Microsoft

Describe the basic concepts of cybersecurity

FIRST DISTRIBUTION™
Epsidon Technology Holdings

Describe what is cybersecurity

People, organizations, and governments are routinely falling victim to cyberattacks. We constantly hear references to concepts like cybersecurity, cyberattacks, cybercriminals, and more. This can all sound daunting and difficult to grasp. To protect yourself and those around you, you'll need to have a basic understanding of these concepts.

What is a cyberattack?

A cyberattack is commonly defined as an attempt to gain illegal access to a computer or computer system to cause damage or harm. But only thinking of computers or computer systems, in a traditional sense, is limiting. The reality is that a cyberattack can occur on almost any modern digital device. The impact can range from an inconvenience for an individual to global economic and social disruption.

An attacker can use people, computers, phones, applications, messages, and system processes to carry out an attack. Individuals, organizations, institutions, and governments can be victims of an attack. These attackers might:

Lock data and processes and demand a ransom.
Remove vital information to cause serious harm.
Steal information.
Publicly expose private information.
Stop vital business processes and systems from running, to cause disruption and malfunction.

With cyberattacks continuously evolving, it's important for you to remember that attackers don't exclusively need a computer to carry out an attack. Also, attacks can vary widely in their nature and scope. Any digitally connected device or entity can be used as part of an attack, or be subject to an attack.

What is a cybercriminal?

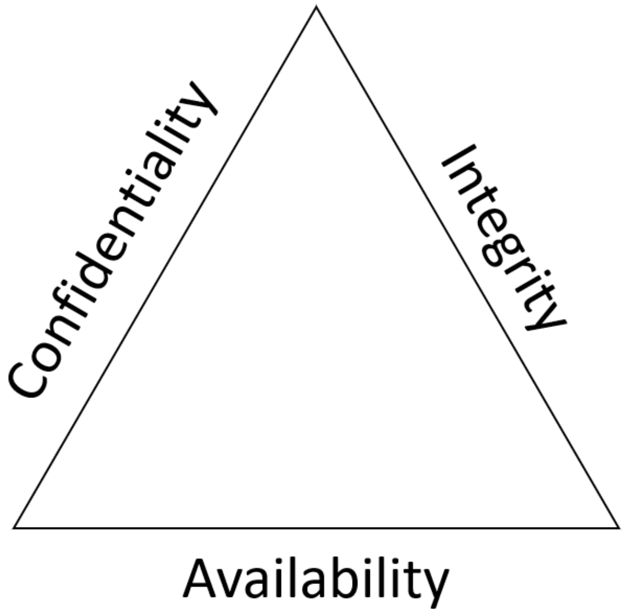
A cybercriminal is anyone who carries out a cyberattack. Cybercriminals can be:

- A single person or a group of people.
- An organization for hire.
- A government entity.

Cybercriminals can be located anywhere, including embedded inside an organization or institution, to cause damage from within.

What is cybersecurity?

Cybersecurity refers to technologies, processes, and training that help protect systems, networks, programs, and data from cyberattacks, damage, and unauthorized access. Cybersecurity enables you to achieve the following goals:



- **Confidentiality**: Information should only be visible to the right people.
- **Integrity**: Information should only be changed by the right people or processes.
- **Availability**: Information should be visible and accessible whenever needed.

https://docs.microsoft.com/en-us/learn/modules/describe-basic-cybersecurity-threats-attacks-mitigations/3-describe-threat-landscape

Describe the threat landscape

Completed100 XP

- 7 minutes

You've now learned about cyberattacks, cybercriminals, and cybersecurity. But you'll also need to understand the means cybercriminals can use to carry out attacks and achieve their aims. To do this, you'll learn about concepts like the threat landscape, attack vectors, security breaches, and more.

What is the threat landscape?

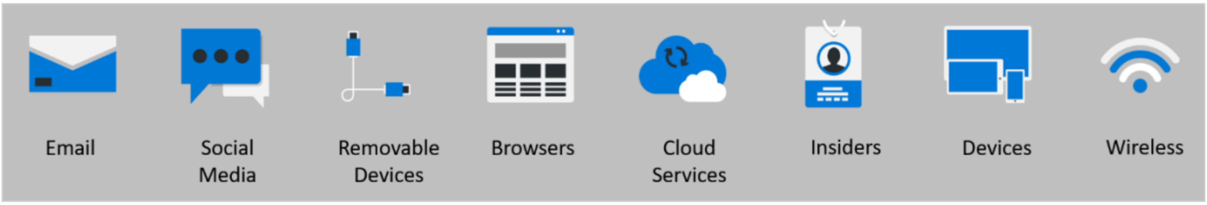
Whether an organization is big or small, the entirety of the digital landscape with which it interacts represents an entry point for a cyberattack. These can include:

- Email accounts
- Social media accounts
- Mobile devices
- The organization's technology infrastructure
- Cloud services
- People

Collectively, these are referred to as the threat landscape. Notice that the threat landscape can cover more than just computers and mobile phones. It can include any elements that are owned or managed by an organization, or some that are not. As you'll learn next, criminals will use any means they can to mount and carry out an attack.

What are attack vectors?

An attack vector is an entry point or route for an attacker to gain access to a system.



Email is perhaps the most common attack vector. Cybercriminals will send seemingly legitimate emails that result in users taking action. This might include downloading a file, or selecting a link that will compromise their device. Another common attack vector is through wireless networks. Bad actors will often tap into unsecured wireless networks at airports or coffee shops, looking for vulnerabilities in the devices of users who access the wireless network. Monitoring social media accounts, or even accessing devices that are left unsecured, are other commonly used routes for cyberattacks. However, you should know that attackers don’t need to rely on any of these. They can use a variety of less obvious attack vectors. Here are some examples:

- **Removable media**. An attacker can use media such as USB drives, smart cables, storage cards, and more to compromise a device. For example, attackers might load malicious code into USB devices that are subsequently provided to users as a free gift, or left in public spaces to be found. When they're plugged in, the damage is done.
- **Browser**. Attackers can use malicious websites or browser extensions to get users to download malicious software on their devices, or change a user's browser settings. The device can then become compromised, providing an entry point to the wider system or network.
- **Cloud services**. Organizations rely more and more on cloud services for day-to-day business and processes. Attackers can compromise poorly secured resources or services in the cloud. For example, an attacker could compromise an account in a cloud service, and gain control of any resources or services accessible to that account. They could also gain access to another account with even more permissions.
- **Insiders**. The employees of an organization can serve as an attack vector in a cyberattack, whether intentionally or not. An employee might become the victim of a cybercriminal who impersonates them as a person of authority to gain unauthorized access to a system. This is a form of social engineering attack. In this scenario, the employee serves as an unintentional attack vector. In some cases, however, an employee with authorized access may use it to intentionally steal or cause harm.

What are security breaches?

Any attack that results in someone gaining unauthorized access to devices, services, or networks is considered a security breach. Imagine a security breach as similar to a break-in where an intruder (attacker) successfully breaks into a building (a device, application, or network).

Security breaches come in different forms, including the following:

Social engineering attacks

It is common to think about security breaches as exploiting some flaw or vulnerability in a technology service or piece of equipment. Likewise, you might believe that security breaches only happen because of vulnerabilities in technology. But that’s not the case. Attackers can use social engineering attacks to exploit or manipulate users into granting them unauthorized access to a system.

In social engineering, impersonation attacks happen when an unauthorized user (the attacker), aims to gain the trust of an authorized user by posing as a person of authority to access a system from some nefarious activity. For example, a cybercriminal might pretend to be a support engineer to trick a user into revealing their password to access an organization's systems.

Browser attacks

Whether on a desktop, laptop, or phone, browsers are an important access tool for the internet. Security vulnerabilities in a browser can have a significant impact because of their pervasiveness. For example, suppose a user is working on an important project with a looming deadline. They want to figure out how to solve a particular problem for their project. They find a website that they believe will provide a solution.

The website asks the user to make some changes to their browser settings so they can install an add-on. The user follows the instructions on the website. Unknown to them, the browser is now compromised. This is a browser modifier attack, one of many different types used by cybercriminals. An attacker can now use the browser to steal information, monitor user behavior, or compromise a device.

Password attacks

A password attack is when someone attempts to use authentication for a password-protected account to gain unauthorized access to a device or system. Attackers often use software to speed up the process of cracking and guessing passwords. For example, suppose an attacker has somehow discovered someone's username for their work account.

The attacker then tries a vast number of possible password combinations to access the user's account. The password only has to be correct once for the attacker to get access. This is known as a brute force attack and is one of many ways in which a cybercriminal can use password attacks.

What are data breaches?

A data breach is when an attacker successfully gains access or control of data. Using the intruder example, this would be similar to that person getting access to, or stealing, vital documents and information inside the building:

When an attacker achieves a security breach, they'll often want to target data, because it represents vital information. Poor data security can lead to an attacker gaining access and control of data. This can lead to serious consequences for the victim, whether that is a person, organization, or even a government. This is because the victim's data could be abused in many ways. For example, it can be held as ransom or used to cause financial or reputational harm.

https://docs.microsoft.com/en-us/learn/modules/describe-basic-cybersecurity-threats-attacks-mitigations/4-describe-malware

Describe malware

Completed 100 XP

- 4 minutes

You've heard about terms like malware, viruses, worms, and so on. But what do these things mean? Is a virus a worm? Exactly what does malware do? These are just some of the basic concepts you'll learn about in this unit.

What is malware?

Malware comes from the combination of the words malicious and software. It's a piece of software used by cybercriminals to infect systems and carry out actions that will cause harm. This could include stealing data or disrupting normal usage and processes.

Malware has two main components:

- Propagation mechanism
- Payload

What is a propagation mechanism?

Propagation is how the malware spreads itself across one or more systems. Here are a few examples of common propagation techniques:

Virus

Most of us are already familiar with this term. But what does it actually mean? First, let’s think about viruses in non-technical terms. In biology, for example, a virus enters the human body, and once inside, can spread and cause harm. Technology-based viruses depend on some means of entry, specifically a user action, to get into a system. For example, a user might download a file or plug in a USB device that contains the virus, and contaminates the system. You now have a security breach.

Worm

In contrast to a virus, a worm doesn't need any user action to spread itself across systems. Instead, a worm causes damage by finding vulnerable systems it can exploit. Once inside, the worm can spread to other connected systems. For example, a worm might infect a device by exploiting a vulnerability in an application that runs on it.

The worm can then spread across other devices in the same network and other connected networks.

Trojan

A trojan horse attack gets its name from classical history, where soldiers hid inside a wooden horse that was presented as a gift to the Trojans. When the Trojans brought the wooden horse into their city, the soldiers emerged from hiding and attacked. In the context of cybersecurity, a trojan is a type of malware that pretends to be a genuine piece of software. When a user installs the program, it can pretend to be working as advertised, but the program also secretly performs malicious actions such as stealing information.

What is a payload?

The payload is the action that a piece of malware performs on an infected device or system. Here are some common types of payload:

- **Ransomware** is a payload that locks systems or data until the victim has paid a ransom. Suppose there's an unidentified vulnerability in a network of connected devices. A cybercriminal can exploit this to access and then encrypt all files across this network. The attacker then demands a ransom in return for decrypting the files. They might threaten to remove all of the files if the ransom hasn't been paid by a set deadline.
- **Spyware** is a type of payload that spies on a device or system. For example, the malware may install keyboard scanning software on a user's device, collect password details, and transmit them back to the attacker, all without the user's knowledge.
- **Backdoors**: A backdoor is a payload that enables a cybercriminal to exploit a vulnerability in a system or device to bypass existing security measures and cause harm. Imagine that a cybercriminal infiltrates a software developing company and leaves some code that allows them to carry out attacks. This becomes a backdoor that the cybercriminal could use to hack into the application, the device it's running on, and even the organization's and customers' networks and systems.
- **Botnet** is a type of payload that joins a computer, server, or another device to a network of similarly infected devices that can be controlled remotely to carry out some nefarious action. A common application of botnet malware is crypto-mining (often referred to as crypto-mining malware). In this case, the malware connects a device to a botnet that consumes the device's computing power to mine or generate cryptocurrencies. A user might notice their computer is running slower than normal and getting worse by the day.

https://docs.microsoft.com/en-us/learn/modules/describe-basic-cybersecurity-threats-attacks-mitigations/1-introduction

Describe basic mitigation strategies

Completed100 XP

- 4 minutes

You've learned that there are many different types of cyberattack. But how do you defend your organization against cybercriminals? There are several different ways that you can keep cyberattackers at bay, from multifactor authentication to improved browser security, and by informing and educating users.

What is a mitigation strategy?

A mitigation strategy is a measure or collection of steps that an organization takes to prevent or defend against a cyberattack. This is usually done by implementing technological and organizational policies and processes designed to protect against attacks. Here are some of the many different mitigation strategies available to an organization:

Multifactor authentication

Traditionally, if someone's password or username is compromised, this allows a cybercriminal to gain control of the account. But multifactor authentication was introduced to combat this.

Multifactor authentication works by requiring a user to provide multiple forms of identification to verify that they are who they claim to be. The most common form of identification used to verify or authenticate a user is a password. This represents something the user knows.

Two other authentication methods provide something the user *is*, such as a fingerprint or retinal scan (a biometric form of authentication), or provide something the user *has*, such as a phone, hardware key, or other trusted device. Multifactor authentication employs two or more of these forms of proof to verify a valid user.

For example, a bank might require a user to provide security codes sent to their mobile device, in addition to their username and password, to access their online account.

Browser security

We all rely on browsers to access the internet to work and carry out our daily tasks. As you've learned earlier, attackers can compromise poorly secured browsers. A user might download a malicious file or install a malicious add-on that can compromise the browser, the device and even propagate itself into an organization's systems. Organizations can protect against these types of attacks by implementing security policies that:

- Prevent the installation of unauthorized browser extensions or add-ons.
- Only allow permitted browsers to be installed on devices.
- Block certain sites using web content filters.
- Keep browsers up to date.

Educate users

Social engineering attacks rely on the vulnerabilities of humans to cause harm. Organizations can defend against social engineering attacks by educating their staff. Users should learn how to recognize malicious content they receive or encounter, and know what to do when they spot something suspicious. For example, organizations can teach users to:

- Identify suspicious elements in a message.
- Never respond to external requests for personal information.
- Lock devices when they're not in use.
- Only store, share and remove data according to the organization's policies.

Threat intelligence

The threat landscape can be vast. Organizations might have many attack vectors that are all possible targets for cybercriminals. This means that organizations need to take as many measures as possible to monitor, prevent, defend against attacks, and even identify possible vulnerabilities before cybercriminals use them to carry out attacks. In short, they need to use threat intelligence.

Threat intelligence enables an organization to collect systems information, details about vulnerabilities, information on attacks, and more. Based on its understanding of this information, the organization can then implement policies for security, devices, user access, and more, to defend against cyberattacks. The collection of information to gain insights, and respond to cyberattacks, is known as threat intelligence.

Organizations can use technological solutions to implement threat intelligence across their systems. These are often threat intelligent solutions that can automatically collect information, and even hunt and respond to attacks and vulnerabilities.

These are just some of the mitigation strategies that organizations can take to protect against cyberattacks. Mitigation strategies enable an organization to take a robust approach to cybersecurity. This will ultimately protect the confidentiality, integrity, and availability of information.

https://docs.microsoft.com/en-us/learn/modules/describe-authentication-authorization-cybersecurity/2-define-authentication

Define authentication

Completed 100 XP

- 5 minutes

Authentication is the process of proving that a person is who they say they are. When someone purchases an item with a credit card, they may be required to show an additional form of identification. This proves that they are the person whose name appears on the card. In this example, the user may show a driver's license that serves as a form of authentication and proves their ID.

When you want to access a computer or device, you'll encounter the same type of authentication. You may get asked to enter a username and password. The username states who you are, but by itself isn't enough to grant you access. When combined with the password, which only that user should know, it allows access to your systems. The username and password are a form of authentication.

Strong authentication methods are essential to maintaining good cybersecurity and ensure that only authorized users can gain access to confidential data and resources.

While authentication will verifying the user, it doesn't govern what a user can do once they've been authenticated. Control over what a user can do is called authorization and we'll cover that later in this module.

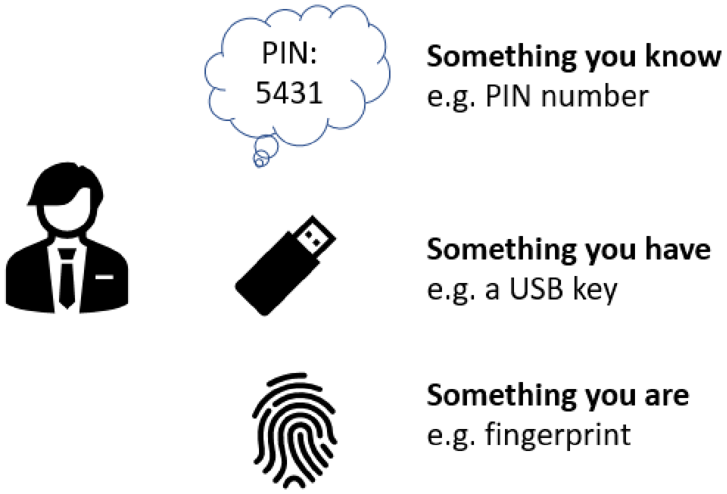
Authentication methods

Authentication can be divided into three types: *something you know*, *something you have*, and *something you are*.

- Something you **know** includes:
  - Passwords
  - PIN numbers
  - Security questions
- Something you **have** includes:
  - Identity cards
  - USB keys

    - Computers
    - Cell phones
- Something you **are** includes:
    - A fingerprint
    - Facial recognition
    - Retinal scan
    - Other forms of biometric ID.

Biometric identification is comprised of physical characteristics that uniquely identify an individual.



Types of authentication

Single-factor authentication

Single-factor authentication is a system where only one authentication type is used, making it the least secure but simplest method.

An example of a this system is when the user provides something they know, such as a password, to authenticate. Simple passwords are straightforward to remember but easy for criminals to hack. Complex passwords might seem more secure, but they'll be impossible to remember. It's more likely that someone will write down this type of password, making it much less secure.

Another single-factor authentication method is to use something you have. For example, using your cell phone to pay for an item. A tap-to-pay service authenticates the user through something that they have but doesn't require another verification method.

A biometric, something you are, can be used as a single-factor authentication method, but in some common scenarios, it's not necessarily more secure. Consider, for example, when you use a fingerprint to unlock your cell phone. You've probably known instances where the fingerprint might not be readily recognized, so you're given the option to enter a pin. This can make it easier for someone to guess. In most biometric cases, it's used in conjunction with another form of authentication.

Single-factor authentication is convenient but isn't suitable for a highly secure system.

Multifactor authentication

Multifactor authentication is a system where two, or even three, authentication types are used. By providing *something that you know, something that you have*, and *something that you are*, the system's security is massively increased. For example, in a multifactor authentication system that uses two types of authentications, you might be asked for a password, and then a number is sent to your cell phone. You input this number, proving that you know the password and have your cell phone. This is a common approach when you use multifactor authentication to access an online bank account. Multifactor authentication reduces the likelihood that a bad actor will be able to get access to confidential information.

As mentioned earlier, biometric authentication is most often used in conjunction with another method of authentication. Consider the example of a bank that has a secured area where it keeps customers' safety deposit boxes. Before someone can gain access, they're typically required to successfully enter both a password and a fingerprint scan.

Multifactor authentication is an important way users and organizations can improve security. It should be the default approach for authentication.

Describe authentication-based attacks

Completed100 XP

- 4 minutes

Authentication attacks occur when someone tries to steal another person's credentials. They can then pretend to be that person. Because an objective of these types of attacks is to impersonate a legitimate user, they can also often be referred to as identity attacks. Common attacks include, but are not limited to:

- Brute force attack
- Dictionary attack
- Credential stuffing

- Keylogging
- Social engineering

Brute force attack

In a brute force attack, a criminal will attempt to gain access simply by trying different usernames and password combinations. Typically, attackers have tools that automate this process by using millions of username and password combinations. Simple passwords, with single-factor authentication, are vulnerable to brute force attacks.

Dictionary attack

A dictionary attack is a form of brute force attack, where a dictionary of commonly used words is applied. To prevent dictionary attacks, it’s important to use symbols, numbers, and multiple word combinations in a password.

Credential stuffing

Credential stuffing is an attack method that takes advantage of the fact that many people use the same username and password across many sites. Attackers will use stolen credentials, usually obtained after a data breach on one site, to attempt to access other areas. Attackers typically use software tools to automate this process. To prevent credential stuffing, it's important not to reuse passwords, and to change them regularly, particularly after a security breach.

Keylogging

Keylogging involves malicious software that logs keystrokes. Using the key logger, an attacker can log (steal) username and password combinations, which can then be used for credential stuffing attacks. This is a common attack at internet cafes or anywhere you use a shared computer for access. To prevent keylogging, don't install untrusted software and use reputable virus-scanning software.

Keylogging isn't limited to just computers. Suppose a bad actor installs a box or device over the card reader and keypad at an ATM. When you insert your card, it passes first through the bad actors card reader - capturing the card details, before feeding it into the ATMs card reader. Now, when you key in your pin using the bad actor's keypad, they get your pin as well.

Social engineering

Social engineering involves an attempt to get people to reveal information or complete an action to enable an attack.

Most authentication attacks involve exploitation of computers or an attempt to try many credential combinations. Social engineering attacks are different in that they exploit the vulnerabilities of humans. The attacker tries to gain the trust of a legitimate user. They persuade the user to divulge information or take an action that enables them to cause damage or steal information.

A number of social engineering techniques can be used for authentication theft, including:

- **Phishing** occurs when an attacker sends a seemingly legitimate email with the objective of having a user reveal their authentication credentials. For example, an email might appear to be from the user's bank. A link opens to what looks like the bank's login page, but is actually a fake site. When a user logs in at the fake site, their credentials become available to the attacker. There are several variations of phishing, including spear-phishing, which targets specific organizations, businesses, or individuals.
- **Pretexting** is a method where an attacker gains the victim's trust and convinces them to divulge secure information. This can then be used to steal their identity. For example, a hacker might call you, pretending to be from the bank, and ask for your password to verify your identity. Another approach uses social media. You might get asked to complete a survey or a quiz, where they asked seemingly random and innocent questions that get you to reveal personal facts, or you'll get something that looks fun, like making up the name for your fantasy pop-star band by using the name of your first pet and the place you were born.
- **Baiting** is a form of attack where the criminal offers a fake reward or prize to encourage the victim to divulge secure information.

Other authentication-based attack methods

These are just a few examples of authentication-based attacks. There's always the potential for new attack types, but all of the ones listed here can be prevented by educating people and using multifactor authentication.

Describe authorization security techniques

Completed100 XP

- 6 minutes

When you authenticate a user, you'll need to decide where they can go, and what they're allowed to see and touch. This process is called authorization.

Suppose you want to spend the night in a hotel. The first thing you'll do is go to reception to start the "authentication process". After the receptionist has verified who you are, you're given a keycard and can go to your room. Think of the keycard as the authorization process. The keycard will only let you open the doors and elevators you're permitted to access, such as for your hotel room.

In cybersecurity terms, authorization determines the level of access an authenticated person has to your data and resources. There are different security techniques that organizations use to manage authorization.

Conditional access

As the name implies, conditional access involves access with conditions. One way to think about conditional access is with if/then statements. If something is true, you're granted access, but if it's false, you're denied.

Let's see how this would work in an IT scenario. Increasingly, people are working from home. Because of this, they might be using their personal computer to access work-related content. With conditional access, an organization might grant access for an authenticated user to a confidential system, such as payroll, only if it's made through secure corporate computers located at their headquarters. If the authenticated user tries to access the payroll system from a personal computer at home, they would be blocked.

Least privileged access

The concept of least privilege is where a user is granted the minimum rights that they require. This concept applies in any security-related setting.

For example, when you board an airplane, you have access to the main cabin area to get to your seat, but no passenger is allowed in to the cockpit. Also, if you're traveling with a coach-class ticket, you will only have access to that section. To improve security, each person can only access the areas they need to.

The same concept applies in the context of cybersecurity. Take the example where users have access to a public folder on a network. If they only need to read a file, they should be given that specific permission.

A user will almost always notify an administrator if they have insufficient rights to perform their role. However, they will seldom tell an administrator if they have excess rights. So there's little risk of being over cautious when assigning user rights.

By implementing the least privileged access, you will reduce an attacker's actions if a breach occurs.

Lateral movement

If an attacker gains access to a system, they might use the compromised account to gather more information. This could be used to infiltrate other systems or gain elevated access. The attacker can move through the system, finding more resources until their target is reached. Because the attacker will attempt to move between different sections, the final attack is unlikely to come from the initial compromised account.

Think of an office building where a criminal gets past the security of the main reception area. They can then generally move around the rest of the building, accessing different floors and offices. It's important to provide added layers of security to protect against intrusion in sensitive areas.

For example, many office buildings require a security code to access the floors where the executive team is located. All offices on those floors are kept locked, allowing access only by employees with a special card. You clearly don’t want a criminal to access your building at all. But by assuming a breach might occur and adding additional layers of security to protect against this type of lateral movement, you can limit the damage.

The same concept applies in an IT scenario. You start with secure authentication to reduce the chance of an attacker accessing your systems. No system is foolproof but you can provide added layers of security. These measures will help mitigate the chance that an attacker who breaks into your system can access other more sensitive resources through lateral movement.

Zero Trust

Zero Trust is a term that's prevalent in cybersecurity. It's a method that mitigates the increasingly common attacks that we see today.

Zero Trust is a model that enables organizations to provide secure access to their resources by teaching us to “never trust, always verify”. It's based on three principles that employ concepts you're already familiar with.

- **Verify explicitly** - With Zero Trust, every request is fully authenticated and authorized before any access is granted. Organizations may implement both multifactor authentication and conditional access to ensure that every request is verified explicitly.
- **Use least privileged access** - as mentioned earlier in this unit, the concept of least privilege is to only authorize a user with the minimum rights that they require. This limits the damage that a user can do and limits lateral flows.
- **Assume breach** - By assuming that a breach has or will occur, an organization can better plan for additional layers of security. This minimizes an attacker’s radius for breaches and prevents lateral movement.

By employing a Zero Trust security model, organizations can better adapt to a modern distributed workplace that provides secure access to resources.

Learn more:
https://docs.microsoft.com/en-us/learn/paths/describe-basic-concepts-of-cybersecurity/