carrying a mobile device, geolocation also identifies the location of a close friend or displays the address of the nearest coffee shop. Location services are used extensively by social media, navigation systems, weather systems, and other mobile-aware applications.
- *Geo-tagging*. Geo-tagging is adding geographical identification data to media such as digital photos taken on a mobile device. A user who, for example, posts a photo on a social networking site may inadvertently identify a private location to anyone who can access the photo.
- *Geofencing*. Geofencing is using the device's GPS to define geographical boundaries where an app can be used.

NOTE 18

Geofencing is commonly used in law enforcement. An individual under house arrest is fitted with an ankle bracelet that alerts authorities if the individual leaves the house.

These technologies can be used for identification and enforcement of how a mobile device can be used based on its location. These are enforced automatically as the device moves into and out of a specific network zone. For example, a tablet containing patient information that leaves the hospital grounds or an employee who attempts to enter a restricted area with a device can result in an alert sent to an administrator. Policies can also include such actions as disabling the camera to prevent users from taking unauthorized pictures in specific geographic locations, disabling automatic screen lock so that users do not have to unlock their device repeatedly while at work, or disabling apps and browsers entirely.

NOTE 19

Geolocation, geo-tagging, and geofencing are all covered in Module 5.

Personnel Policies

Several policies relate to matters of personnel. While these policies cannot be enforced through technology as with account management policies and mobile device location, nevertheless, they are important for creating cybersecurity resiliency. The personnel policies include separation of duties, job rotation, mandatory vacations, clean desk space, least privilege, onboarding and offboarding, and acceptable use.

Separation of Duties News headlines such as "County Official Charged with Embezzlement" appear all too frequently. Often this fraud results from a single user being trusted with a set of responsibilities that place the person in complete control of the process. For example, one person may be given total control over the collection, distribution, and reconciliation of money. If no other person is involved, it might be too tempting for that person to steal, knowing that nobody else is watching and that there is a good chance the fraud will go undetected. To counteract this possibility, most organizations require that more than one person be involved with functions that relate to handling money, because it would require a conspiracy of all the individuals for fraud to occur.

Likewise, a foundational principle of computer access control is not to give one person total control. Known as **separation of duties**, this practice requires that if the fraudulent application of a process could potentially result in a breach of security, the process should be divided between two or more individuals. For example, if the duties of the owner and the custodian are performed by a single individual, it could provide that person with total control over all security configurations. It is recommended that these responsibilities be divided so that the system is not vulnerable to the actions performed by a single person.

Job Rotation Another way to prevent one individual from having too much control is to use **job rotation**. Instead of one person having sole responsibility for a function, individuals are periodically moved from one job responsibility to another. Employees can rotate either within their home department or across positions in other departments. The best rotation procedure involves multiple employees rotating across many positions for different lengths of time to gain exposure to different roles and functions.

Job rotation has several security advantages. It limits the amount of time that individuals are in a position to manipulate security configurations. It also helps to expose any potential avenues for fraud by having multiple individuals with different perspectives learn about the job and uncover vulnerabilities that someone else may have overlooked.

NOTE 20

Job rotation also has disadvantages. In some cases, employees may not be in a specific job long enough to develop proficiency, and productivity may be lost in the time it takes to train employees in new tasks. Also, job rotation is often limited to less specialized positions. For these reasons, job rotation might not always be practical.

Mandatory Vacation In many fraud schemes, the perpetrator must be present every day to continue the fraud or keep it from being exposed. Many organizations require **mandatory vacations** for all employees to counteract this. For sensitive positions within an organization, an audit of the employees' activities is usually scheduled while they are away on vacation.

Clean Desk Space A **clean desk space** policy is designed to ensure that all confidential or sensitive materials, either in paper form or electronic, are removed from a user's workspace and secured when the items not in use or employees leaves their workspace. This not only reduces the risk of theft or "prying eyes" reading confidential information, but it can also increase the employee's awareness about the need to protect sensitive information. A clean desk space policy may include such statements as the following:

- Computer workstations must be locked when the workspace is unoccupied and turned off at the end of the business day.
- Confidential or sensitive information must be removed from the desk and locked in a drawer or safe when the desk is unoccupied and at the end of the work day.
- File cabinets must be kept closed and locked when not in use or not attended, and keys may not be left at an unattended desk.
- Laptops must be either locked with a locking cable or locked in a drawer or filing cabinet.
- Mass storage devices such as USB flash drives or portable external hard drives must be locked in a drawer or filing cabinet.
- Paper documents no longer needed must be shredded using the official shredder bins.
- Printouts should be immediately removed from the printer.
- Whiteboards containing confidential or sensitive information should be erased.

Least Privilege As its name implies, the cybersecurity principle of **least privilege** means that only the minimum amount of privileges necessary to perform a job or function should be allocated. This helps reduce the attack surface by eliminating unnecessary privileges that could provide an avenue for an attacker. Least privilege should apply both to user accounts and to processes running on the system.

NOTE 21

One of the reasons home computers are so frequently and easily compromised is that they use an account with administrative rights. A more secure option is to use an account with lower privileges and then invoke administrative privileges only when necessary.

Onboarding and Offboarding Employee **onboarding** refers to the tasks associated with hiring a new employee. **Background checks** are now considered essential when hiring a new employee. In addition, viewing the social media posts of potential candidates (**social media analysis**) can also reveal important insights into applicants.

CAUTION

Many serious issues surround social media analysis of posts made by applicants and employees. For example, while looking at social media posts, employers could easily learn other details such as religion, disability, or pregnancy of an applicant. By law, hiring decisions cannot take these into account, but just knowing them could introduce bias in hiring decisions. Yet if an employer ignores a history of inflammatory social media posts, it could expose that employer to liability. One solution is to use artificial intelligence (AI) software to perform social media analysis.

Once an employee is "onboard," several steps should be taken. Most new hires are required to sign an employee **nondisclosure agreement (NDA)** to make clear to employees that they may not disclose trade secrets and confidential information without permission. In addition, the setup and account configuration of new employees must be performed. In a common Microsoft Windows environment using Active Directory, the steps may include provisioning the new computer (the new computer can be added to the Active Directory domain and then moved into a specific organizational unit (OU), or the computer account can be set up inside the correct OU before it is joined), creating email mailboxes, adding user accounts to groups, and creating a home folder. It is also important to review the security settings of the different accounts to ensure that they fit within the policy guidelines of the enterprise.

Employee **offboarding** entails actions to be taken when an employee leaves an enterprise. The necessary steps should include backing up all employee files from the local computer and file server, archiving email, forwarding email to a manager or coworker, hiding the name from the email address book, etc. In addition, when an employee leaves an organization, that employee's accounts should be immediately disabled.

NOTE 22

Orphaned accounts are user accounts that remain active after an employee has left an organization and are a serious security risk. For example, an employee who left under unfavorable circumstances might be tempted to "get even" with the organization by stealing or erasing sensitive information through her account. To assist with controlling dormant accounts, *account expiration* can be used. Account expiration is the process of setting a user's account to expire. Account expiration can be explicit, in that the account expires on a set date, or it can be based on a specific number of days of inactivity.

Acceptable Use Policy (AUP) An **acceptable use policy (AUP)** is a written policy that defines the actions users may perform while accessing systems and networking equipment. The users are not limited to employees but should also include vendors, contractors, and visitors, each with different privileges. AUPs typically cover all computer use, including mobile devices.

An AUP may have an overview regarding what is covered by the policy, as in the following sample:

> *Internet/intranet/extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, and web browsing, are the property of the Company. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers, in the course of normal operations. Personal use is strictly prohibited.*

The AUP usually provides explicit prohibitions regarding security and proprietary information:

> *Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.*
>
> *All computers and laptops should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging off when the host is unattended.*
>
> *Postings by employees from a Company device or using a Company email address to personal blogs or personal social media accounts is prohibited.*

Unacceptable use may also be outlined by the AUP, as in the following sample:

> *The following actions are not acceptable ways to use the system:*
>
> - *Introduction of malicious programs into the network or server*
> - *Revealing your account password to others or allowing use of your account by others, including family and other household members when work is being done at home*
> - *Using the Company's computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction*
> - *Any form of harassment via email, telephone, text, or social media, whether through language, frequency, or size of messages*
> - *Unauthorized use, or forging, of email header information*

Organizational Policies Several policies relate to the management and functioning of the organization as a whole (**organizational policies**). These include the following:

- *Change management.* Change management refers to a formal process for making modifications to a system and keeping track of those changes. A **change management policy** is a written document that defines the types of changes that can be made and under what circumstances.
- *Change control.* A **change control policy** stipulates the processes to be followed for implementing system changes. It involves communicating the changes to relevant stakeholders and reviewing the processes for validating a change. Change control should be made following the standards set in the change management policy.
- *Asset management*. An **asset management policy** provides the guidelines and practices that govern decisions about how assets should be acquired, maintained, and disposed.

Data Policies Organizations also need policies to address data. This includes how it should be classified, governed, and retained.

Data classification policy Not all data is the same: Some is critical and must be protected at all costs (such as research and development data), while other data is of lesser importance (such as marketing data). Labels can be assigned to similar data elements based on their importance (sometimes called their *sensitivity level*), a process known as data classification. A written policy that addresses assigning labels is a **data classification policy**.

NOTE 23

The measure of the importance of data can often be gauged by asking the basic question, *what would an unexpected loss or disclosure of this information mean to us?*

In a commercial (corporate) environment, no standards exist for data classification. Some organizations simply use *Public* and *Confidential* as their only classifications. However, using multiple data classification levels can help clarify the data's importance and prevent data that is "mostly public but a little confidential" from being mislabeled. Table 14-5 lists a typical commercial data classification from the lowest level of sensitivity to the highest.

Table 14-5 Commercial data classification levels (lowest to highest)

Classification level	Description	Example
Public	Data that is the least sensitive and would cause only a small amount of harm if disclosed	Number of current employees
Proprietary	Data disclosed outside the company on only a limited basis to trusted third parties; an unexpected disclosure could reduce the company's competitive advantage	Nontechnical specifications for a new product
Private	Data that might not harm the company itself but could cause damage to others	Human resources data of employees
Confidential	Data used internally within the company; a public disclosure would cause significant harm to the organization	News of an impending merger or acquisition
Sensitive	Data that could cause catastrophic harm to the company if disclosed	Technical specifications for a new product

NOTE 24

When considering which classification a data element should be assigned, the confidentiality of the data should be considered along with its integrity and availability.

Government data classifications have continued to evolve. At one time, the classification levels were *top secret*, *secret*, *confidential*, *sensitive but unclassified (SBU)*, and *unclassified*, but now only the first three levels are used (*top secret*, *secret*, and *confidential*). The level of sensitivity is based on a calculation of the damage to national security that the information's disclosure would cause.

Data governance policy A **data governance policy** is a series of formal guidelines regarding the data itself. This includes who is responsible for the data, how it can be accessed, how it should be used, and how its integrity can be maintained.

Data retention policy A **data retention policy** (also called a *records retention policy*) specifies how long data should be retained after it has fulfilled its initial purpose. This policy should outline the business reasons or regulatory requirements for retaining the data, how it can be accessed and by whom while it is in retention, how it should be disposed, and how that disposal is documented.

TWO RIGHTS & A WRONG

1. A policy is a collection of suggestions that should be implemented.
2. Risky IP address examines the IP address that was used to attempt a login and compares it against a list of IP addresses involved in malicious activities.
3. Employee offboarding entails actions to be taken when an employee leaves an enterprise.

See Appendix B for the answer.

VM LAB You're now ready to complete the live, virtual machine labs for this module. The labs can be found in the Practice It folder in each MindTap module.

SUMMARY

- Business continuity, which is the ability of an organization to maintain its operations and services in the face of a disruptive event, involves identifying exposure to threats, creating preventive and recovery procedures, and then testing the procedures to determine if they are sufficient. A business continuity plan (BCP) is a document that provides alternative modes of operation for business activities. One important tool in BCP is a business impact analysis (BIA), which analyzes the most mission-essential business functions and identifies critical systems and single points of failure.
- While business continuity planning and testing look at the needs of the business as a whole in recovering from a catastrophe, a subset of BCP focuses on continuity in the context of IT. IT contingency planning involves developing an outline of procedures to follow in the event of a major IT incident or an incident that directly impacts IT. This outline is called a disaster recovery plan (DRP), which is the plan for restoring IT functions and services to their former state. Disaster recovery planning involves creating, implementing, and testing DRPs. Most DRPs also cover a standard set of topics. One common topic is the sequence of reinstating different systems.
- One way to prevent certain issues from crippling an enterprise is to incorporate resilience, also called fault tolerance, into IT systems. Because no IT system can ever be completely free of faults, the solution to fault tolerance is to build in redundancy, or the use of duplicated equipment to improve the availability of the system. Due to how they are used, endpoints rarely require hardware redundancy. Because servers play such a key role in a network infrastructure, the loss of a single server that supports a critical application can have a significant impact. A common approach is for the organization to design the network infrastructure so that multiple servers are incorporated into the network yet appear to users and applications as a single computing resource. One method of doing this is by using a server cluster, which is the combination of two or more servers that are interconnected to appear as one. A system of hard drives based on redundancy can be achieved through using a technology known as RAID, which uses multiple hard disk drives for increased reliability and performance. SAN multipath, a technique for creating more than one physical path between devices and a SAN, can also be used to protect disks.
- Most network hardware components can be duplicated to provide a redundant network. Maintaining electrical power is also essential when planning for redundancy. An uninterruptible power supply (UPS) is a device that maintains power to equipment in the event of an interruption in the primary electrical power source. Because a UPS can supply power for a limited amount of time, some organizations turn to a backup generator to create power. Just as redundancy can be planned for servers, storage, networks, and power, it also can be planned for the entire site. A major disaster such as a flood or hurricane can inflict such extensive damage to a building that the organization may have to temporarily move to another location. Many organizations maintain redundant sites in case this occurs. Three basic types of redundant sites are hot sites, cold sites, and warm sites.
- The most important redundancy is that of the data itself, which is accomplished through data backups. A data backup is copying information to a different medium and storing it so that it can be used in the event of a disaster. The storage location is preferably at an offsite facility. The recovery point objective (RPO) is the maximum length of time that an organization can tolerate between backups. The recovery time objective (RTO) is the length of time it will take to recover data that has been backed up. The three common types of backups are full backup, differential backup, and incremental backup. Another newer backup technology is continuous data protection (CDP), which performs continuous data backups that can be restored immediately, thus providing excellent RPO and RTO times. A key consideration with backups is where they should be stored. Today most organizations store their offsite backups using an online cloud repository.
- A policy is a document that outlines specific requirements or rules that must be met. A security policy is a written document that states how an organization plans to protect the company's information technology assets. There are several types of security policies. Account management involves the restrictions regarding user accounts. This includes not only who is authorized to access resources, but when, how, and from what location they can do so. Unlike most other written policies that an organization may have, written account management policies can be enforced through technology. Different technologies can be used to enforce these policies. In a Microsoft environment, these can be enforced through Windows Group Policy, Active Directory, and Cloud App Security. Policies can also enforce what mobile devices can access or perform based on the location of the device.

- Several policies relate to matters of personnel. These include separation of duties (dividing a process between two or more individuals), job rotation (periodically moving employees from one job responsibility to another), mandatory vacation (requiring that employees take periodic vacations), clean desk space (ensuring that all confidential or sensitive materials, either in paper form or electronic, are removed from a user's workspace and secured), least privilege (assigning permissions only relative to the user's necessary job functions), onboarding and offboarding (tasks associated with when a new employee is hired and when that employee leaves), and acceptable use policy (defines the actions users may perform while accessing systems and networking equipment).
- Several policies relate to the management and functioning of the organization as a whole (organizational policies). Change management refers to a formal process for making modifications to a system and keeping track of those changes. A change management policy is a written document that defines the types of changes that can be made and under what circumstances. A change control policy stipulates the processes to be followed for implementing system changes. It involves communicating the changes to relevant stakeholders and reviewing the processes for validating a change. An asset management policy provides the guidelines and practices that govern decisions about how assets should be acquired, maintained, and disposed.
- A data classification policy identifies types of data. A data governance policy is a series of formal guidelines regarding the data itself. This includes who is responsible for the data, how it can be accessed, how it should be used, and how its integrity can be maintained. A data retention policy (also called a records retention policy) specifies how long data should retained after it has fulfilled its initial purpose. This policy should outline the business reasons or regulatory requirements for retaining the data, how it can be accessed and by whom while it is in retention, and how it should be disposed and how that disposal is documented.

Key Terms

acceptable use policy (AUP)
access policy
Account Audits
account permissions
asset management policy
background checks
backup copy
business continuity plan (BCP)
business impact analysis (BIA)
change control policy
change management policy
clean desk space
cold site
continuity of operation planning (COOP)
credential policies
data backup
data classification policy
data governance policy
data retention policy
differential backup
disablement
disaster recovery plan (DRP)
distance considerations
diversity
dual power supply
environmental disasters
external disasters
full backup
functional recovery plan
generator
geographic dispersal
high availability
hot site
identification of critical systems
image backup
Impossible Travel
incremental backup
internal disasters
job rotation
last known good configuration
least privilege
live boot media
lockout
mandatory vacations
man-made disasters
mean time between failures (MTBF)
mean time to recovery (MTTR)
mission-essential function
multipath
network-attached storage (NAS)
Network Location
NIC teaming
nondisclosure agreement (NDA)
nonpersistent
offboarding
onboarding
organizational policies
password complexity
password history
password reuse
policy
power distribution unit (PDU)
RAID (Redundant Array of Independent Drives or Redundant Array of Inexpensive Disks)
recovery point objective (RPO)
recovery time objective (RTO)
redundancy
replication
restoration order
revert to known state
Risky IP address
scalability
separation of duties
single point of failure
site risk assessment
snapshot
social media analysis
storage area network (SAN)
time of day
time-based login
uninterruptible power supply (UPS)
warm site

Review Questions

1. Mary Alice has been asked to help develop an outline of procedures to be followed in the event of a major IT incident or an incident that directly impacts IT. What type of planning is this?
   - **a.** Business impact analysis planning
   - **b.** IT contingency planning
   - **c.** Disaster recovery planning
   - **d.** Risk IT planning
2. Which of the following is NOT an element that should be part of a BCP?
   - **a.** High availability
   - **b.** Robustness
   - **c.** Diversity
   - **d.** Scalability
3. Which of the following is a federal initiative that is designed to encourage organizations to address how critical operations will continue under a broad range of negative circumstances?
   - **a.** DPPR
   - **b.** BIA
   - **c.** MTBF
   - **d.** COOP
4. A BIA can be a foundation for which of the following?
   - **a.** Functional recovery plan
   - **b.** Site risk assessment
   - **c.** Contingency reaction plan
   - **d.** Resumption assessment plan
5. Which of the following will a BIA NOT help determine?
   - **a.** Mission-essential functions
   - **b.** Identification of critical systems
   - **c.** Single point of failure
   - **d.** Percentage availability of systems
6. Which of these is NOT a factor in determining restoration order?
   - **a.** Dependencies
   - **b.** Speed of implementation
   - **c.** Process of fundamental importance
   - **d.** Alternative business practices
7. What is the average amount of time that it will take a device to recover from a failure that is not a terminal failure?
   - **a.** MTTR
   - **b.** RTO
   - **c.** RPO
   - **d.** MTBF
8. Which of the following is NOT true about RAID?
   - **a.** It can be implemented in hardware or software.
   - **b.** Nested levels can combine other RAID levels.
   - **c.** It is designed primarily to backup data.
   - **d.** The most common levels of RAID are Level 0, 1, 5, 6, and 10.
9. Linnea is researching a type of storage that uses a single storage device to serve files over a network and is relatively inexpensive. What type of storage is Linnea researching?
   - **a.** SAN
   - **b.** NAS
   - **c.** RAID
   - **d.** ARI
10. Which of the following is a document that outlines specific requirements or rules that must be met?
    - **a.** Guideline
    - **b.** Policy
    - **c.** Framework
    - **d.** Specification
11. What device is always running off its battery while the main power runs the battery charger?
    - **a.** Secure UPS
    - **b.** Backup UPS
    - **c.** Offline UPS
    - **d.** Online UPS
12. Which type of site is essentially a duplicate of the production site and has all the equipment needed for an organization to continue running?
    - **a.** Cold site
    - **b.** Warm site
    - **c.** Hot site
    - **d.** Replicated site
13. Which of the following can a UPS NOT perform?
    - **a.** Prevent certain applications from launching that will consume too much power
    - **b.** Disconnect users and shut down the server
    - **c.** Prevent any new users from logging on
    - **d.** Notify all users that they must finish their work immediately and log off
14. What is a definition of RPO?
    - **a.** The maximum length of time that can be tolerated between backups
    - **b.** Length of time it will take to recover data that has been backed up
    - **c.** The frequency that data should be backed up
    - **d.** How a backup utility reads an archive bit

15. What does an incremental backup do?
- **a.** Copies all files changed since the last full or incremental backup
- **b.** Copies only user-selected files
- **c.** Copies all files
- **d.** Copies all files since the last full backup

16. Molly needs to access a setting in Microsoft Windows Group Policy to change the type of a network to which a computer is attached. Which setting must Molly change?
- **a.** Wi-Fi/Wired Network Policy
- **b.** Network Config
- **c.** Network Type
- **d.** Network Location

17. Thea has received a security alert that someone in London attempted to access the email account of Sigrid, who had accessed it in Los Angeles one hour before. What feature determined an issue and send this alert to Thea?
- **a.** Impossible Travel
- **b.** Incompatible Location
- **c.** Remote IP address
- **d.** Risky IP address

18. Which of the following is NOT used to identify or enforce what mobile devices can do based on the location of the device?
- **a.** Geo-spatial
- **b.** Geolocation
- **c.** Geo-tagging
- **d.** Geofencing

19. Margaux is reviewing the corporate policy that stipulates the processes to be followed for implementing system changes. Which policy is she reviewing?
- **a.** Change management policy
- **b.** Change format policy
- **c.** Change modification policy
- **d.** Change control policy

20. Which commercial data classification level would be applied to a data set of the number of current employees at an organization and would only cause a small amount of harm if disclosed?
- **a.** Public
- **b.** Open
- **c.** Private
- **d.** Confidential

Hands-On Projects

CAUTION If you are concerned about installing any of the software in these projects on your regular computer, you can instead use the Windows Sandbox or install the software in the Windows virtual machine created in the Module 1 Hands-On Projects. Software installed within the virtual machine will not impact the host computer.

Project 14-1: Using Windows File History to Perform Data Backups

Time Required: 25 minutes

Objective: 2.5 Given a scenario, implement cybersecurity resilience.
- Backup types

Description: The software backup utility File History is the Microsoft Windows 10 primary tool for backing up user files. Once configured, File History will automatically back up files to a storage device on a schedule. Note that File History is designed to back up user files and does not create a system image of the drive. In this project, you configure and use File History.

1. Connect an external storage device such as a large-capacity USB flash drive or external hard drive to the computer as a repository for the backups. (You cannot back up files to the same drive that contains the user files.)
2. Click **Start** and then click **Settings**.
3. Click **Update & Security**.
4. Click **Backup**.
5. Click **More options**.
6. Click **See advanced settings**.
7. Click **Turn on**.

8. Click **Advanced settings**.
9. Click the down arrow under **Save copies of files**. Note the default setting is **Every hour (default)**. Scroll through the other options. Which would you consider the best option for you? Why?
10. Click the down arrow under **Keep saved versions**. Note the default setting is **Forever (default)**. Scroll through the other options. What is the advantage to having backups kept indefinitely? What is the disadvantage? Which would you consider the best option for you? Why?
11. Click the **Back** arrow and look at the list of items that File History automatically backs up under **Copy files from**. By default, File History is set to back up important folders in the user account's home folder, such as Desktop, Libraries (Documents, Downloads, Music, Pictures, Videos, and so on), and Favorites. Do these folders include all your important data?
12. Click **Exclude folders**.
13. Click **Add** and select a folder that does not contain your important data such as **Downloads**. Click **Select folder**.
14. Click the **Back** arrow to return to the File History window.
15. Click **Advanced settings** again.
16. Under **Event logs,** click **Open File History event logs to view recent events or errors**. This allows you to see the log of any errors that may have occurred during the backup. Why is this important? How often should this log be viewed?
17. How easy is File History to use? Would you recommend it as a basic file backup software utility? Why or why not?
18. Close all windows.

Project 14-2: Viewing and Changing the Backup Archive Bit

Time Required: 20 minutes

Objective: 2.5 Given a scenario, implement cybersecurity resilience.

- Backup types

Description: One of the keys to backing up files is to know which files need to be backed up. Backup software can internally designate which files have already been backed up by setting an archive bit in the properties of the file. A file with the archive bit cleared (set to 0) indicates that the file has been backed up. However, when the contents of that file are changed, the archive bit is set (to 1), meaning that this modified file now needs to be backed up. In this project, you view and change the backup archive bit.

1. Start Microsoft Word and create a document that contains your name and today's date.
2. Save this document as **Bittest.docx**, and then close Microsoft Word.
3. Click **Start**, enter **cmd**, and then press **Enter**. The Command Prompt window opens.
4. Navigate to the folder that contains **Bittest.docx**.
5. Type **attrib/?** and then press **Enter** to display the options for this command.
6. Type **attrib Bittest.docx** and then press **Enter**. The attributes for this file are displayed. The A indicates that the bit is set and the file should be backed up.
7. You can clear the archive bit like the backup software does after it copies the file. Type **attrib –a Bittest.docx** and then press **Enter**.
8. Now look at the setting of the archive bit. Type **attrib Bittest.docx** and then press **Enter**. Has it been cleared?
9. Close the Command Prompt window.

Project 14-3: Creating and Using a Nonpersistent Live Boot Media

Time Required: 25 minutes

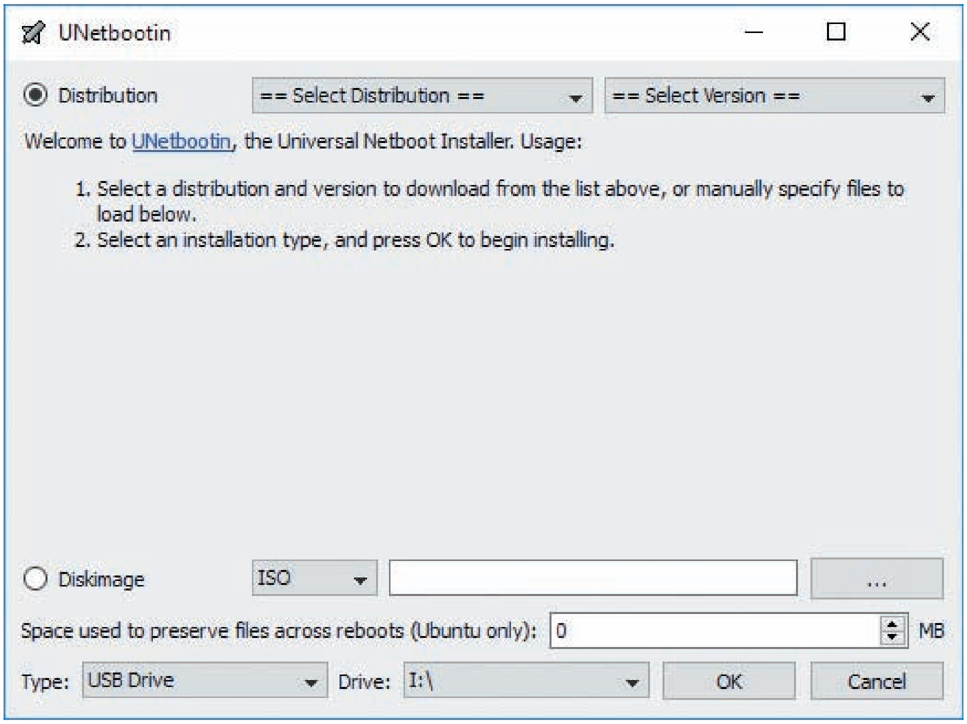
Objective: 2.5 Given a scenario, implement cybersecurity resilience.

- Nonpersistence

Description: Another nonpersistence tool is a live boot media, which is an operating system that boots from a USB flash drive or optical disc but retains no information. In this project, you will create a Linux live boot media USB flash drive using UNetbootin. Note that you will need a flash drive of at least 32 GB formatted as FAT32.

1. Use your web browser to go to **unetbootin.github.io**. (If you are no longer able to access the program through the above URL, use a search engine and search for "unetbootin.")

2. Read through the features of UNetbootin.
3. Under **Supported Distributions**, note that UNetbootin has built-in support for several different Linux distributions.
4. Click **Linux Mint**.
5. On the Linux Mint website, click **About** to see more information on Linux Mint. It is a graphical user interface distribution that has many similarities to Microsoft Windows and Apple macOS.
6. Click your browser's **Back** button to return to UNetbootin.
7. Scroll up to select the operating system of your computer and then click **Download**.
8. When the download is complete, launch UNetbootin. Note that no installation is required. The UNetbootin screen is shown in Figure 14-8.



Source: UNetbootin

Figure 14-8 UNetbootin screen

9. Click the down arrow under **Select Distribution**. Scroll through the list of natively supported distributions from which a live boot media can be created.
10. Click **Linux Mint**.
11. Under **Type**, be sure that **USB Drive** is selected and that is the correct flash drive on which to install it is selected under **Drive**.
12. Click **OK**. UNetbootin will download the Linux Mint files and then create the bootable USB flash drive. Note that this may take several minutes to complete depending upon your network bandwidth.
13. After the installation is complete, reboot the computer to boot from the USB flash drive. (Many systems require pressing the **F12** key when rebooting to choose an alternative booting device.)
14. Boot from the USB flash drive to load the live boot media Linux Mint.
15. Reboot your computer again to access the operating system on the hard drive.

Project 14-4: Using Windows Local Security Policy

Time Required: 25 minutes

Objective: 3.7 Given a scenario, implement identity and account management controls.

- Account policies

Description: The Local Group Policy Editor is a Microsoft Management Console (MMC) snap-in that gives a single user interface through which all the Computer Configuration and User Configuration settings of Local Group Policy objects can be managed. The Local Security Policy settings are among the security settings contained in the Local Group Policy Editor.

An administrator can use these to set policies that are applied to the computer. In this project, you will view and change local security policy settings.

CAUTION You need to be an administrator to open the Local Group Policy Editor.

1. Click **Start**.
2. Type **secpol.msc** in the Search box and then click **secpol**.

NOTE 25

If your computer is already joined to a domain, then searching for secpol.msc might not launch the application. If this is the case, click **Start** and type **mmc.msc**. On the File menu, click **Add/Remove** snap-in and then click **Add**. In **Add Standalone Snap-in**, double-click **Group Policy Object Editor**.

3. First create a policy regarding passwords. Expand **Account Policies** in the left pane and then expand **Password Policy**.
4. Double-click **Enforce password history** in the right pane. This setting defines how many previously used passwords Windows will record. This prevents users from "recycling" old passwords.
5. Change **passwords remembered** to **4**, and then click **OK**.
6. Double-click **Maximum password age** in the right pane. The default value is 42, meaning that a user must change the password after 42 days.
7. Change **days** to **30**, and then click **OK**.
8. Double-click **Minimum password length** in the right pane. The default value is a length of 8 characters.
9. Change **characters** to **10**, and then click **OK**.
10. Double-click **Password must meet complexity requirements** in the right pane. This setting forces a password to include at least two opposite case letters, a number, and a special character (such as a punctuation mark).
11. Click **Enabled**, and then click **OK**.
12. Double-click **Store passwords using reversible encryption** in the right pane. Because passwords should be stored in an encrypted format, this setting should not be enabled.
13. If necessary, click **Disabled**, and then click **OK**.
14. In the left pane, click **Account lockout policy**.
15. Double-click **Account lockout threshold** in the right pane. This is the number of times that a user can enter an incorrect password before Windows will lock the account from being accessed. (This prevents an attacker from attempting to guess the password with unlimited attempts.)
16. Change **invalid login attempts** to **5**, and then click **OK**.
17. Note that the Local Security Policy suggests changes to the **Account lockout duration** and the **Reset account lockout counter after** values to 30 minutes. Click **OK**.
18. Expand **Local Policies** in the left pane and then click **Audit Policy**.
19. Double-click **Audit account logon events**.
20. Check both **Success** and **Failure**, and then click **OK**.
21. Right-click **Security Settings** in the left pane.
22. Click **Reload** to have these policies applied.
23. Close all windows.

Case Projects

Case Project 14-1: Business Impact Analysis

Using your school or organization, develop a brief business impact analysis. What are the impacts? What is the mission-essential function? What are the critical systems? What is the single point of failure? Use the steps outlined earlier in the module. Share your plan with others if possible. What did you learn? Modify your plan accordingly.

Case Project 14-2: Impossible Travel

Impossible Travel detection identifies two user activities originating from geographically distant locations within a time period shorter than the user could travel between locations. Research Impossible Travel. How does it work? How does Impossible Travel learn about a user's normal activities? What are the levels that the sensitivity slider allows administrators to configure to define how strict the detection logic is? What happens if a user regularly uses two more locations on a regular basis? How accurate would you determine Impossible Travel to be? How could the information gleaned by Impossible Travel pose a threat? Write a one-page analysis of your research.

Case Project 14-3: Continuous Data Protection (CDP)

Use the Internet to research continuous data protection (CDP). Identify three different solutions and compare their features. Create a table of the different features to make a side-by-side comparison. Which product would you consider to be the best solution for an enterprise environment? Why?

Case Project 14-4: Personal Disaster Recovery Plan

Create a one-page document of a personal disaster recovery procedure for your home computer. Be sure to include what needs to be protected and why. Does your DRP show that what you are doing to protect your assets is sufficient? Should any changes be made?

Case Project 14-5: RAID Level 6 Costs

Use the Internet to research the costs of adding RAID Level 6 to a computer, which is generally recognized as the best general RAID level. Create a chart that lists the features, costs, and operating systems supported for this level. Would you purchase this for your computer? Why or why not?

Case Project 14-6: Personal Backup Procedures

What are your personal data backup procedures? Write a one-paragraph description of how you back up your data, what data you back up, how often you perform a backup, where your backup is stored, etc. Use the information in this module to compare it with your current backup procedures. Write a second paragraph that identifies the strengths and weaknesses of your current procedures. Finally, write a third paragraph that outlines how you could change your current procedures to make your backups more secure.

Case Project 14-7: Online Backup Services

Several good online backup services can help make data backup easy for the user. Use a search engine to search for *online backup service reviews*, and select three different services. Research these services and note their features. Create a table that lists each service and compare their features. Be sure to also include costs. Which would you recommend? Why?

Case Project 14-8: North Ridge Security

North Ridge Security provides security consulting and assurance services. You have recently been hired as an intern to assist them.

Operation Appreciation is a statewide charity service that assists military veterans who are struggling. Recently, one of its primary servers crashed. When the IT department tried to restore from a recent backup, they found that there was a flaw, and several months' worth of the backups was useless. Fortunately, North Ridge Security was able to restore the server that crashed and obtain a good backup before it was installed on a new system. (North Ridge did this service without charging Operating Appreciation.) Now North Ridge now wants to assist Operating Appreciation with creating a secure backup system. You have been asked to make a presentation to them.

1. Create a PowerPoint presentation for Operation Appreciation about backups, including the types of data backups, where they should be stored, how they should be tested, etc. Your presentation should contain at least 10 slides.
2. After the presentation, Operation Appreciation is most interested in cloud backups and has asked for your opinion. Use the Internet to research cloud backups and then create a memo about your findings and recommendations.

Case Project 14-9: Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. Go to **community.cengage.com/infosec2** and click the *Join or Sign in* icon to log in, using your login name and password that you created in Module 1. Click **Forums (Discussion)** and click on **Security+ Case Projects (7th edition)**. Read the following case study.

Serious issues surround social media analysis of posts made by applicants and employees. For example, while looking at social media posts, employers could easily learn details such as religion, disability, or pregnancy of an applicant. By law, employers cannot take these into account, but just knowing them could introduce bias in hiring decisions. Yet if an employer ignores a history of inflammatory social media posts, it could expose that employer to liability. So should a prospective or current employer read your social media posts? Does that fall outside the boundaries of when you are at work? Or do you represent your employer even when you are away from work? Take your side of this argument, and post your opinions to on the Community Site discussion board.

References

1. Wang, T, "Global economic losses from natural disasters 2000-2019," *Statista*, Jan. 24, 2020, accessed Jul. 30, 2020, www.statista.com/statistics/510894/natural-disasters-globally-and-economic-losses/.
2. "Study: 40% of businesses fail to reopen after a disaster," *Access*, Apr. 14, 2020, accessed Jul. 30, 2020, www.accesscorp.com/access-in-the-news/study-40-percent-businesses-fail-reopen-disaster/.

MODULE 15

RISK MANAGEMENT AND DATA PRIVACY

After completing this module, you should be able to do the following:

1. Define risk
2. Describe strategies for reducing risk
3. Explain concerns surrounding data privacy
4. List methods for protecting data

Front-Page Cybersecurity

The COVID-19 pandemic, which is believed to have started in late 2019, caused unprecedented upheaval around the world. Virtually every part of everyone's life was impacted in ways too numerous to mention. One particular area that the virus dramatically changed is personal data privacy. There is concern that these changes will continue well into the future.

One of the three major defenses against COVID-19, along with social distancing and wearing protective masks, is "contact tracing." As the name implies, contact tracing is walking back in time to identify the people a patient infected with COVID-19 may have been in contact with recently. Because infected people may not show any symptoms (they are "asymptomatic") for several days, they could be infecting others without knowing it just by being around them. Those who begin to show symptoms and are then tested as positive would likely have difficulty remembering everyone they came in contact with over several days—especially if they are now sick—in order to warn others.

To stem the tide of the outbreak, governments around the world first turned to smartphones used by the general public to conduct contact tracing. Because COVID-19 was the first global pandemic in the age of the ubiquitous smartphone, these devices gave governments immediate surveillance capabilities. The most aggressive pandemic surveillance using smartphones started in China. Authorities there used cellular phone numbers and location data to trace the identities of thousands of residents who had left Wuhan, the earliest center of the outbreak, over the Chinese Lunar New Year holiday to return home. This information was then passed to local officials and "neighborhood minders," who contacted the targeted individuals and asked them to voluntarily self-quarantine for two weeks, even though many showed no symptoms.

However, the Chinese government soon decided that more drastic measures needed to be taken—and that more data was needed. China turned to travel records and security cameras to identify people who had been in contact with any coronavirus patients on trains, airplanes, and even in passing on street corners. Those individuals were also put in forced isolation.

Other governments soon followed, using both smartphone location data and other means of technology surveillance. In Western Australia, lawmakers approved a bill to install surveillance devices inside the homes of those placed under quarantine to ensure that they did not leave. Authorities in Hong Kong and India used geofencing from smartphones and wearables to create virtual fences around quarantine zones: infected offenders who ventured outside these zones could be sent to jail. The most popular Japanese messaging app regularly sent health-status questions to its users on behalf of the government.

Authorities in Moscow used facial-recognition technology to catch a Chinese woman who broke quarantine and was walking down the street. The police in England used drones to spot residents venturing out to a scenic overlook.

South Korea, after reporting 900 COVID-19 cases per day in early 2020, by mid-April only averaged 30 cases per day, without using lockdowns. Instead, the government heavily relied on technology. After the nation suffered a botched attempt to contain a different coronavirus in 2015, a law was passed that authorized officials to produce dossiers of confirmed patients using smartphone data, credit card transactions, and security video footage. Authorities started using such information to identify people who had come into contact with coronavirus patients to encourage them to get tested or stay home. South Korean government websites also published detailed reports about confirmed coronavirus cases. These online reports include patients' ages, work and home addresses, and personal details such as the restaurants they frequented, trips taken to family get-togethers, and even where they went to get massages. This was done to warn others not to visit these establishments. The South Korean law was expanded during the spring of 2020 to grant both health officials and local governments the power to request more information. The government said it could identify and locate at-risk patients in 10 minutes or less by automating access to personal information.

The United States likewise has used data to monitor the movement of its citizens. For example, the state of Kansas announced it used third-party GPS tracking data to monitor whether suspected infected people were following the advice of phone calls instructing them to stay at home.

In the wake of COVID-19, polls have indicated a dramatic shift in thinking among the general public about the usage of this type of privacy data. In a survey conducted in 2019 prior to the pandemic, Americans indicated data privacy was the biggest issue facing companies. But in a poll taken just weeks after the COVID-19 infections began in the United States, more than half of Americans said they backed anonymized and involuntary use of smartphone and other digital data to conduct contact tracing.

Privacy advocates have expressed concern not only for how this data is used today but also into the future. Will governments continue to collect and use this data after the pandemic? Some advocates have said that COVID-19 may become a watershed moment similar to the September 11, 2001, terrorist attacks, which ushered in new government surveillance powers around the world in the name of protecting public safety. Historically, once such surveillance powers are in place, they rarely are rescinded. Instead, the data continues to be collected and is quietly used for other purposes.

Two elements of cybersecurity are of high importance to both enterprises and users. The first involves risk. Although all organizations as well as users face innumerable risks, many choose to focus only on "putting out the fire" of the most recent incident and do not consider overall risk at a higher level. They often fail to understand their own philosophy toward risk and do not see how this drives their approach to cybersecurity as a whole. Ignoring an understanding of risk can have a significant impact on the overall security posture of an enterprise and user.

A second element of high importance is data privacy. As technology devices gather data on user behavior at an unprecedented rate, users are becoming increasingly concerned about how their private data is being used. Only recently have governments started enacting regulations about what user data can be collected, how it can be used, how the user is informed, and what options are given to consumers about the collection and protection of their data. Enterprises faced with growing government and user concerns over data privacy must wrestle with how they can use private data while responsibly protecting it from falling into the wrong hands.

This module examines these twin elements of high importance to cybersecurity. First, you learn about risk and study strategies for mitigating risks. Next, you explore data privacy and the issues that surround it.

MANAGING RISK

CERTIFICATION

5.1 Compare and contrast various types of controls.

5.3 Explain the importance of policies to organizational security.

5.4 Summarize risk management processes and concepts.

Managing risk is an important task for enterprises and users. Managing risk involves defining what it is, understanding risk types, knowing different methods of risk analysis, and realizing how to manage risk.

Defining Risk

An *asset* is any item that has a positive economic value. In an enterprise, assets have the following qualities: they provide value to the enterprise; they cannot easily be replaced without a significant investment in expense, time, worker skill, and/or resources; and they can form part of the enterprise's corporate identity. Examples of enterprise assets range from people (employees, customers, business partners, contractors, and vendors) to physical assets (buildings, automobiles, and plant equipment).

Obviously, not all assets have the same value or worth. The **asset value** is the relative worth of an asset. Consider the assets in an enterprise's information technology (IT) infrastructure. Some assets have a very high value while others do not. For example, a faulty desktop computer that can easily be replaced is not be considered an asset with a high value, yet the information contained on that computer can be an asset. Table 15-1 describes the elements of an enterprise's IT infrastructure and whether these assets would normally be considered as having a high value.

Table 15-1 Typical IT assets

Asset	Description	Example	High value?
Information	Data that has been collected, classified, organized, and stored in various forms	Customer, personnel, production, sales, marketing, and finance databases	Yes: Extremely difficult to replace
Customized business software	Software that supports the business processes of the enterprise	Customized order transaction application	Yes: Unique and customized for the enterprise
System software	Software that provides the foundation for application software	Operating system	No: Can be easily replaced
Physical items	Computer equipment, communications equipment, storage media, furniture, and fixtures	Servers, routers, and power supplies	No: Can be easily replaced
Services	Outsourced computing services	Voice and data communications	No: Can be easily replaced

Assets are continually under threat, which is a type of action that has the potential to cause harm. Several threat classifications are listed in Table 15-2.

Table 15-2 Threat classifications

Threat category	Description	Example
Strategic	Action that affects the long-term goals of the organization	Theft of intellectual property, not pursuing a new opportunity, loss of a major account, competitor entering the market
Compliance	Following (or not following) a regulation or standard	Breach of contract, not responding to the introduction of new laws
Financial	Impact of financial decisions or market factors	Increase in interest rates, global financial crisis
Operational	Events that impact the daily business of the organization	Fire, hazardous chemical spill, power blackout
Technical	Events that affect information technology systems	Denial of service attack, SQL injection attack, virus
Managerial	Actions related to the management of the organization	Long-term illness of company president, key employee resigning

Organizations must determine how realistic the chance is that a given threat will compromise an asset, called the **likelihood of occurrence**. This is stated in terms of risk. At a basic level, **risk** may be defined as a situation that involves exposure to some type of danger. At a more advanced level, risk can be described as a function of threats, consequences of those threats, and the resulting vulnerabilities.

Risk Types

There are many types of risk. Risk types can be grouped into these broad categories:

- *Internal and external*. An **internal risk** comes from within an organization (such as employee theft), while an **external risk** is from the outside (like the actions of a hactivist).
- *Legacy systems*. One type of platform that is well known for its risks is a legacy system. A legacy system is no longer in widespread use, often because it has been replaced by an updated version of the earlier technology. Although legacy hardware introduces some risks, more often risks result from legacy software, such as an OS or program.
- *Multiparty*. Often overlooked in identifying risk types is the impact that vulnerabilities of one organization can have on other organizations that are connected to it. These are called **multiparty** risks that impact multiple "downstream" organizations.

NOTE 1

The results from the vulnerability of one organization rippling downstream are staggering. One study that examined more than 90,000 cyber events found that multiparty risks that were exploited resulted in financial losses 13 times larger than single-party incidents. The number of organizations impacted by multiparty incidents outnumber primary victims by 850 percent, and these multiparty incidents will continue to increase at an average rate of 20 percent annually.

- *Intellectual property (IP) theft*. Intellectual property (IP) is an invention or a work that is the result of creativity. The owner of IP can apply for protection from others who attempt to duplicate it; these protections over IP or its expression are patent, trademark, copyright, and trade secret. Threat actors attempt to steal IP (**IP theft**) that may include research on a new product from an enterprise so that they can sell it to an unscrupulous foreign supplier who will then build an imitation model of the product to sell worldwide. This deprives the legitimate business of profits after investing hundreds of millions of dollars in product development, and because these foreign suppliers may be in a different country, they are beyond the reach of domestic enforcement agencies and courts.
- *Software compliance and licensing*. Specialized software used by an enterprise is subject to licensing restrictions that protect the rights of the developer. An obvious violation would be for an organization to license software for a single manufacturing plant but then distribute that software to five other plants without paying for its usage. **Software compliance and licensing** risks are today considered a serious problem for organizations. Most organizations unknowingly violate one or more licensing agreements. Several of the reasons for this are listed in Table 15-3.

Table 15-3 Reasons for software noncompliance

Reason	Example	Explanation
Software licensed for one reason but now used for a different reason	Limited-use license purchased only to be used in nonproduction development environment used in a production environment.	Organizations may purchase limited-use licenses rather than full-use licenses to obtain a pricing discount; a newly hired technician is not aware of the restriction and copies software into the production facility.
Product use rights changed	A third party accesses software purchased by the organization that is used in violation of new product use rights.	Although developers initially allowed third parties approved by the organization to use their software, now this "indirect access" is changed so a new license requires all users to have a purchased license.
Software installed on a virtual machine	Software migrated to a virtual machine and moved to multiple other machines in violation of license.	Some developers restrict software from being installed and then moved among multiple virtual machines without purchasing a new license.

Risk Analysis

It is important for an organization to regularly perform a *risk analysis*, or a process to identify and assess the factors that may jeopardize the success of a project or reaching a stated goal. Following a methodology or process for performing a risk analysis is crucial. Risk assessments and tools for representing risk can be used to assist an organization in a risk analysis.

Methodology

Which is more difficult: identifying a risk or mitigating it? At first glance, it may seem that identifying risks through a risk analysis should be a straightforward process, and the more difficult work would involve addressing that risk. However, that is not always the case. Often simply seeing the risk can be difficult.

This difficulty is due to two factors. First, risks can be elusive and often hard to identify. While obvious risks seem readily apparent (such as a firewall that unplugged), not all risks are so clear (such as the danger of opening an email attachment that appears to come from a friend). Risks, by their very nature, are often hidden below the surface and are not apparent.

A second reason for the difficulty of identifying risks is due to human nature. One recognized reason for this difficulty is *unconscious human biases*.[1] All individuals have their own set of biases developed through preferences, intuition, or past experiences. These biases influence decision making and "vision." They may have a bias toward which foods to eat, what clothes to wear, or even the order of tasks to be tackled each day. Table 15-4 lists commonly recognized biases and effects.

Table 15-4 Decision-making biases and effects

Bias	Explanation
Aggregate bias	Inferring something about an individual by using data that actually describes trends for the broader population
Anchoring bias	Holding onto a specific feature or set of features of information early in the decision-making process
Availability bias	Perceiving how likely an event is to occur given how frequently the event is heard of
Confirmation bias	Making a decision before investigating and then only looking for data that supports the theory
Present bias	Tending to discount future risks and gains in favor of immediate gratification
Framing effect	Deciding on an option based on how the choices are worded
Fundamental attribution error	Viewing the failures or mistakes of others as part of their identity rather than attributing them to contextual or environmental influences

These unconscious biases and effects can influence risk identification. For example, an anchoring bias may cause someone to focus on one of the first risks exposed and then marginalize other risks. People with a confirmation bias could quickly decide that a risk is relatively unimportant—particularly on a system for which they are responsible—and then look for data to support their position. These biases could easily lead to identifying the wrong individual as the source of a risk, making incorrect estimates about the potential impact of a risk, focusing on an unlikely risk, or even spending too much time on incorrect theories.[2]

Research into human behavior has also revealed that most people have difficulty seeing risks and are prejudiced toward particular risks while minimizing others. Generally, when dealing with risks, people tend to

- Overreact to risks caused by intentional actions
- Underreact to risks associated with accidents, abstract events, and natural phenomena
- Overreact to risks that are considered insulting, disgusting, or offensive to our moral standards
- Overreact to immediate risks
- Underreact to long-term risks
- Underreact to risks and changes that occur slowly and over time

Due to the difficulty in identifying risks, a methodology has been developed that can be helpful in identifying risks. This methodology helps to minimize human factors in identifying risk by not relying on a few employees in an organization but instead involving many individuals in the process. As more employees are involved, biases and prejudices are minimized. An analysis of risk that involves a wide array of users is considered the most effective approach. **Risk Control Self-Assessment (RCSA)** is an "empowering" methodology by which management and staff at all levels collectively work to identify and evaluate risks. The goal of RCSA is to not only minimize biases and prejudices but also to integrate risk management practices into the culture of the organization. As staff perform their normal activities and as business units work toward their objectives, the topic of risk permeates all of these activities.

Risk Assessment

An organization that can accurately calculate risk is better prepared to address the risk. For example, if a customer database is determined to be of high value and to have a high risk, the necessary resources should be used to strengthen the defenses surrounding that database.

There are two risk assessment approaches. One is **qualitative risk assessment**. This approach uses an "educated guess" based on observation. For example, if it is observed that the customer database contains important information, it would be assigned a high asset value. Also, if it is observed that this database has been frequently the target of attacks, it would be assigned a high-risk value as well. Qualitative risk typically assigns a numeric value (*1–10*) or label (*High, Medium,* or *Low*) that represents the risk.

The second approach, **quantitative risk assessment**, is considered more formal and systematic. Instead of arbitrarily assigning a number or label based on observation, the quantitative risk calculation attempts to create "hard" numbers associated with the risk of a system element by using historical data. For example, if the customer database has a higher risk calculation than a product database, more resources would be allocated to protecting it.

Quantitative risk calculations can be divided into the likelihood of a risk and the impact of a risk being successful.

Risk Likelihood Historical data is valuable in providing information on how likely it is that a risk will become a reality within a specific period of time. For example, when considering the risk of equipment failure, several quantitative tools can be used to predict the likelihood of the risk, including the following:

- *Mean Time Between Failure (MTBF)*. MTBF calculates the average (*mean*) amount of time until a component fails, cannot be repaired, and must be replaced. It is a reliability term used to provide the amount of failures. Calculating the MTBF involves dividing the total time measured by the total number of failures observed.

CAUTION Although MTBF is sometimes used to advertise the reliability of consumer hardware products such as hard disk drives, this value is seldom considered by the purchaser. This is because most consumer purchases are simply price driven. MTBF is considered more important for industries than for consumers.

NOTE 2

MTBF and MTTR are covered in Module 14.

- *Mean Time To Recovery (MTTR)*. MTTR is the average amount of time that it will take a device to recover from a nonterminal failure. Although MTTR is sometimes called *Mean Time To Repair* because in most systems this means replacing a failed hardware instead of repairing it, the Mean Time To Recovery is considered a more accurate term.
- *Mean Time To Failure (MTTF)*. MTTF is a basic measure of reliability for systems that cannot be repaired. It is the average amount of time expected until the first failure of a piece of equipment.
- *Failure In Time (FIT)*. The FIT calculation is another way of reporting MTBF. FIT can report the number of expected failures per one billion hours of operation for a device. This term is used particularly by the semiconductor industry. FIT can be stated as *devices for one billion hours*, *one billion devices for 1,000 hours each*, or in other combinations.

Other historical data for calculating the likelihood of risk can be acquired through a variety of sources. These are summarized in Table 15-5.

Table 15-5 Historical data sources

Source	Explanation
Law enforcement agencies	Crime statistics on the area of facilities to determine the probability of vandalism, break-ins, or dangers potentially encountered by personnel
Insurance companies	Risks faced by other companies and the amounts paid out when these risks became reality
Computer incident monitoring organizations	Data regarding a variety of technology-related risks, failures, and attacks

Once historical data is compiled, it can be used to determine the likelihood of a risk occurring within a year. This is known as the **Annualized Rate of Occurrence (ARO)**.

Risk Impact Once historical data is gathered so that the ARO can be calculated, the next step is to determine the impact of that risk. This can be done by comparing it to the monetary loss associated with an asset to determine how much money would be lost if the risk occurred.

CAUTION When calculating the loss, all costs must be considered. For example, if a network firewall failed, the costs would include the amount needed to purchase a replacement, the hourly wage of the person replacing the equipment, and the pay for employees who could not perform their job functions because they could not use the network while the firewall was not functioning.

Two risk calculation formulas are commonly used to calculate expected losses. The **Single Loss Expectancy (SLE)** is the expected monetary loss every time a risk occurs. The SLE is computed by multiplying the Asset Value (AV) by the Exposure Factor (EF), which is the proportion of an asset's value that is likely to be destroyed by a particular risk (expressed as a percentage). The SLE formula is as follows:

$$SLE = AV \times EF$$

For example, consider a building with a value of \$10,000,000 (AV) of which 75 percent of it is likely to be destroyed by a tornado (EF). The SLE would be calculated as follows:

$$7{,}500{,}000 = \$10{,}000{,}000 \times 0.75$$

The **Annualized Loss Expectancy (ALE)** is the expected monetary loss that can be expected for an asset due to a risk over a one-year period. It is calculated by multiplying the SLE by the ARO, which is the probability that a risk will occur in a particular year. The ALE formula is as follows:

$$ALE = SLE \times ARO$$

In this example, if flood insurance data suggests that a serious flood is likely to occur once in 100 years, then the ARO is 1/100 or 0.01. The ALE would be calculated as follows:

$$75{,}000 = 0.01 \times \$7{,}500{,}000$$

Representing Risks

Different tools can be used to represent risks identified through a risk assessment. A **risk register** is a list of potential threats and associated risks. Often shown as a table, a risk register can help provide a clear snapshot of vulnerabilities and risks. A sample risk register is shown in Figure 15-1.

Another tool is called a **risk matrix/heatmap**. This is a visual color-coded tool that lists the impact and likelihood of risks. Figure 15-2 illustrates a risk matrix/heatmap.

Risk Register												
Risk Id	Risks	Current risk			Status	Owner	Raised	Mitigation Strategies	Residual risk		
		Likelihood	Impact	Severity					Likelihood	Impact	Severity
Category 1: Projecty selection and project finance											
RP-01	Financial attraction of project to investors	4	4	15	Open		01-march	• Data collection • Information of financial capability of investor • Giving them assurance of tremendous future return.	4	3	12
RP-02	Availability of finance	3	4	12	Open		03-march	• Own resources • Commitment with financial institution • Exclusive management of investor.	3	3	9
RP-03	Level of demand for project	3	3	9	Open		08-march	• Making possibility and identification of low cost and best quality material • Eradication of extra expenses from petty balance.	2	3	6
RP-04	Land acquisition (site availability)	3	3	9	Open		13-march	• Making feasibilites • Analysis and interpretation of feasibilities • Possession and legal obligation of land.	2	2	4
RP-05	_High finance costs	2	2	4	Open		15-march	• Lowering operational expenses and transportation expenses • Proper management of current expenses.	1	2	2

Figure 15-1 Risk register

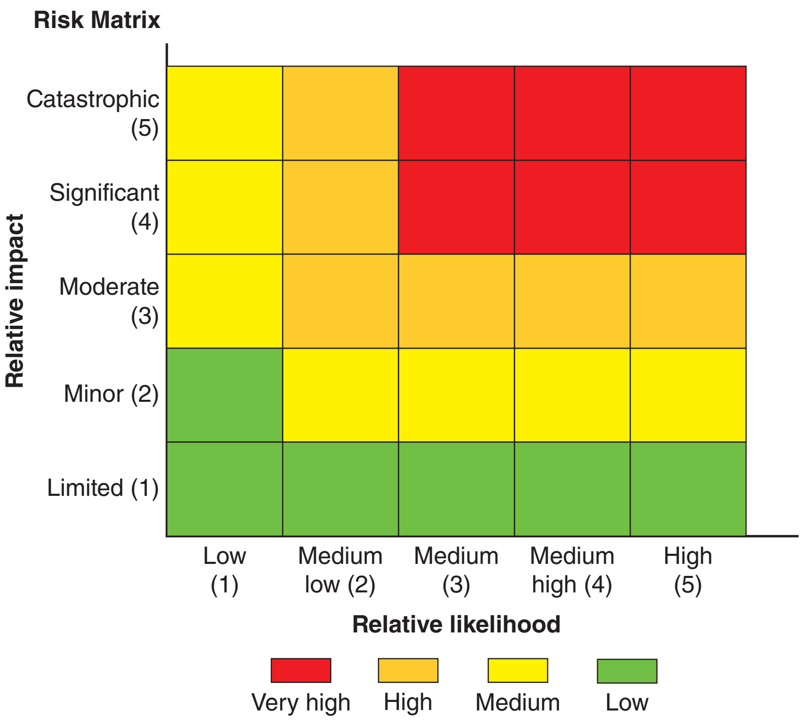


Figure 15-2 Risk matrix/heatmap

Risk Management

The objective of managing risk is to create a level of protection that mitigates the vulnerabilities to the threats and reduces the potential consequences—that is, to reduce risk to a level that is considered acceptable for the organization (called a **risk appetite**). Managing risk involves using specific strategies and control types, addressing third-party risk, and incorporating user training.

Determining a Strategy

There are four strategies for dealing with risks. These can be illustrated through the following scenario. Suppose that Ellie wants to purchase a new motorized Italian scooter to ride from her apartment to school and work. However, because several scooters have been stolen near her apartment, she is concerned about its protection. Although she parks the scooter in the gated parking lot in front of her apartment, a hole in the fence surrounding the apartment complex makes it possible for someone to access the parking lot without restriction.

Ellie has different options when dealing with the risk of her scooter being stolen, and these are the same that can be used by an organization:

- *Acceptance.* Risk **acceptance** simply means that the risk is acknowledged but no steps are taken to address it. In Ellie's case, she could accept the risk and buy the new scooter, knowing there is the chance a thief could steal it by entering the parking lot through the hole in the fence. In a similar fashion, an organization may decide to accept the risk that a flood will engulf its manufacturing plant if that flood is estimated to occur only once every 50 years.
- *Transference.* Ellie could transfer the risk to a third party. She can do this by purchasing insurance so that the insurance company absorbs the loss and pays if the scooter is stolen. This is known as risk **transference**. An organization may elect to purchase **cybersecurity insurance** as an example of transference so that in exchange for paying premiums to the insurance company, the organization is compensated in the event of a successful attack.
- *Avoidance*. Risk **avoidance** involves identifying the risk but making the decision to not engage in the activity. Ellie could decide based on the risk of the scooter being stolen that she will not purchase the new scooter. Likewise, an organization may decide that after an analysis, building a new plant in another location is not feasible.
- *Mitigation.* Risk **mitigation** is the attempt to address risk by making it less serious. Ellie could complain to the apartment manager about the hole in the fence to have it repaired, and an organization could erect a fence around a plant to deter thieves.

Using Controls

A security control is a safeguard or countermeasure employed within an organizational information system to protect the confidentiality, integrity, and availability of the technology system and its data. A security control attempts to limit exposure to a danger. There are three broad categories of controls. These are listed in Table 15-6, using phishing as an example.

Table 15-6 Categories of controls

Control category	Description	Phishing example
Managerial	Controls that use administrative methods	Acceptable use policy that specifies users should not visit malicious websites.
Operational	Controls implemented and executed by people	Conducting workshops to help train users to identify and delete phishing messages.
Technical	Controls incorporated as part of hardware, software, or firmware	Unified threat management (UTM) device that performs packet filtering, antiphishing, and web filtering.

Specific types of controls are found within the three broad categories of controls. These include the following:

- *Deterrent controls*. A **deterrent control** attempts to discourage security violations before they occur.
- *Preventative controls*. A **preventative control** works to prevent the threat from coming in contact with the vulnerability.
- *Physical controls*. A **physical control** implements security in a defined structure and location.
- *Detective controls*. A **detective control** is designed to identify any threat that has reached the system.
- *Compensating controls*. A **compensating control** is a control that provides an alternative to normal controls that for some reason cannot be used.
- *Corrective controls*. A control that is intended to mitigate or lessen the damage caused by the incident is called a **corrective control**.

These control types are summarized along with examples in Table 15-7.

Table 15-7 Control types

Control type	Description	When it occurs	Example
Deterrent control	Discourage attack	Before attack	Posting signs indicating that the area is under video surveillance
Preventive control	Prevent attack	Before attack	Providing security awareness training for all users
Physical control	Prevent attack	Before attack	Building fences that surround the perimeter
Detective control	Identify attack	During attack	Installing motion detection sensors
Compensating control	Alternative to normal control	During attack	Isolating an infected computer on a different network
Corrective control	Lessen damage from attack	After attack	Cleaning a virus cleaned from an infected server

CAUTION Security professionals do not universally agree on the nomenclature and classification of control types. Some researchers divide control types into administrative, logical, and physical. Other security researchers specify up to 18 control types.

NOTE 3

Inherent risk is sometimes viewed as a negative. That is, it represents the amount of risk that exists in the absence of controls.

Controls change over time as new hardware and software are added and new procedures are implemented. **Inherent risk** is defined as the current risk level given the existing set of controls. **Residual risk** is the risk level that remains after additional controls are applied. A specific type of risk is a **control risk** or the probability that financial statements are materially misstated because of failures in the organization's system of controls. When there are significant control failures, a business's financial statements may reveal a profit when there is actually a loss.

Remember that the goal of security is not to eliminate all risk; that simply is not possible. Instead, the goal in designing and implementing controls is to reach a balance between achieving an acceptable level of risk and expense while minimizing losses. Some assets, however, must be protected irrespective of the perceived risk. For example, controls based upon regulatory requirements may be required regardless of risk (**regulations that affect risk posture**).

Implement Third-Party Risk Management

NOTE 4

Third parties and supply chains are covered in Module 1.

Almost all businesses use external entities known as third parties. These include **vendors** (those from whom an organization purchases goods and services), **business partners** (a commercial entity with whom an organization has an alliance), and those as part of a *supply chain* (a network that moves a product from the supplier to the customer).

There are several risks associated with using third parties. First, with the sheer number of third parties used, it can be difficult to coordinate their diverse activities with the organization. Second, almost all third parties today require access to the organization's computer network to provide these external entities the ability to perform their IT-related functions (such as outsourced code development) and even do basic tasks such as submitting online invoices. Yet one of the major risks of this third-party system integration involves the principle of the weakest link: if the security of the third party has a vulnerability, it can provide an opening for attackers to infiltrate the organization's computer network. Third, the difficulties associated with third-party integration, or combining systems and data with outside entities, is significant. The risks associated with this integration include the following:

- *On-boarding and off-boarding*. *Partner on-boarding* refers to the startup relationship between partners, while *partner off-boarding* is the termination of such an agreement. Significant consideration must be given to how the entities will combine their services without compromising their existing security defenses. Also, when the relationship ends, particularly if it has been in effect for a significant length of time, work must be done to ensure that as the parties and their IT systems separate, no gaping holes are left open for attackers to exploit.
- *Application and social media network sharing*. How will applications be shared between the partners? Who will be responsible for support and vulnerability assessments? As social media becomes more critical for organizations in their interactions with customers, which partner will be responsible for sharing social media information?
- *Privacy and risk awareness*. What happens if the privacy policy of one partner is less restrictive than that of the other partner? How will risk assessment be performed on the combined systems?
- *Data considerations*. All parties must have a clear understanding of who owns data generated through the partnership and how that data will be backed up. Restrictions on unauthorized data sharing also must be reached.

One of the means by which the parties can reduce risk is to reach an understanding of their relationships and responsibilities is through interoperability agreements, or formal contractual relationships, particularly as they relate to security policy and procedures. These agreements, which should be regularly reviewed to verify compliance and performance standards, include the following:

- A **service-level agreement (SLA)** is a service contract between a vendor and a client that specifies what services will be provided, the responsibilities of each party, and any guarantees of service.
- A **business partnership agreement (BPA)** is a contract between two or more business partners that is used to establish the rules and responsibilities of each partner, including withdrawals, capital contributions to the partnership, and financial reporting.
- A **memorandum of understanding (MOU)** describes an agreement between two or more parties. It demonstrates a "convergence of will" between the parties so that they can work together. An MOU generally is not a legally enforceable agreement but is more formal than an unwritten agreement.
- A **nondisclosure agreement (NDA)** is a legal contract between parties that specifies how confidential material will be shared between the parties but restricted to others. An NDA creates a confidential relationship between the parties to protect any type of confidential and proprietary information.
- A **measurement system analysis (MSA)** uses scientific tools to determine the amount of variation that is added to a process by a measurement system. For example, a third party who manufactures a product for an organization would need to demonstrate that how it measures the size, weight, dimensions, and other properties of the product is both valid and does not contribute to any variation of the product.
- **End of life (EOL)** is a term used by a manufacturer to indicate that a product has reached the end of its "useful life" and the manufacturer will no longer market, sell, or update it after a specified date, although the manufacturer may still offer maintenance options but at a premium price. **End of service (EOS)** indicates the end of support, which is when the manufacturer quits selling a piece of equipment and no longer provides maintenance services or updates after a certain date; EOS is the final phase of a piece of an equipment's life cycle. Organizations should clearly communicate EOL and EOS between themselves and third parties so that there are no sudden surprises that a product or equipment is no longer available.

Provide User Training

An often-overlooked consideration in risk management is the importance of providing training to users. Training results in **risk awareness**, which is the raising of understanding of what risks exist, their potential impacts, and how they are managed. Training can make users aware of common risks and how they can become a "human firewall" to help mitigate these risks.

All computer users in an organization have a shared responsibility to protect the assets of the organization. However, it cannot be assumed that all users have the knowledge and skill to protect these assets. Instead, users need training in the importance of securing information, the roles that they play in security, and the steps they need to take to prevent attacks. Because new attacks appear regularly, and new security vulnerabilities are continuously being exposed, user awareness and training must be ongoing. User training is an essential element of security.

NOTE 5

Education in an enterprise is not limited to the average employee. Human resource personnel also need to keep abreast of security issues because in many organizations, it is their role to train new employees on all aspects of the organization, including security. Even upper management needs to be aware of the security threats and attacks that the organization faces, if only to acknowledge the necessity of security in planning, staffing, and budgeting.

One of the challenges of organizational education and training is to understand the traits of learners. Table 15-8 lists general traits of individuals born in the United States since 1946.

Table 15-8 Traits of learners

Year born	Traits	Number in U.S. population
Prior to 1946	Patriotic, loyal, have faith in institutions	75 million
1946–1964	Idealistic, competitive, question authority	80 million
1965–1981	Self-reliant, distrustful of institutions, adaptive to technology	46 million
1982–2000	Pragmatic, globally concerned, computer literate, media savvy	76 million

In addition to traits of learners, training style also impacts how people learn. The way that one person is taught may not be the best way to teach all others. Most people are taught using a *pedagogical* approach (from a Greek word meaning *to lead a child*). Adult learners, however, often prefer an *andragogical* approach (the art of helping an adult learn). Some of the differences between pedagogical and andragogical approaches are summarized in Table 15-9.

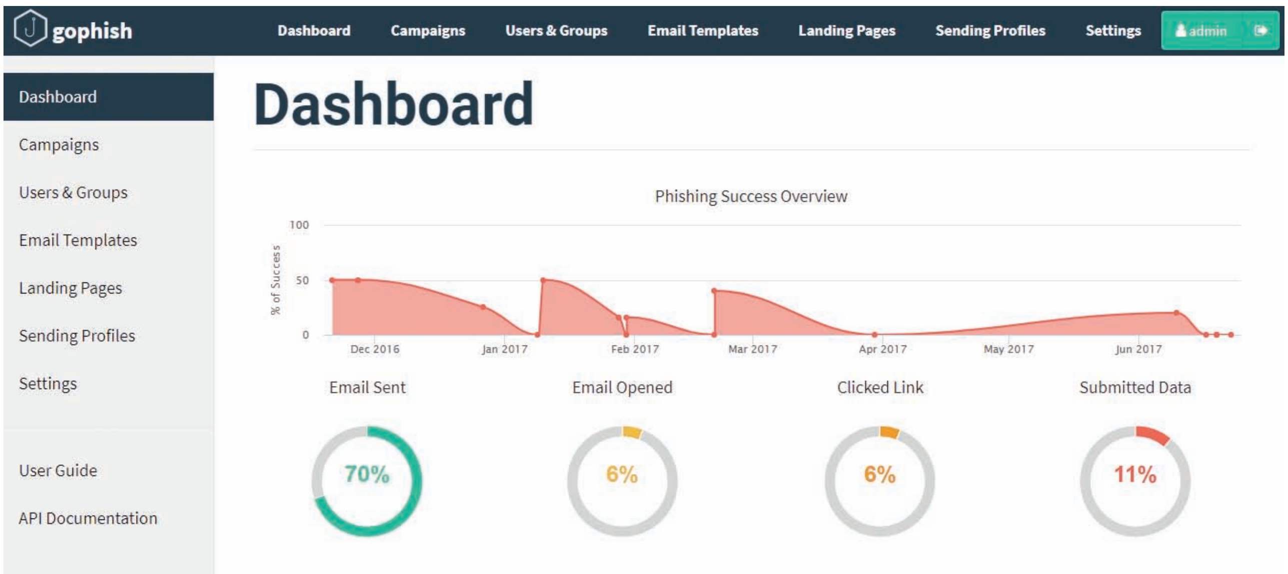
Table 15-9 Approaches to training

Subject	Pedagogical approach	Andragogical approach
Desire	Motivated by external pressures to get good grades or pass on to next grade	Motivated by higher self-esteem, more recognition, desire for better quality of life
Student	Dependent on teacher for all learning	Self-directed and responsible for own learning
Subject matter	Defined by what the teacher wants to give	Learning is organized around situations in life or at work
Willingness to learn	Students are informed about what they must learn	A change triggers a readiness to learn or students perceive a gap between where they are and where they want to be

In addition to training styles, people have different learning styles. Visual learners learn through taking notes, being at the front of the class, and watching presentations. Auditory learners tend to sit in the middle of the class and learn best through lectures and discussions. The third style is kinesthetic, which many information technology professionals tend to have. These students learn through a lab environment or other hands-on approaches. Most people use a combination of learning styles, with one style being dominant. To aid in knowledge retention, trainers should incorporate all three learning styles and present the same information using different techniques. For example, a course could include a lecture, PowerPoint slides, and an opportunity to work directly with software and replicate what is being taught.

Different techniques are employed for user training:

- *Computer-based training (CBT)*. **Computer-based training (CBT)** uses a computer to deliver the instruction. CBT is popular for user training due its flexibility (training can be done from any location and at any time) and ability to provide feedback about the progress of the learner. However, CBT is not always considered the best means for training. Instead, a variety of other modalities, such as specialized face-to-face instruction or informal "lunch-and-learn" sessions, may provide better overall learning results.
- *Role-based awareness training*. Many organizations use **role-based awareness training**. Role-based training involves specialized training that is customized to the specific role that an employee holds in the organization. An office associate, for example, should be provided security training different from training provided to an upper-level manager, because the duties and tasks of these two employees are significantly different.
- *Gamification*. The fast-growing field of digital gaming is generally divided into two distinct markets: recreational gaming for entertainment and instructional gaming for training and education. **Gamification** is using game-based scenarios for instruction. User training can often include gamification in an attempt to heighten the interest and retention of the learner.
- *Capture the flag*. When training security professionals, organizations sometimes add an incentive called a **capture the flag (CTF)** exercise. A series of challenges with varying degrees of difficulty is outlined in advance. When one challenge is solved, a "flag" is awarded, and the points are totaled once time has expired. The winning player or team is the one that earns the highest score.
- *Phishing simulations*. Because phishing is the primary means by which threat actors initially launch an attack, many organizations use **phishing simulations** to help employees recognize phishing emails. These tools can be highly customized and provide detailed feedback on a dashboard, as seen in Figure 15-3, which shows a phishing simulation dashboard from gophish. Phishing simulators can be one part of an entire **phishing campaign** that uses a variety of other tools (such as email reminders, printed posters, and points earned to be redeemed for prizes) to counteract phishing attacks.



Source: gophish

Figure 15-3 Phishing simulation dashboard

TWO RIGHTS & A WRONG

1. At a basic level, risk may be defined as a situation that involves exposure to some type of danger, while at a more advanced level, risk can be described as a function of threats, consequences of those threats, and the resulting vulnerabilities.
2. The Annualized Loss Expectancy (ALE) is the expected monetary loss that can be expected for an asset due to a risk over a one-year period.
3. Risk avoidance uses cybersecurity insurance.

See Appendix B for the answer.

DATA PRIVACY

CERTIFICATION

2.1 Explain the importance of security concepts in an enterprise environment.

2.7 Explain the importance of physical security controls.

4.1 Given a scenario, use the appropriate tool to assess organizational security.

5.5 Explain privacy and sensitive data concepts in relation to security.

Privacy is defined as the state or condition of being free from public attention, observation, or interference to the degree that the person chooses. In short, privacy is the right to be left alone to the level that you want.

Prior to the current age of technology, almost everybody (with the exception of media celebrities and politicians) generally could choose the level of privacy that they desired. Those who wanted to have open and public lives could freely provide information about themselves to others. Those who wanted to live quiet or even unknown lives could limit what information was disseminated. In short, both those wanting a public life and those wanting a private life could choose to do so by controlling information about themselves.

However, today that is no longer possible. Data is collected on almost all actions and transactions that individuals perform. This includes data collected through web surfing, purchases (online and in stores), user surveys and questionnaires, and smartphone apps. Data is also collected on benign activities such as the choice of movies streamed through the Internet, the location signals emitted by a smartphone, and even the walking path recorded by a surveillance camera.

As technology devices gather data on user behavior at an unprecedented rate, users are becoming increasingly concerned about how their private data is being collected, used, and stored. Organizations are faced with these growing user concerns and increasing government regulations over data privacy. They must wrestle with how to make legitimate use of user data while responsibly collecting, using, and protecting that data.

Understanding data privacy includes knowing the reasons for user concerns, understanding the consequences of a data breach, and identifying data types. It also involves protecting user private data and destroying it at the end of its life cycle.

NOTE 6

Sometimes a distinction is made between data protection and data privacy. Data protection involves securing data against *unauthorized* access, while data privacy is concerned with the *authorized* access of data, namely who has it and how it is being used. Data protection is a technical issue whereas data privacy is a legal issue.

User Concerns

Users are increasingly concerned over the collection, usage, and protection of their personal data, whether that data is collected with or without their authorization. These user concerns revolve around the risks associated with the use of their private data. This falls into three broad categories:

- *Individual inconveniences and identity theft.* Data that has been collected on individuals is frequently used to direct personalized ad marketing campaigns. These campaigns—which include email, direct mail marketing promotions, and telephone calls—generally are considered annoying and unwanted. In addition, personal data can be used as the basis for identity theft.
- *Associations with groups.* Another use of personal data is to group what appears to be similar individuals. One data broker has 70 distinct segments (*clusters*) within 21 consumer and demographic characteristic groups (*life stages*). These groups range from *Boomer Barons* (baby boomer–aged households with high education and income), *Hard Chargers* (well-educated and professionally successful singles), and *True Blues* (working parents who hold blue-collar jobs with teenage children about to leave home). Once a person is placed in a group, the characteristics of that group are applied, such as whether a person is a "potential inheritor" or an "adult with senior parent," or whether a household has a "diabetic focus" or "senior needs." However, these assumptions may not always be accurate for someone placed within a group. Individuals might be offered fewer services or the wrong types of services based on their association with a group.
- *Statistical inferences.* Statistical inferences are often made that go beyond groupings. For example, researchers have demonstrated that by examining only four data points of credit card purchases (such as the dates and times of purchases) of 1.1 million people, they could correctly identify 90 percent of the people. In another study, the *Likes* indicated by Facebook users can statistically reveal their sexual orientation, drug use, and political beliefs.

NOTE 7

Identity theft is covered in Module 1.

The concerns raised regarding how private data is gathered and used are listed in Table 15-10.

Table 15-10 Concerns regarding how private data is gathered and used

Issue	Explanation
The data is gathered and kept in secret.	Users have no formal rights to find out what private information is being gathered, who gathers it, or how it is being used.
The accuracy of the data cannot be verified.	Because users do not have the right to correct or control what personal information is gathered, its accuracy may be suspect. In some cases, inaccurate or incomplete data may lead to erroneous decisions made about individuals without any verification.
Identity theft can impact the accuracy of data.	Victims of identity theft often have information added to their profile that was the result of actions by the identity thieves, and even the victims have no right to see or correct the information.
Unknown factors can impact overall ratings.	Ratings are often created from combining thousands of individual factors or data streams, including race, religion, age, gender, household income, zip code, presence of medical conditions, transactional purchase information from retailers, and hundreds more data points about individual consumers. How these different factors impact a person's overall rating is unknown.
Informed consent is usually missing or is misunderstood.	Statements in a privacy policy such as "We may share your information for marketing purposes with third parties" is not clearly informed consent to freely allow the use of personal data. Often users are not even asked for permission to gather their information.
Data is being used for increasingly important decisions.	Private data is being used on an ever-increasing basis to determine eligibility in significant life opportunities, such as jobs, consumer credit, insurance, and identity verification.

NOTE 8

Unlike consumer reporting agencies, which are required by federal law to give consumers free copies of their credit reports and allow them to correct errors, those who collect data are not required by federal law to show consumers information that has been collected about them or provide a means of correcting it.

Data Breach Consequences

Once a data breach occurs, specific actionable steps must be taken by the organization. When required, it must notify those impacted by the breach (**public notifications and disclosures**) along with relevant stakeholders. It must also outline the actions that are being taken. Depending upon the severity of the breach, a regulatory agency may even require that a breach be classified as a "major incident" and that additional steps be taken (**escalation**).

The consequences to an organization that has suffered a data breach are not insignificant. These consequences include the following:

- *Reputation damage*. The bad publicity surrounding an organization that has been the victim of a data breach usually results in a tarnished reputation (**reputation damage**). This has been evidenced by the loss of customers and a drop in the stock price of publicly traded organizations following a breach.
- *IP theft*. Another consequence of a data breach is the theft of IP that the organization or its customers may own.
- *Fines*. A financial penalty (**fine**) may be assessed against the organization following a data breach. Several federal and state laws have been enacted to protect the privacy of electronic data, and businesses that fail to protect data they possess may face serious financial penalties. Some of these laws include the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Sarbanes-Oxley Act of 2002 (Sarbox), the Gramm-Leach-Bliley Act (GLBA), the Payment Card Industry Data Security Standard (PCI DSS), the Family Educational Rights and Privacy Act (FERPA), and various state notification and security laws. Organizations in nations that belong to the European Union (EU) face two tiers of fines due to a data breach based on the General Data Protection Regulation (GDPR). The first tier is a fine of up to 10 million euros or 2 percent of the firm's worldwide annual revenue from the preceding year, whichever amount is higher. The second tier is 20 million euros or 4 percent of worldwide annual revenue.

NOTE 9

Many users are surprised to learn that the rules regarding a breach of a small number of medical records are not strong. The HIPAA Breach Notification Rule requires that data breaches of 500 or more records must be reported to the Secretary of the Department of Health and Human Services (HHS) no later than 60 days after the discovery of a breach. Breaches of fewer than 500 records can be reported to the Secretary at any time, but no later than 60 days from the end of the calendar year in which the data breach was experienced. That means a breach of 450 records that occurred in January 2021 would not have to be reported until March 2022.

Data Types

Different data types require protection besides customer data, financial information, and government data. Several of these are listed in Table 15-11.

Protecting Data

An organization may take various steps to protect consumer data. It is important to begin with an **impact assessment**, which is a means for measuring the effectiveness of the organization's activities. The impact assessment can help reveal any shortcomings around the use and protection of privacy data.

In most instances, organizations fall short of informing users of what is being collected and how it is being used. Organizations should have a **privacy notice** that outlines how the organization uses personal information it collects. A typical privacy notice for consumers is shown in Figure 15-4.

A **terms of agreement** document sets out what is expected from both the organization and its users. This agreement can be used to manage users' activity and expectations and also to protect the organization from legal issues.

Different technologies can be used to enhance the protection of privacy data. These include the following:

- *Data minimization*. **Data minimization** is limiting the collection of personal information to that which is directly relevant and necessary to accomplish a specific task. In other words, the collection of privacy data should be adequate, relevant, and not excessive in relation to the designated purpose. Organizations should periodically review their privacy data collection to ensure that the collection is following the principle of data minimization.

Table 15-11 Data types

Data type	Description	Recommended handling
Confidential	Highest level of data sensitivity	Should only be made available to users with highest level of pre-approved authentication
Private	Restricted data with a medium level of confidentiality	For users who have a need-to-know basis of the contents
Sensitive	Data that could cause catastrophic harm to the company if disclosed, such as technical specifications for a new product	Restricted to employees who have a business need to access the data and have been approved
Critical	Data classified according to availability needs; if critical data not available, the function and mission would be severely impacted	Critical data must be rigorously protected
Proprietary	Belongs to the enterprise	Can be available to any current employee or contractor
Public	No risk of release	For all public consumption; data is assumed to be public if no other data label is attached
Personally Identifiable Information (PII)	Data that could potentially identify a specific individual	Should be kept secure so that an individual cannot be singled out for identification
Protected Health Information (PHI)	Data about a person's health status, provision of health care, or payment for health care	Must be kept secure as mandated by HIPAA

- *Data masking*. **Data masking** involves creating a copy of the original data but obfuscating (making unintelligible) any sensitive elements such as a user's name or Social Security number. Data masking should replace all actual information that is not absolutely required. Because data masking involves replacing data elements, it is also called **data anonymization**: there is not a means to reverse the process to restore the data back to its original state. Data masking is one way to perform **data sanitization**, which is the process of cleaning data to provide privacy protection.
- *Tokenization*. Similar to masking, tokenization obfuscates sensitive data elements, such as an account number, into a random string of characters (token). The original sensitive data element and the corresponding token are then stored in a database called a token vault so that if the actual data element is needed, it can be retrieved. Unlike encryption, which requires using an algorithm and a key, tokenization can hide the data while making the retrieval process more seamless. Because it is possible to restore the original data, tokenization is also called **pseudo-anonymization**.

In general, you can visit us on the Internet without telling us who you are and without giving any personal information about yourself. There are times, however, when we or our partners may need information from you. You may choose to give us personal information in a variety of situations. For example, you may want to give us information, such as your name and address or e-mail, to correspond with you, to process an order, or to provide you with a subscription. You may give us your credit card details to buy something from us or a description of your education and work experience in connection with a job opening for which you wish to be considered. We intend to let you know how we will use such information before we collect it from you. You may tell us that you do not want us to use this information to make further contact with you beyond fulfilling your request. If you give us personal information about somebody else, such as a spouse or work colleague, we will assume that you have their permission to do so.

Figure 15-4 Privacy notice

NOTE 10

Data masking and tokenization are covered in Module 9.

A final consideration is to know the country-specific government regulations that apply to protecting data. However, these regulations are not necessarily those where the organization is headquartered. **Data sovereignty** is the country-specific requirements that apply to data. Generally, data is subject to the laws of the country in which it is collected or processed. In many instances, the data must remain within its borders. Countries such as Russia, China, Germany, France, Indonesia, and Vietnam require that citizen data must be stored on physical servers within the country's borders, arguing that it is in the citizens' (and government's) best interest to protect private data against any misuse from foreign governments, and this is not possible if the data is outside of that country's jurisdiction.

NOTE 11

Many countries have had laws on the books for decades that data of its citizens must be stored within its borders, but it was less of an issue and was not always enforced. However, new privacy laws such as the GDPR in the European Union is now making data sovereignty and data privacy more prominent. With the rising popularity of cloud computing and Software as a Service (SaaS) solutions, data sovereignty issues have taken on even greater importance.

Data Destruction

The **information life cycle** is the flow of an information system's data (and metadata) from data creation to the time it becomes obsolete. Once data is no longer useful, it should be properly destroyed.

Because data itself is intangible, destroying data that is no longer needed involves destroying the media on which the data is stored. If any data is on paper and is not labeled as public, that media should never be thrown away in a dumpster, recycle bin, or trash receptacle. Paper media can be destroyed by **burning** (lighting it on fire), **shredding** (cutting it into small strips or particles), **pulping** (breaking the paper back into wood cellulose fibers after the ink is removed), or **pulverizing** ("hammering" the paper into dust).

If data is on electronic media, the data should never be erased using the operating system's "delete" command (*purging*). Deleted data can still be retrieved using third-party tools. Instead, data sanitation tools can be employed to securely remove data. One technique is called *wiping* (overwriting the disk space with zeroes or random data). For a magnetic-based hard disk drive, **degaussing** permanently destroys the entire drive by reducing or eliminating the magnetic field. Normally, degaussing is a **third-party solution** because it is a specialized technique requiring special equipment.

NOTE 12

There is no universal agreement on the differences between purging and wiping.

Consideration on which data destruction technique to use may hinge upon the need to verify the destruction for regulatory purposes. Some techniques cannot provide this verification. For example, degaussing cannot verify that the drive was destroyed. In this instance, it may be necessary to first wipe the drive to verify that all data has been destroyed and then degauss the drive to destroy the data completely and permanently.

TWO RIGHTS & A WRONG

1. The data type "confidential" has the highest level of data sensitivity.
2. Tokenization is a process that is part of data anonymization.
3. "Pulverizing" is hammering paper into dust.

See Appendix B for the answer.

VM LAB You're now ready to complete the live, virtual machine labs for this module. The labs can be found in the Practice It folder in each MindTap module.

SUMMARY

- A risk is a situation that involves exposure to some type of danger. There are many different types of risk. An internal risk comes from within an organization (such as employee theft), while an external risk is from the outside (such as the actions of a hactivist). One type of platform well known for its risks is a legacy system. Although legacy hardware introduces some risks, more often risks result from legacy software, such as an OS or program. Often overlooked in identifying risk types is the impact that vulnerabilities of one organization can have on other organizations connected to it. Intellectual property (IP) theft involves threat actors who attempt to steal IP and profit from it. Specialized software that an enterprise uses is subject to licensing restrictions to protect the rights of the developer. Software compliance and licensing risks are today considered a serious problem for organizations. Most organizations unknowingly violate one or more licensing agreements.

- It is important for an organization to regularly perform a risk analysis, or a process to identify and assess the factors that may jeopardize the success of a project or reaching a stated goal. Identifying risks can be difficult due to the elusive nature of risks, unconscious human biases, and prejudices toward certain types of risks. Risk Control Self-Assessment (RCSA) is an "empowering" methodology by which management and staff at all levels collectively work to identify and evaluate risks. The goal of RCSA is to not only minimize biases and prejudices but also to integrate risk management practices into the culture of the organization.
- There are two approaches to risk calculation: qualitative risk calculation, which uses an "educated guess" based on observation, and quantitative risk calculation, which is considered more scientific. Quantitative risk calculations can be divided into the likelihood of a risk and the impact of a risk being successful. The tools used for calculating risk likelihood include Mean Time Between Failure (MTBF), Mean Time To Recovery (MTTR), Mean Time To Failure (MTTF), Failure In Time (FIT), and the Annualized Rate of Occurrence (ARO). Risk impact calculation tools include Single Loss Expectancy (SLE) and Annual Loss Expectancy (ALE).
- Several approaches are used to reduce risk. An organization can accept, transfer, avoid, or mitigate risks. A security control is a safeguard or countermeasure employed within an organizational information system to protect the confidentiality, integrity, and availability of a technology system and its data. It attempts to limit exposure to a danger. There are three broad categories of controls: managerial, operational, and technical. Specific types of controls are found within these three broad categories. Inherent risk is defined as the current risk level given the existing set of controls. Residual risk is the risk level that remains after additional controls are applied. A specific type of risk is a control risk or the probability that financial statements are materially misstated because of failures in the system of controls used by an organization.
- Several risks are associated with using third parties. One of the means by which the parties can reduce risk is to reach an understanding of their relationships and responsibilities through interoperability agreements, or formal contractual relationships, particularly as they relate to security policy and procedures. These agreements should be regularly reviewed to verify compliance and performance standards.
- An often-overlooked consideration in risk management is the importance of providing training to users. Training results in risk awareness, which is the raising of understanding of what risks exist, their potential impacts, and how they are managed. When conducting training, all users should be involved. Understanding the traits of learners and different learning styles is important. Different techniques are used for user training. Computer-based training (CBT) uses a computer to deliver the instruction. It is popular for user training due its flexibility (training can be done from any location and at any time) and ability to provide feedback about the progress of the learner. However, CBT is not always considered the best means for training. Role-based training involves specialized training that is customized to the specific role that an employee holds in the organization. Gamification is using game-based scenarios for instruction. User training can often include gamification in an attempt to heighten the interest and retention of the learner. When training security professionals, sometimes organizations add an incentive called a capture the flag (CTF) exercise. A series of challenges with varying degrees of difficulty is outlined in advance. When one challenge is solved, a "flag" is given to the participant, and the points are totaled once time has expired. The winning player or team is the one that earns the highest score. Because phishing is the primary means by which threat actors initially launch an attack, many organizations use phishing simulations to help employees recognize phishing emails.
- Privacy is defined as the state or condition of being free from public attention, observation, or interference to the degree that the person chooses. Today data is collected on almost all actions and transactions that individuals perform. As technology devices gather data on user behavior at an unprecedented rate, users are becoming increasingly concerned about how their private data is being collected, used, and stored. Organizations are faced with these growing user concerns and increasing government regulations over data privacy. They must wrestle with how to legitimately employ user data while responsibly collecting, using, and protecting that data.
- Once a data breach occurs, an organization must take specific actionable steps. When required, it must notify those impacted by the breach (public notifications and disclosures) along with relevant stakeholders. It must also outline the actions that are being taken. Depending upon the severity of the breach, a regulatory agency

may even require that a breach be classified as a "major incident" and that additional steps be taken (escalation). The consequences to an organization that has suffered a data breach are significant. These include reputation damage, IP theft, and fines.

- Different data types require protection besides customer data, financial information, and government data. These types are confidential, private, sensitive, critical, proprietary, public, personally identifiable information (PII), and protected health information (PHI). An organization may take various steps to protect consumer data. It is important to begin with an impact assessment, which is a means for measuring the effectiveness of the organization's activities. Technologies that can be used to enhance data protection include data minimization, data anonymization, data sanitization, and pseudo-anonymization. Data sovereignty is the country-specific requirements that apply to data. Generally, data is subject to the laws of the country in which it is collected or processed.
- Once data is no longer useful, it should be properly destroyed. Because data itself is intangible, destroying data that is no longer needed involves destroying the media on which the data is stored. Data on paper that is not labeled as public should never be thrown away in a dumpster, recycle bin, or trash receptacle. Paper media can be destroyed by burning (lighting it on fire), shredding (cutting it into small strips or particles), pulping (breaking the paper back into wood cellulose fibers after the ink is removed), or pulverizing ("hammering" the paper into dust). If data is on electronic media, the data should never be erased using the operating system "delete" command (purging). Deleted data can still be retrieved by using third-party tools. Instead, data sanitation tools can be employed to securely remove data. One technique is called wiping (overwriting the disk space with zeroes or random data). For a magnetic-based hard disk drive, degaussing will permanently destroy the entire drive by reducing or eliminating the magnetic field.

Key Terms

acceptance
Annualized Loss Expectancy (ALE)
Annualized Rate of Occurrence (ARO)
asset value
avoidance
burning
business partners
business partnership agreement (BPA)
capture the flag (CTF)
compensating controls
computer-based training (CBT)
confidential
control risk
corrective controls
critical
cybersecurity insurance
data anonymization
data masking
data minimization
data sanitization
data sovereignty
degaussing
detective controls
deterrent controls
end of life (EOL)
end of service (EOS)
escalation
external risk
fine
gamification
impact assessment
information life cycle
inherent risk
internal risk
IP theft
likelihood of occurrence
managerial controls
measurement system analysis (MSA)
memorandum of understanding (MOU)
mitigation
multiparty
nondisclosure agreement (NDA)
operational controls
Personally Identifiable Information (PII)
phishing campaign
phishing simulations
physical controls
preventative controls
privacy notice
privacy
private
proprietary
Protected Health Information (PHI)
pseudo-anonymization
public
public notifications and disclosures
pulping
pulverizing
qualitative risk assessment
quantitative risk assessment
regulations that affect risk posture
reputation damage
residual risk
risk
risk appetite
risk awareness
Risk Control Self-Assessment (RCSA)
risk matrix/heatmap
risk register
role-based awareness training
sensitive
service-level agreement (SLA)
shredding
Single Loss Expectancy (SLE)
software compliance and licensing
technical controls
terms of agreement
third-party solution
transference
vendors

Review Questions

1. Which of the following threats would be classified as the actions of a hactivist?
   a. External threat
   b. Internal threat
   c. Environmental threat
   d. Compliance threat

2. Which of these is NOT a response to risk?
   a. Mitigation
   b. Transference
   c. Resistance
   d. Avoidance

3. Which of the following is NOT a threat classification category?
   a. Compliance
   b. Financial
   c. Tactical
   d. Strategic

4. In which of the following threat classifications would a power blackout be classified?
   a. Operational
   b. Managerial
   c. Technical
   d. Strategic

5. Which of the following approaches to risk calculation typically assigns a numeric value (*1–10*) or label (*High, Medium,* or *Low*) to represent a risk?
   a. Quantitative risk calculation
   b. Qualitative risk calculation
   c. Rule-based risk calculation
   d. Policy-based risk calculation

6. What is a list of potential threats and associated risks?
   a. Risk assessment
   b. Risk matrix
   c. Risk register
   d. Risk portfolio

7. Giovanni is completing a report on risks. To which risk option would he classify the action that the organization has decided not to construct a new a data center because it would be located in an earthquake zone?
   a. Transference
   b. Avoidance
   c. Rejection
   d. Prevention

8. Which of the following control categories includes conducting workshops to help users resist phishing attacks?
   a. Managerial
   b. Operational
   c. Technical
   d. Administrative

9. Emiliano needs to determine the expected monetary loss every time a risk occurs. Which formula will he use?
   a. AV
   b. SLE
   c. ARO
   d. ALE

10. Enzo is reviewing the financial statements and has discovered a serious misstatement. What type of risk has he found?
    a. Control risk
    b. Financial risk
    c. Reporting risk
    d. Monetary risk

11. Simona needs to research a control that attempts to discourage security violations before they occur. Which control will she research?
    a. Deterrent control
    b. Preventive control
    c. Detective control
    d. Corrective control

12. Which of the following is NOT a legally enforceable agreement but is still more formal than an unwritten agreement?
    a. BPA
    b. SLA
    c. MOU
    d. MSA

13. Angelo has received notification that a business partner will no longer sell or update a specific product. What type of notification is this?
    a. EOA
    b. EOP
    c. EOL
    d. EOS

14. Which of the following is NOT a concern for users regarding the usage of their privacy data?
    a. Associations with groups
    b. Individual inconveniences and identity theft
    c. Timeliness of data
    d. Statistical inferences

15. Which of the following is NOT a consequence to an organization that has suffered a data security breach?
- **a.** Reputation damage
- **b.** IP theft
- **c.** De-escalation of reporting requirements
- **d.** Monetary fine

16. Which of the following data types has the highest level of data sensitivity?
- **a.** Private
- **b.** Secure
- **c.** Sensitive
- **d.** Confidential

17. Sergio has been asked to make a set of data that was once restricted now available to any users. What data type will Sergio apply to this set of data?
- **a.** Open
- **b.** Unrestricted
- **c.** Public
- **d.** Available

18. Which of the following uses data anonymization?
- **a.** Tokenization
- **b.** Data masking
- **c.** Data minimization
- **d.** Data obfuscation sanitization (DOS)

19. Which of the following is NOT true about data sovereignty?
- **a.** Data sovereignty is a concept that until recently was less of an issue.
- **b.** Generally, data is subject to the laws of the country in which it is collected or processed.
- **c.** Governments cannot force companies to store data within specific countries.
- **d.** Regulations are not necessarily on where an organization is headquartered.

20. Bob needs to create an agreement between his company and a third-party organization that demonstrates a "convergence of will" between the parties so that they can work together. Which type of agreement will Bob use?
- **a.** SLA
- **b.** BPA
- **c.** ISA
- **d.** MOU

Hands-On Projects

CAUTION If you are concerned about installing any of the software in these projects on your regular computer, you can instead use the Windows Sandbox or install the software in the Windows virtual machine created in the Module 1 Hands-On Projects. Software installed within the virtual machine will not impact the host computer.

Project 15-1: Viewing Your Annual Credit Report

Time Required: 25 minutes

Objective: 5.5 Explain privacy and sensitive data concepts in relation to security.
- Organizational consequences of privacy breaches

Description: Security experts recommend that consumers reduce personal risk and protect their identity by receiving a copy of their credit report at least once per year to check its accuracy. In this project, you access your free credit report online.

1. Use your web browser to go to **www.annualcreditreport.com**. Although you could send a request individually to one of the three credit agencies, this website acts as a central source for ordering free credit reports.
2. Click **Request your free credit reports**.
3. Read through the three steps and click **Request your credit reports**.
4. Enter the requested information, click **Continue**, and then click **Next**.
5. Click **TransUnion**. Click **Next**.
6. After the brief processing completes, click **Continue**.
7. You may then be asked personal information about your transaction history to verify your identity. Answer the requested questions and click **Next**.
8. Follow the instructions to print your report.

9. Review it carefully, particularly the sections of "Potentially negative items" and "Requests for your credit history." If you see anything that might be incorrect, follow the instructions on that website to enter a dispute.
10. Follow the instructions to exit from the website.
11. Close all windows.

Project 15-2: Using a Nonpersistent Web Browser

Time Required: 25 minutes

Objective: 5.5 Explain privacy and sensitive data concepts in relation to security.

- Privacy enhancing technologies

Description: Nonpersistence tools are used to ensure that unwanted data is not carried forward but instead a clean image is used. This helps protect user privacy. One common tool is a web browser that retains no information such as cookies, history, passwords, or any other data and requires no installation but runs from a USB flash drive. In this project, you download and install a nonpersistent web browser.

1. Use your web browser to go to **www.browzar.com**. (If you are no longer able to access the program through this URL, use a search engine and search for "Browzar.")
2. Click **Key Features** and read about the features of Browzar.
3. Click **Help & FAQs** and read the questions and answers.
4. Click **Download now – it's FREE!**
5. Choose one of the available themes and click **Download**.
6. Click **Accept**.
7. Click **Download**.
8. Click the downloaded file to run Browzar. Note that no installation is required and the browser can be run from a USB flash drive.
9. From Browzar, go to **www.google.com**.
10. Enter **Cengage** in the search bar to search for information about Cengage.
11. Click the red **X** in the upper-right corner to close the browser. What information appears in the pop-up window? What happens when you close the browser?
12. Launch Browzar again.
13. Click **Tools**.
14. Click **Secure delete**.
15. Click **More**. What additional protections does Secure Delete give?
16. Close all windows.

Project 15-3: Online Phishing Training

Time Required: 25 minutes

Objective: 5.3 Explain the importance of policies to organizational security.

- Diversity of training techniques

Description: In this project, you will use an online phishing training tool. Note the user awareness training features in this simulation as you proceed.

1. Use your web browser to go to **public.cyber.mil/training/phishing-awareness/**. (If you are no longer able to access the program through this URL, use a search engine and search for "phishing awareness.")
2. Click **Launch Training**.
3. If necessary, adjust your web browser settings, and then click **Start/Continue Phishing Awareness**.
4. Watch the brief video on accessibility features. Click the right arrow button.
5. Read the information. Click either the URL or **Continue**, depending upon your needs.
6. Listen to the video message about your choice. Is this a good learning technique? Why? Click the right arrow button.
7. Continue through the phishing training. Slides 16–18 ask you for answers to questions about what you have learned.
8. How effective was this training? What did you learn? Would you recommend this to others to learn about phishing?
9. Close all windows.

Case Projects

Case Project 15-1: Multiparty Risks

Until recently, multiparty risks have not been considered as serious. Use the Internet to research multiparty risks. Why is there now heightened emphasis on multiparty risks? What are three examples of security incidents that were the result of a vulnerability in one organization affecting multiple other organizations? What were the outcomes of each of these? Should an organization that allows other organizations to be compromised through a multiparty risk be held liable? What should be the penalty? How can these be mitigated? Write a one-page paper on your findings.

Case Project 15-2: Intellectual Property (IP) Theft

Use the Internet to find details on four recent incidents of intellectual property (IP) theft from an organization. What was stolen? What vulnerability did the threat actors exploit? How valuable was the IP? What did the threat actors do with it? What loss did it create for the organization? How could it have been prevented? Write a one-page paper on your findings.

Case Project 15-3: Unconscious Biases in Cybersecurity

How could unconscious biases impact cybersecurity? Review the information in Table 15-4 and select four of the biases. Then create a practical example of how each bias or effect could impact cybersecurity. Now return to the table and list in order what you consider your own biases from most prevalent to least. What can be done to minimize the impact of these biases?

Case Project 15-4: Reacting to Risks

Using the six reactions to risks in this module, identify a specific risk that you would place in each category. This risk should be something that involves you by identifying intentional actions, accidents, etc. Evaluate your reaction to these risks. Could these play a part in how you might evaluate cybersecurity risks in an organization? How could they be addressed? Write a one-page paper on your analysis.

Case Project 15-5: User Awareness and Training

What user security awareness and training is available at your school or place of business? How frequently is it performed? Is it available online or in person? Is it required? Are the topics up to date? On a scale of 1–10, how would you rate the training? How could it be improved? Write a one-page summary.

Case Project 15-6: Privacy Notices

Identify four different privacy notices and read through them. What information do they contain? How easy are they to understand? Who are they intended to protect, the user or the organization? Now assign a letter grade (A–F) for each notice. Finally, using these as a basis, write your own privacy notice that you consider to be thorough and fair. How does it differ from those that you have found? Why? Write a one-page summary.

Case Project 15-7: North Ridge Security

North Ridge Security provides security consulting and assurance services. You have recently been hired as an intern to assist them.

Firm and Fit (FAF) is a regional health and fitness chain that is rapidly expanding. However, a new CIO is concerned that FAF has not been realistic about the cybersecurity risks that they face, yet he is having difficulty convincing the other senior vice presidents (SVPs) of this concern. Because FAF has not been the victim of a major attack, the other SVPs think that the security posture of PIU is fine. The new CIO has contracted with North Ridge Security to help provide information to the SVPs about risk. You have been asked to make a presentation to them.

1. Create a PowerPoint presentation for the SVPs of FAF about managing risk. Include a definition of risk, different risk types, how to perform a risk analysis, and good risk management procedures. Your presentation should contain at least 10 slides.
2. After the presentation, the SVPs have agreed that they need to look more thoroughly into risk at FAF, particularly as it relates to their business partners and other third-party entities. They have asked you how best to implement third-party risk management. Create a memo with your recommendations.

Case Project 15-8: Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. Go to **community.cengage.com/infosec2** and click the *Join or Sign in* icon to log in, using your login name and password that you created in Module 1. Click **Forums (Discussion)** and click on **Security+ Case Projects (7th edition)**. Read the following case study.

Are you concerned about your data privacy? Have you taken concrete steps to limit the exposure of your data? If so, what are they? How far would you go to protect your data? Would you stop using social media if it meant your data was less exposed? What, if any, restrictions should there be on organizations that collect, use, and store your personal information? Should there be government regulations on user data? If so, what should they look like? Post your opinions to on the Community Site discussion board.

References

1. Cunningham, Margaret, "'Thinking about thinking' is critical to cybersecurity," *Forcepoint*, June 10, 2019, accessed June 17, 2019, www.forcepoint.com/blog/insights/thinking-about-thinking-critical-cybersecurity.
2. Zorz, Zeljka, "How human bias impacts cybersecurity decision making," *HelpNetSecurity*, June 10, 2019, accessed June 12, 2019, www.helpnetsecurity.com/2019/06/10/cybersecurity-decision-making/.