INTRODUCTION TO CYBERSECURITY

What is Cybersecurity?!

Cybersecurity is the ongoing effort to protect individuals, organizations and governments from digital attacks by protecting networked systems and data from unauthorized use or harm.

- **Personal:** On a personal level, you need to safeguard your identity, your data, and your computing devices.
    - ✓ ***Offline identity:*** Your offline identity is the real-life persona that you present on a daily basis at home, at school or at work. As a result, family and friends know details.
    - ✓ ***Online identity:*** Your online identity is not just a name. it includes the username or alias you use for your online accounts, as well as the social identity you establish and portray on online communication and websites. You sure know how to keep your online identity safe. When choosing a username, it's important not to reveal any personal information. It should be something appropriate and respectful and should not lead strangers to think you are an easy target for cybercrimes or unwanted attention.
        - Don't use your full name or parts of your address or phone number.
        - Don't use your email username.
        - Don't use the same username and password combination, especially on financial accounts.
        - Don't choose a super-odd username and then reuse it again and again — it makes you easier to track.
        - Don't choose a username that gives clues to your passwords such as a series of numbers/letters or the first part of a two-part phrase, such as knock-knock or starlight, or the department in which you work, such as IT.
        - Do choose a username that's appropriate for the type of account, i.e., business, social or personal.

    "Many people think that if they don't have any social media or online accounts set up, then they don't have an online identity. This is not the case. If you use the web, you have an online identity."

- **Organizational:** At an organizational level, it is everyone's responsibility to protect the organization's reputation, data and customers
- **Government:** As more digital information is being gathered and shared, its protection becomes even more vital at the government level, where national security, economic stability and the safety and wellbeing of citizens are at stake.

Your data

Personal data describes any information about you, including your name, social security number, driver license number, date and place of birth, your mother's maiden name, and even pictures or messages that you exchange with family and friends.

Cybercriminals can use this sensitive information to identify and impersonate you, infringing on your privacy and potentially causing serious damage to your reputation.

i. ***Medical records:*** Every time you visit the doctor, personal information regarding your physical and mental health and wellbeing is added to your electronic health records (EHRs). Since the majority of these records are saved online, you need to be aware of the medical information that you share.
ii. ***Education records:*** Educational records contain information about your academic qualifications and achievements. However, these records may also include your contact information, attendance records, disciplinary reports, health and immunization records as well as any special education records including individualized education programs
iii. ***Employment and financial records***: Employment data can be valuable to hackers if they can gather information on your past employment, or even your current performance reviews. Your financial records may include information about your income and expenditure. Your tax records may include

Aside from Hackers, who else want my data?

a) **Your ISP (Internet service provider):** Your ISP tracks your online activity and, in some countries, they can sell this data to advertisers for a profit. In certain circumstances, ISPs may be legally required to share your information with government surveillance agencies or authorities.
b) **Advertisers:** Targeted advertising is part of the Internet experience. Advertisers monitor and track your online activities such as shopping habits and personal preferences and send targeted ads your way.
c) **Search engine and social media platforms:** These platforms gather information about your gender, geolocation, phone number and political and religious ideologies based on your search histories and online identity. This information is then sold to advertisers for a profit.
d) **Websites you visit:** Websites use cookies to track your activities in order to provide a more personalized experience. But this leaves a data trail that is linked to your online identity that can often end up in the hands of advertisers!

Organizational Data

Organizational Data refers to structured information that describes the structure, operations, and resources of a business or institution. This includes data about departments, employees, roles, processes, and business units, and it supports decision-making and operational efficiency.

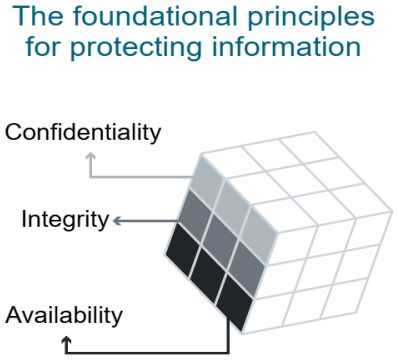
Type of Organizational Data

1. **Traditional data:** Traditional data is typically generated and maintained by all organizations, big and small. It includes the following:
    i. **Transactional data** such as details relating to buying and selling, production activities and basic organizational operations such as any information used to make employment decisions.
    ii. **Intellectual property** such as patents, trademarks and new product plans, which allows an organization to gain economic advantage over its competitors. This information is often considered a trade secret and losing it could prove disastrous for the future of a company.
    iii. **Financial data** such as income statements, balance sheets and cash flow statements, which provide insight into the health of a company.
2. **Internet of Things (IoT) and Big Data:** IoT is a large network of physical objects, such as sensors, software and other equipment. All of these ‘things’ are connected to the Internet, with the ability to collect and share data. And given that storage options are expanding through the cloud and virtualization, it’s no surprise that the emergence of IoT has led to an exponential growth in data, creating a new area of interest in technology and business called 'Big Data.'

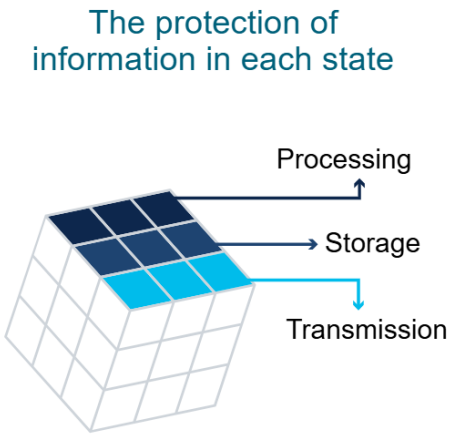
The cube

The McCumber Cube is a model framework created by John McCumber in 1991 to help organizations establish and evaluate information security initiatives by considering all of the related factors that impact them. This security model has three dimensions:

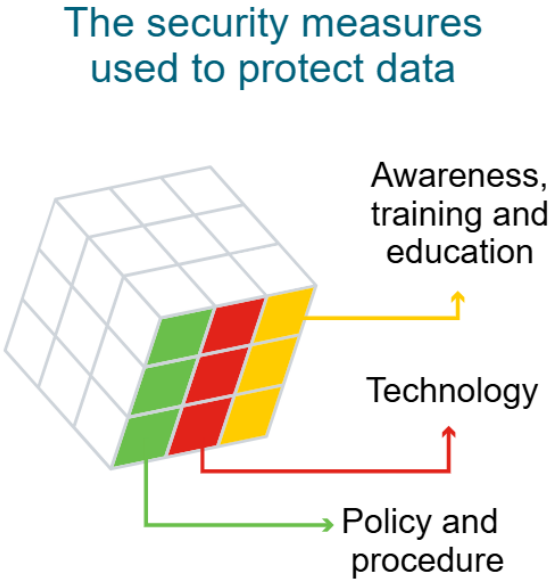
1. The foundational principles for protecting information systems.
2. The protection of information in each of its possible states.
3. The security measures used to protect data.



- **C - Confidentiality:** is a set of rules that prevents sensitive information from being disclosed to unauthorized people, resources and processes. Methods to ensure confidentiality include **data encryption**, **identity proofing** and **two factor authentication**.
- **I - Integrity** ensures that system information or processes are protected from intentional or accidental modification. One way to ensure integrity is to use a **hash function** or **checksum**.
- **A - Availability** means that authorized users are able to access systems and data when and where needed and those that do not meet established conditions are not. This can be achieved by **maintaining equipment**, **performing hardware repairs**, **keeping operating systems and software up to date** and **creating backups**.



- **Processing:** refers to data that is being used to perform an operation such as updating a database record (data in process).
- **Storage:** refers to data stored in memory or on a permanent storage device such as a hard drive, solid-state drive or USB drive (data at rest).
- **Transmission:** refers to data traveling between information systems (data in transit).



- **Awareness, training and education:** are the measures put in place by an organization to ensure that users are knowledgeable about potential security threats and the actions they can take to protect information systems.
- **Technology:** refers to the software- and hardware-based solutions designed to protect information systems such as firewalls, which continuously monitor your network in search of possible malicious incidents.
- **Policy and procedure:** refers to the administrative controls that provide a foundation for how an organization implements information assurance, such as incident response plans and best practice guidelines.

Consequences of a Security Breach

1. **Reputational damage:** A security breach can have a negative long-term impact on an organization's reputation that has taken years to build. Customers, particularly those who have been adversely affected by the breach, will need to be notified and may seek compensation and/or turn to a reliable and secure competitor. Employees may also choose to leave in light of a scandal. Depending on the severity of a breach, it can take a long time to repair an organization's reputation.
2. **Vandalism:** A hacker or hacking group may vandalize an organization's website by posting untrue information. They might even just make a few minor edits to your organization's phone number or address, which can be trickier to detect. In either case, online vandalism can portray unprofessionalism and have a negative impact on your organization's reputation and credibility.
3. **Theft:** A data breach often involves an incident where sensitive personal data has been stolen. Cybercriminals can make this information public or exploit it to steal an individual's money and/or identity.
4. **Loss of revenue:** The financial impact of a security breach can be devastating. For example, hackers can take down an organization's website, preventing it from doing business online. A loss of customer information may impede company growth and expansion. It may demand further investment in an organization's security infrastructure. And let's not forget that organizations may face large fines or penalties if they do not protect online data.
5. **Damaged intellectual property:** A security breach could also have a devastating impact on the competitiveness of an organization, particularly if hackers are able to get their hands on confidential documents, trade secrets and intellectual property.

Cyber attackers

Attackers are individuals or groups who attempt to exploit vulnerability for personal or financial gain. As we've already seen, they are interested in **everything**, from credit cards to product designs!

Types of attackers

Let's look at some of the main types of cyber attackers who'll try anything to get their hands on our information. They are often categorized as **white hat, gray hat** or **black hat** attackers. Let's take a look example

- After hacking into ATM systems remotely using a laptop, this attacker worked with the ATM manufacturers to resolve the identified security vulnerabilities. - **gray hat**
- This attacker transferred $10 million into their bank account using customer account and PIN credentials gathered from recordings. - **black hat**
- This attacker's job is to identify weaknesses in a company's computer system. - **white hat**

Internal and external threats: Cyber attacks can originate from within an organization as well as from outside of it.

- **Internal Threats:** Risks from inside the organization, like employees or contractors who may misuse access, steal data, or cause damage intentionally or accidentally using devices like company computers, USB drives, or smartphones.
- **External Threats:** Risks from outside, such as hackers or malware that exploit vulnerabilities to steal data, disrupt systems, or gain unauthorized access using tools like laptops, phishing emails, or malicious software.

Analyzing a cyber attack

Types of malware

Cybercriminals use many different types of malicious software, or malware, to carry out their activities. Malware is any code that can be used to steal data, bypass access controls, or cause harm to or compromise a system. Knowing what the different types are and how they spread is key to containing and removing them.

1. **Spyware:** Designed to track and spy on you, spyware monitors your online activity and can log every key you press on your keyboard, as well as capture almost any of your data, including sensitive personal information such as your online banking details. Spyware does this by modifying the security settings on your devices. It often bundles itself with legitimate software or Trojan horses.
2. **Adware:** Adware is often installed with some versions of software and is designed to automatically deliver advertisements to a user, most often on a web browser. You know it when you see it! It's hard to ignore when you're faced with constant pop-up ads on your screen. It is common for adware to come with spyware.

3. **Backdoor:** This type of malware is used to gain unauthorized access by bypassing the normal authentication procedures to access a system. As a result, hackers can gain remote access to resources within an application and issue remote system commands. A backdoor works in the background and is difficult to detect.
4. **Ransomware:** This malware is designed to hold a computer system or the data it contains captive until a payment is made. Ransomware usually works by encrypting your data so that you can't access it. Some versions of ransomware can take advantage of specific system vulnerabilities to lock it down. Ransomware is often spread through phishing emails that encourage you to download a malicious attachment or through software vulnerability.
5. **Scareware:** This is a type of malware that uses 'scare' tactics to trick you into taking a specific action. Scareware mainly consists of operating system style windows that pop up to warn you that your system is at risk and needs to run a specific program for it to return to normal operation. If you agree to execute the specific program, your system will become infected with malware.
6. **Rootkit**: This malware is designed to modify the operating system to create a backdoor, which attackers can then use to access your computer remotely. Most rootkits take advantage of software vulnerabilities to gain access to resources that normally shouldn't be accessible (privilege escalation) and modify system files. Rootkits can also modify system forensics and monitoring tools, making them very hard to detect. In most cases, a computer infected by a rootkit has to be wiped and any required software reinstalled.
7. **Virus:** A virus is a type of computer program that, when executed, replicates and attaches itself to other executable files, such as a document, by inserting its own code. Most viruses require end-user interaction to initiate activation and can be written to act on a specific date or time. Viruses can be relatively harmless, such as those that display a funny image. Or they can be destructive, such as those that modify or delete data. Viruses can also be programmed to mutate in order to avoid detection. Most viruses are spread by USB drives, optical disks, network shares or email.
8. **Trojan horse:** This malware carries out malicious operations by masking its true intent. It might appear legitimate but is, in fact, very dangerous. Trojans exploit your user privileges and are most often found in image files, audio files or games. Unlike viruses, Trojans do not self-replicate but act as a decoy to sneak malicious software past unsuspecting users.
9. **Worms:** This is a type of malware that replicates itself in order to spread from one computer to another. Unlike a virus, which requires a host program to run, worms can run by themselves. Other than the initial infection of the host, they do not require user participation and can spread very quickly over the network. Worms share similar patterns: They exploit system vulnerabilities, they have a way to propagate themselves, and they all contain malicious code (payload) to cause damage to computer systems or networks. Worms are responsible for some of the most devastating attacks on the Internet. In 2001, the Code Red worm had infected over 300,000 servers in just 19 hours.

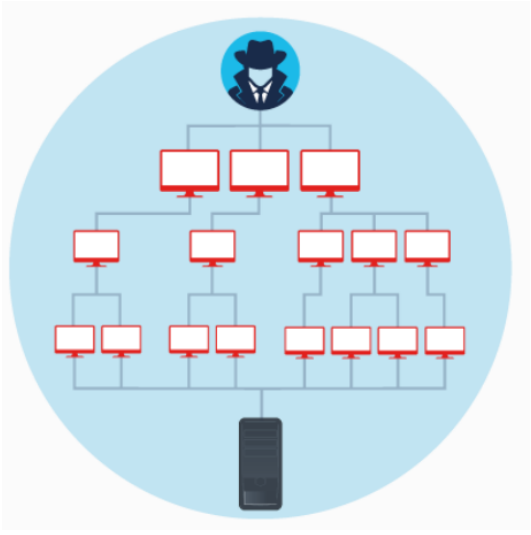
Symptoms of Malware:

- **Slow computer performance:** Malware uses system resources, making your device sluggish.
- **Increasing CPU usage:** Malware runs hidden processes that overload the processor.
- **Frequent crashes or freezes:** Malicious code can cause instability.
- **Unexpected pop-up ads:** Often caused by adware injecting unwanted ads.
- **Programs opening or closing automatically:** Malware may control software without your input.
- **Unusual network activity:** Malware can send or receive data secretly.
- **Disabled antivirus or security software:** Some malware tries to avoid detection by turning off protections.
- **Files missing or corrupted:** Malware may delete or damage files.
- **Strange emails sent from your account:** Malware can hijack your email to spread itself or scams.

Methods of Infiltration: Methods of Infiltration are ways malware or attackers enter a system.

a) **Social engineering:** Social engineering is the manipulation of people into performing actions or divulging confidential information. Social engineers often rely on people's willingness to be helpful, but they also prey on their weaknesses. For example, an attacker will call an authorized employee with an urgent problem that requires immediate network access and appeal to the employee's vanity or greed or invoke authority by using name-dropping techniques in order to gain this access.

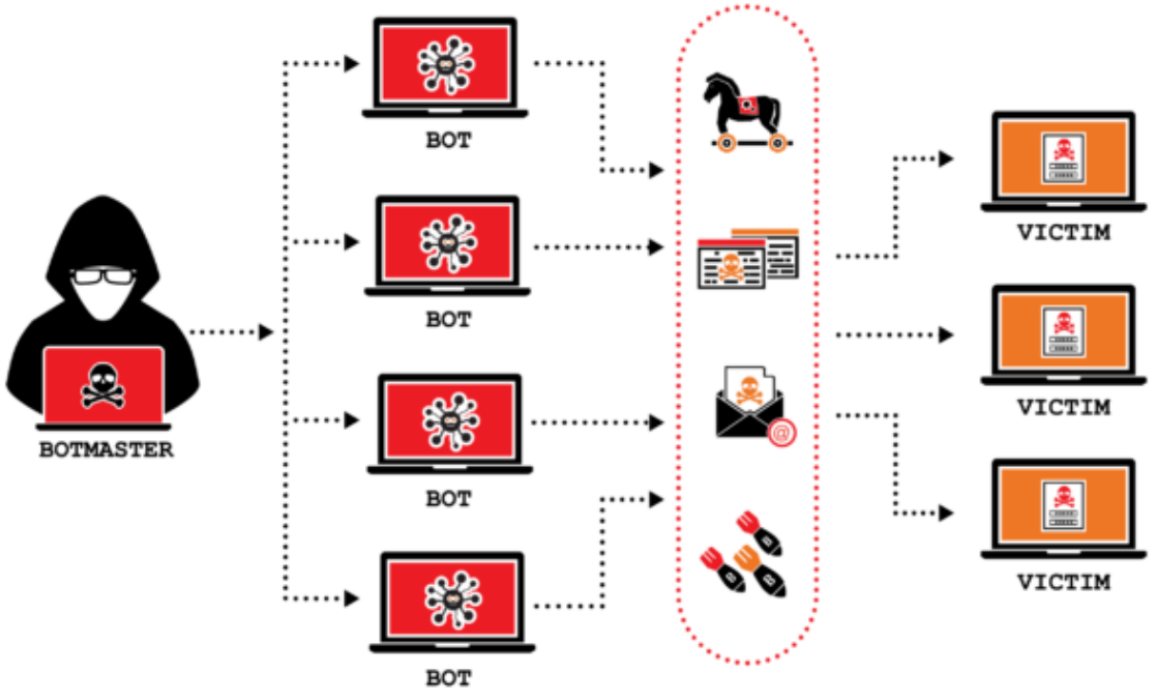
b) **Denial-of-Service (DoS):** DoS attacks are network attacks that disrupt service to users, devices, or applications. They are simple enough for even unskilled attackers to perform. DoS attacks are considered a major risk because they can easily interrupt communication and cause significant loss of time and money.



DoS: Attack from one device to disrupt service.

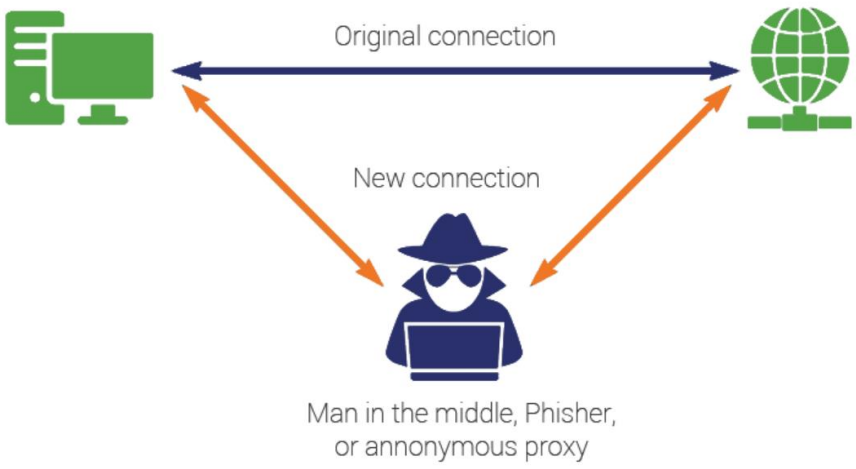
c) **Distributed DoS (DDoS):** A Distributed DoS (DDoS) attack is similar to a DoS attack but originates from multiple, coordinated sources. For example:

- ✓ An attacker builds a network (botnet) of infected hosts called zombies, which are controlled by handler systems.
- ✓ The zombie computers will constantly scan and infect more hosts, creating more and more zombies.
- ✓ When ready, the hacker will instruct the handler systems to make the botnet of zombies carry out a DDoS attack.

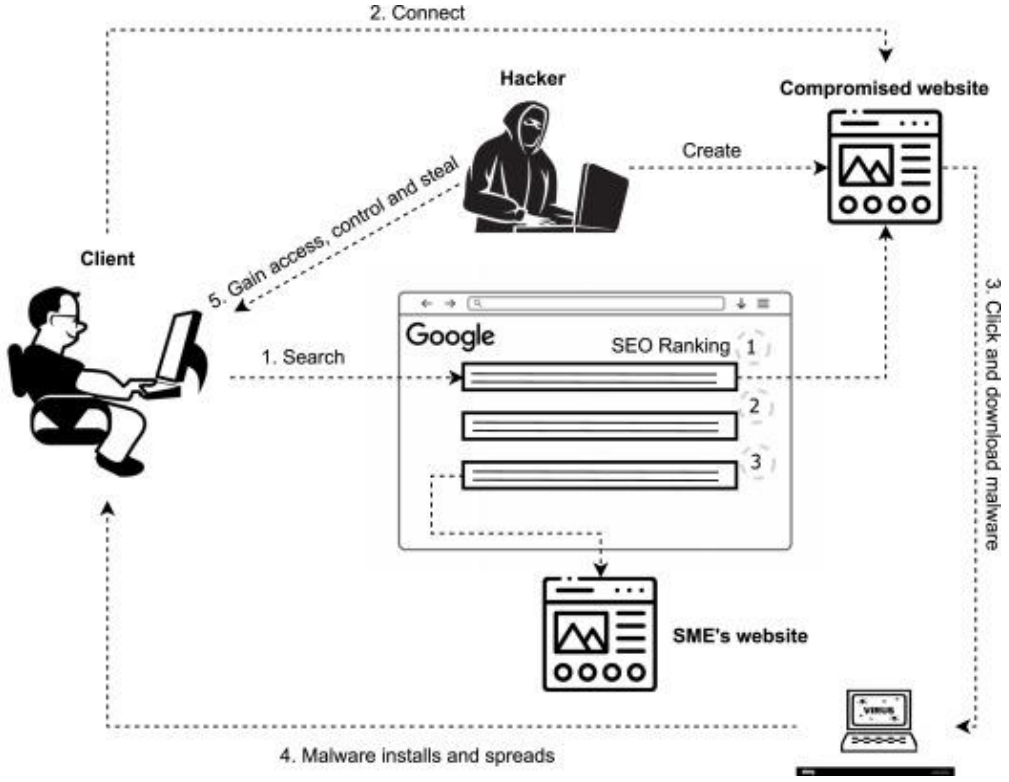


DDoS: Attack from many devices simultaneously to overwhelm service.

d) **Man-in-the-middle:** On-path attackers intercept or modify communications between two devices, such as a web browser and a web server, either to collect information from or to impersonate one of the devices.



e) **SEO poisoning:** You've probably heard of search engine optimization or SEO which, in simple terms, is about improving an organization's website so that it gains greater visibility in search engine results.



f) **Wi-Fi password cracking:** Wi-Fi password cracking is a method used to gain unauthorized access to a wireless network by guessing or decrypting its password. Attackers use tools to capture network data and analyze it to find the password. Common techniques include brute force, dictionary attacks, and exploiting weak encryption Once the password is cracked, attackers can intercept data, use the internet connection, or launch further attacks. Strong passwords and encryption help prevent this.

g) **Password attack:** Entering a username and password is one of the most popular forms of authenticating to a web site. Therefore, uncovering your password is an easy way for cybercriminals to gain access to your most valuable information.

   i. **Password spraying:** This technique attempts to gain access to a system by 'spraying' a few commonly used passwords across a large number of accounts. For example, a cybercriminal uses 'Password123' with many usernames before trying again with a second commonly-used password, such as 'qwerty.' This technique allows the perpetrator to remain undetected as they avoid frequent account lockouts.

   ii. **Dictionary attack:** A hacker systematically tries every word in a dictionary or a list of commonly used words as a password in an attempt to break into a password-protected account.

iii. **Brute-force attacks:** The simplest and most commonly used way of gaining access to a password-protected site, brute-force attacks see an attacker using all possible combinations of letters, numbers and symbols in the password space until they get it right.

iv. **Rainbow attacks:** Passwords in a computer system are not stored as plain text, but as hashed values (numerical values that uniquely identify data). A rainbow table is a large dictionary of precomputed hashes and the passwords from which they were calculated. Unlike a brute-force attack that has to calculate each hash, a rainbow attack compares the hash of a password with those stored in the rainbow table. When an attacker finds a match, they identify the password used to create the hash.

v. **Traffic interception:** Plain text or unencrypted passwords can be easily read by other humans and machines by intercepting communications. If you store a password in clear, readable text, anyone who has access to your account or device, whether authorized or unauthorized, can read it.

Security Vulnerability and Exploits

- **Hardware vulnerabilities:** Hardware vulnerabilities are most often the result of hardware design flaws. For example, the type of memory called RAM basically consists of lots of capacitors (a component which can hold an electrical charge) installed very close to one another. However, it was soon discovered that, due to their close proximity, changes applied to one of these capacitors could influence neighbor capacitors. Based on this design flaw, an exploit called Rowhammer was created. By repeatedly accessing (hammering) a row of memory, the Rowhammer exploit triggers electrical interferences that eventually corrupt the data stored inside the RAM. Hardware vulnerabilities are specific to device models and are not generally exploited through random compromising attempts. While hardware exploits are more common in highly targeted attacks, traditional malware protection and good physical security are sufficient protection for the everyday user.

- **Software vulnerabilities:** Software vulnerabilities are usually introduced by errors in the operating system or application code. Categorizing Software Vulnerabilities

  i. **Buffer overflow:** Buffers are memory areas allocated to an application. Vulnerability occurs when data is written beyond the limits of a buffer. By changing data beyond the boundaries of a buffer, the application can access memory allocated to other processes. This can lead to a system crash or data compromise, or provide escalation of privileges.

ii. **Non-validated input:** Programs often require data input, but this incoming data could have malicious content, designed to force the program to behave in an unintended way. For example, consider a program that receives an image for processing. A malicious user could craft an image file with invalid image dimensions. The maliciously crafted dimensions could force the program to allocate buffers of incorrect and unexpected sizes.

iii. **Race conditions:** This vulnerability describes a situation where the output of an event depends on ordered or timed outputs. A race condition becomes a source of vulnerability when the required ordered or timed events do not occur in the correct order or at the proper time.

iv. **Weaknesses in security practices:** Systems and sensitive data can be protected through techniques such as authentication, authorization and encryption. Developers should stick to using security techniques and libraries that have already been created, tested and verified and should not attempt to create their own security algorithms. These will only likely introduce new vulnerabilities.

v. **Access control problem:** Access control is the process of controlling who does what and ranges from managing physical access to equipment to dictating who has access to a resource, such as a file, and what they can do with it, such as read or change the file. Many security vulnerabilities are created by the improper use of access controls. Nearly all access controls and security practices can be overcome if an attacker has physical access to target equipment. For example, no matter the permission settings on a file, a hacker can bypass the operating system and read the data directly off the disk. Therefore, to protect the machine and the data it contains, physical access must be restricted, and encryption techniques must be used to protect data from being stolen or corrupted.

- **Software updates:** The goal of software updates is to stay current and avoid exploitation of vulnerabilities. Microsoft, Apple and other operating system producers release patches and updates almost every day and applications such as web browsers, mobile apps and web servers are often updated by the companies or organizations responsible for them.

  Despite the fact that organizations put a lot of effort into finding and patching software vulnerabilities, new vulnerabilities are discovered regularly. That's why some organizations use third party security researchers who specialize in finding vulnerabilities in software, or actually invest in their own penetration testing teams dedicated to search, find and patch software vulnerabilities before they can get exploited.

  Google's Project Zero is a great example of this practice. After discovering a number of vulnerabilities in various software used by end users, Google formed a permanent team dedicated to finding software vulnerabilities. You can find out more about Google's security research https://project-zero.issues.chromium.org/issues?q=status:open

The Cybersecurity Landscape

- **Cryptocurrency**: Cryptocurrency is digital money that can be used to buy goods and services, using strong encryption techniques to secure online transactions. Banks, governments and even companies like Microsoft and AT&T are very aware of its importance and are jumping on the cryptocurrency bandwagon!

    - ✓ Cryptocurrency owners keep their money in encrypted, virtual 'wallets.' When a transaction takes place between the owners of two digital wallets, the details are recorded in a decentralized, electronic ledger or blockchain system. This means it is carried out with a degree of anonymity and is self-managed, with no interference from third parties such as central banks or government
    - ✓ Approximately every ten minutes, special computers collect data about the latest cryptocurrency transactions, turning them into mathematical puzzles to maintain confidentiality. These transactions are then verified through a technical and highly complex process known as 'mining.' This step typically involves an army of 'miners' working on high-end PCs to solve mathematical puzzles and authenticate transactions.
    - ✓ Once verified, the ledger is updated and electronically copied and disseminated worldwide to anyone belonging to the blockchain network, effectively completing a transaction.

- **Cryptojacking:** Cryptojacking is an emerging threat that hides on a user's computer, mobile phone, tablet, laptop or server, using that machine's resources to 'mine' cryptocurrencies without the user's consent or knowledge. Many victims of cryptojacking didn't even know they'd been hacked until it was too late!

Protecting Your Devices and Network

You've probably heard of the term 'online security.' It's all about taking the necessary steps to prevent your personal information from falling into the wrong hands.

- **Protecting your computing devices:** Your computing devices are the portal to your online life, storing a lot of your personal data. Therefore, it's important to protect the security of your devices.

    i. **Turn the firewall on:** You should use at least one type of firewall (either a software firewall or a hardware firewall on a router) to protect your device from unauthorized access. The firewall should be turned on and constantly updated to prevent hackers from accessing your personal or organization data. You can click this link https://support.microsoft.com/en-us/windows/firewall-and-network-protection-in-the-windows-security-app-ec0844f7-aebd-0583-67fe-601ecf5d774f

to learn how to turn on the firewall in Windows 10, or click this link https://support.apple.com/en-ke/guide/mac-help/mh34041/mac for Mac OS X devices.

ii. **Install antivirus and antispyware:** Malicious software, such as viruses and spyware, are designed to gain unauthorized access to your computer and your data. Once installed, viruses can destroy your data and slow down your computer. They can even take over your computer and broadcast spam emails using your account. Spyware can monitor your online activities, collect your personal information or produce unwanted pop-up ads on your web browser while you are online. To prevent this, you should only ever download software from trusted websites. However, you should always use antivirus software to provide another layer of protection. This software, which often includes antispyware, is designed to scan your computer and incoming email for viruses and delete them. Keeping your software up to date will protect your computer from any new malicious software that emerges.

iii. **Manage your operating system and browser:** Hackers are always trying to take advantage of vulnerabilities that may exist in your operating system (such as Microsoft Windows or macOS) or web browser (such as Google Chrome or Apple Safari). Therefore, to protect your computer and your data, you should set the security settings on your computer and browser to medium level or higher. You should also regularly update your computer's operating system, including your web browser, and download and install the latest software patches and security updates from the vendors.

iv. **Set up password protection:** All of your computing devices, including PCs, laptops, tablets and smartphones, should be password protected to prevent unauthorized access. Any stored information, especially sensitive or confidential data, should be encrypted. You should only store necessary information on your mobile device, in case it is stolen or lost. Remember, if any one of your devices is compromised, the criminals may be able to access all of your data through your cloud storage service provider, such as iCloud or Google Drive.

"IoT devices pose an even greater risk than your other computing devices. While desktop, laptop and mobile platforms receive frequent software updates, most IoT devices have their original software. If vulnerabilities are found in the software, the IoT device is likely to be vulnerable. And to make the problem worse, IoT devices require Internet access, most often relying on your local network. The result is that when IoT devices are compromised, they allow hackers access to your local network and data. The best way to protect yourself from this scenario is to set up any IoT devices on an isolated network.

Check out https://www.shodan.io/, a web-based IoT device scanner that helps you identify any vulnerable devices on the Internet. "

Wireless Network Security at Home

Wireless networks allow Wi-Fi enabled devices, such as laptops and tablets, to connect to the network by way of a preset network identifier, known as the service set identifier (SSID). Although a wireless router can be configured so that it doesn't broadcast the SSID, this should not be considered adequate security for a wireless network.

Hackers will be aware of the preset SSID and default password. Therefore, these details should be changed to prevent intruders from entering your home wireless network. Furthermore, you should encrypt wireless communication by enabling wireless security and the WPA2 encryption feature on your wireless router. But be aware, even with WPA2 encryption enabled, a wireless network can still be vulnerable.

Public Wi-Fi Risks

When you are away from home, you can access your online information and surf the Internet via public wireless networks or Wi-Fi hotspots. However, there are some risks involved, which mean that it is best not to access or send any personal information when using public Wi-Fi.

You should always verify that your device isn't configured with file and media sharing and that it requires user authentication with encryption.

You should also use an encrypted VPN service to prevent others from intercepting your information (known as 'eavesdropping') over a public wireless network. This service gives you secure access to the Internet, by encrypting the connection between your device and the VPN server. Even if hackers intercept a data transmission in an encrypted VPN tunnel, they will not be able to decipher it.

Click here https://www.fcc.gov/consumers/guides/how-protect-yourself-online to find out more about protecting yourself when using wireless networks.

"Don't forget that the Bluetooth wireless protocol, found on many smartphones and tablets, can also be exploited by hackers to eavesdrop, establish remote access controls, distribute malware and drain batteries! Therefore, my top tip is to keep Bluetooth turned off when you aren't using it."

Password Security

You've logged into your new laptop and it has prompted you to change your network password. You already struggle to remember the few passwords you use for your personal accounts online.

You ask one of your colleagues for their advice. They tell you to use one of the passwords you use for your personal accounts — that are what they do! They keep their personal passwords written down at the back of their diary, just in case they forget them.

How would you rate your colleague's attitude to password security on a scale of 1 (bad practice) to 5 (good practice)? 1 – ***Bad practice***

Strong Password Tips with Examples:

- Use at least 12 characters (e.g., Tg7!xLp9@wQ2)
- Mix uppercase and lowercase letters (e.g., PaSsWoRd123!)
- Include numbers and special symbols (e.g., Summer2025#)
- Avoid common words or phrases (avoid password123)
- Don't use easily guessable info like birthdays (avoid John1985)
- Use unique passwords for different accounts
- Consider using a password manager (e.g., LastPass, 1Password)

Click here https://pages.nist.gov/800-63-3/ to find out more about these NIST password requirements.

Data maintenance

Data Maintenance refers to the ongoing process of managing and updating data to ensure its accuracy, consistency, and reliability. It involves tasks like correcting errors, removing duplicates, backing up data, and updating records to keep information current and useful for decision-making.

Encryption

Encryption is the process of converting information into a form in which unauthorized parties cannot read it. Only a trusted, authorized person with the secret key or password can decrypt the data and access it in its original form. Note that the encryption itself does not prevent someone from intercepting the data. It can only prevent an unauthorized person from viewing or accessing the content. In fact, some criminals may decide to simply encrypt your data and make it unusable until you pay a ransom.

How Do You Encrypt Your Data?

Software programs are used to encrypt files, folders, and even entire drives. Encrypting File System (EFS) is a Windows feature that can encrypt data. It is directly linked to a specific user account, and only the user who encrypts the data will be able to access it after it has been encrypted using EFS.

Encrypt data using EFS in all Windows versions.

i. Step 1: Select one or more files or folders.
ii. Step 2: Right click the selected data and go to '**Properties**.'
iii. Step 3: Find and click '**Advanced**.'
iv. Step 4: Select the '**Encrypt contents to secure data**' check box.
v. Step 5: Files and folders that have been encrypted with EFS are displayed in green as shown here.

Backup up your data

Having a backup may prevent the loss of irreplaceable data. To back up data properly, you will need an additional storage location for the data and you must copy the data to that location regularly.

- Home network: Storing your data locally means that you have total control of it.
- Secondary location: You could copy all of your data to a network attached storage device (NAS), a simple external hard drive or maybe even back up important folders on thumb drives, CDs, DVDs or tapes. In this scenario, you are the owner of the data and you are totally responsible for the cost and maintenance of the storage device equipment.
- The cloud: You could subscribe to a cloud storage service, like Amazon Web Services (AWS). The cost of this service will depend on the amount of storage space you need, so you may need to be more selective about what data you back up. You will have access to your backup data as long as you have access to your account. One of the benefits of using a cloud storage service is that your data is safe in the event of a storage device failure or if you experience an extreme situation such as a fire or theft.

How Do You Delete Your Data Permanently?

Have you ever had to delete data or get rid of a hard drive? If so, did you take any precautions to safeguard the data to keep it from falling into the wrong hands? To ensure you delete your files securely and permanently.

- To erase data so that if is no longer recoverable, it must be overwritten with ones and zeroes, using tools specifically designed to do just that. **SDelete** from Microsoft claims to have the ability to remove sensitive files completely. **Shred** from Linux and secure empty trash for Mac OS X claims to provide a similar service.
- The only way to be certain that data or files are not recoverable is to physically destroy the hard drive or storage device. Have criminals have taken advantage of files through to be impenetrable or irrecoverable.

"Don't forget about data that may be stored online in the cloud. These copies will also need to be deleted."

Before You Sign Up: What factors should you consider before you sign up to an online service?

1. Have you read the terms of service?
2. What are your rights regarding your data?
3. Can you request a copy of your data?
4. What can the provider do with the data you upload?
5. What happens to your data when you close your account?

Safeguarding Your Online Privacy

Two factor authentication

Popular online services, such as Google, Facebook, Twitter, LinkedIn, Apple and Microsoft, use two factor authentications to add an extra layer of security for account logins. Besides your username and password or personal identification number (PIN), two factor authentications requires a second token to verify your identity. This may be a:

- physical object such as a credit card, mobile phone or fob
- biometric scan such as a fingerprint or facial and voice recognition
- Verification code sent via SMS or email.

Click here https://brainstation.io/cybersecurity/two-factor-auth to find out more about two factor authentications.

"Be careful! Even with two factor authentication, hackers can still gain access to online accounts through phishing attacks, malware and social engineering."

Open authorization

Open authorization (OAuth) is an open standard protocol that allows you to use your credentials to access third-party applications without exposing your password this mean Instead of having to reset your login details, you log into the eLearning portal using your existing social media accounts and register for your next course with ease. You can't wait to get started!

"The Internet is a great tool for not only accessing information quickly and easily but also for communicating with friends, family and colleagues. But did you know that anyone with physical access to your device or router can view what websites you've visited? And that every time you send an email, it is readable by anyone who has access to the digital chain between you and your recipient?"

Email and web browser privacy

These problems can be minimized by enabling the in-private browsing mode on your web browser. Many of the most commonly used web browsers have their own name for private browser mode:

- **Microsoft Internet Explorer**: InPrivate
- **Google Chrome**: Incognito
- **Mozilla Firefox**: Private tab or private window
- **Safari**: Private browsing

"When private mode is enabled, cookies – files saved to your device to indicate what websites you've visited – are disabled. Therefore, any temporary internet files and removed and your browsing history is deleted when you close the window or program. This may help to prevent others from gathering information about your online activities and trying to entice your to buy something with targeted ads. Even with private browsing enabled and cookies disabled, companies are constantly developing new ways of fingerprinting users in order to track their online behavior. For example, some intermediary devices like routers, can gather information about a user's web surfing history"

Cybersecurity Devices and Technologies

There is no single security appliance or piece of technology that will solve all the network security needs in an organization. You must consider what tools will be most effective as part of your security system.

Security appliances

Security appliances can be standalone devices like a router or software tools that are run on a network device. They fall into six general categories.

- **Routers:** while routers are primarily used to interconnect various network segments together, they usually also provide basic traffic filtering capabilities. This information can help you define which computer from a given network segments can communicate with network segments.
- **Firewalls:** firewalls can look deeper into network traffic itself and identify malicious behavior that has to be blocked. Firewalls can have sophisticated security policies applied to the traffic that is passing through them.
- **Intrusion prevention systems (IPS):** An IPS system uses a set of traffic signatures that match and block malicious traffic and attacks.
- **Virtual private networks (VPN):** VPN systems let remote employees use a secure encrypted tunnel from their mobile computer and securely connect back to the organization's network. VPN systems can also securely interconnect branch offices with the central office network.

- **Antimalware or antivirus:** These systems use signature or behavioral analysis of applications to identify and block malicious code from being executed.
- **Other security devices:** other security devices include web and email security appliances, decryption devices, client access control servers and security management systems

Firewalls

In computer networking, a firewall is designed to control or filter which communications are allowed in and which are allowed out of a device or network. A firewall can be installed on a single computer with the purpose of protecting that one computer (host-based firewall) or it can be a standalone network device that protects an entire network of computers and all of the host devices on that network (network-based firewall).

As computer and network attacks have become more sophisticated, new types of firewalls have been developed, which serve different purposes.

Common firewall types:

1. **Network layer firewall:** This filters communications based on source and destination IP addresses.
2. **Transport layer firewall:** Filters communications based on source and destination data ports, as well as connection states.
3. **Application layer firewall:** Filters communications based on an application, program or service.
4. **Context aware layer firewall:** Filters communications based on the user, device, role, and application type and threat profile.
5. **Proxy server:** Filters web content requests like URLs, domain names and media types.
6. **Reverse proxy server:** Placed in front of web servers, reverse proxy servers protect, hide, offload and distribute access to web servers.
7. **Network address translation (NAT) firewall:** This firewall hides or masquerades the private addresses of network hosts.
8. **Host-based firewall:** Filters ports and system service calls on a single computer operating system.

Port scanning

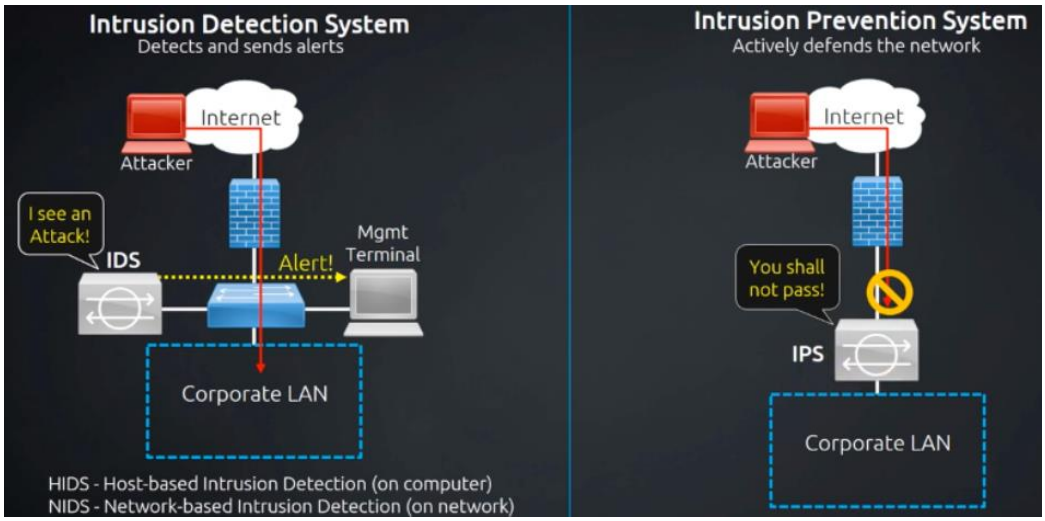
In networking, each application running on a device is assigned an identifier called a port number. This port number is used on both ends of the transmission so that the right data is passed to the correct application. Port scanning is a process of probing a computer, server or other network host for open ports. It can be used maliciously as a reconnaissance tool to identify the operating system and services running on a computer or host, or it can be used harmlessly by a network administrator to verify network security policies on the network.

Find out how to carry out a port scan on a computer on your local home network.

i. Download and launch a port scanning tool like Zenmap https://nmap.org/zenmap/ . Enter the IP address of your computer, choose a default scanning profile and press 'scan.'
ii. The scan will report any services that are running, such as web or email services, and their port numbers.
iii. The scan will also report one of the following responses:
    - ✓ 'Open' or 'Accepted' means that the port or service running on the computer can be accessed by other network devices.
    - ✓ 'Closed,' 'Denied' or 'Not Listening' means that the port or service is not running on the computer and therefore cannot be exploited.
    - ✓ 'Filtered,' 'Dropped' or 'Blocked' means that access to the port or service is blocked by a firewall and therefore it cannot be exploited.
iv. To execute a port scan from outside of your network, you will need to run it against your firewall or router's public IP address. Enter the query 'what is my IP address?' into a search engine such as Google to find out this information.
v. Go to the Nmap Online Port Scanner https://hackertarget.com/nmap-online-port-scanner/ enter your public IP address in the input box and press 'Quick Nmap Scan.' If the response is open for ports 21, 22, 25, 80, 443 or 3389 then most likely, port forwarding has been enabled on your router or firewall and you are running servers on your private network.

Intrusion detection systems and intrusion prevention systems

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are critical network security technologies designed to identify and respond to malicious activities. While IDS primarily monitors and detects suspicious behavior, alerting administrators to potential threats, IPS actively blocks and prevents these threats in real time to protect the network from harm. Together, they provide a comprehensive approach to network defense by combining detection and prevention capabilities.



"Software is not perfect. And more than ever before, hackers are exploiting flaws in software before creators get a chance to fix them. When they do this, hackers are said to have carried out a zero-day attack! The ability to detect these attacks in real time, and stop them immediately, or within minutes of occurring, is the ultimate goal."

Real-Time Detection

Many organizations today are unable to detect attacks until days or even months after they occur.

- Detecting attacks in real time requires actively scanning for attacks using firewall and IDS/IPS network devices. Next generation client and server malware detection with connections to online global threat centers must also be used. Today, active scanning devices and software must detect network anomalies using context-based analysis and behavior detection.
- DDoS is one of the biggest attack threats requiring real-time detection and response. For many organizations, regularly occurring DDoS attacks cripple Internet servers and network availability. These attacks are extremely difficult to defend against because the attacks originate from hundreds, even thousands, of zombie hosts, and the attacks appear as legitimate traffic.

Protecting Against Malware

One way of defending against zero-day attacks and advanced persistent threats (APTs) is to use an enterprise-level advanced malware detection solution, like Cisco's Advanced Malware Protection (AMP) Threat Grid.

This is client/server software that can be deployed on host endpoints, as a standalone server or on other network security devices. It analyzes millions of files and correlates them against hundreds of millions of other analyzed malware artifacts for behaviors that reveal an APT. This approach provides a global view of malware attacks, campaigns and their distribution.

Find out more about the benefits of Cisco's Threat Grid.

- **Secure operations center team:** The Threat Grid allows the Cisco Secure Operations Center team to gather more accurate, actionable data.
- **Incidence Response team:** The Incidence Response team therefore has access to forensically sound information from which it can more quickly analyze and understand suspicious behaviors.
- **Threat Intelligence team:** Using this analysis, the Threat Intelligence team can proactively improve the organization's security infrastructure.
- **Security Infrastructure engineering team:** Overall, the Security Infrastructure Engineering team is able to consume and act on threat information faster, often in an automated way.

Security Best Practices

Many national and professional organizations have published lists of security best practices. Some of the most helpful guidelines are found in organizational repositories such as the National Institute of Standards and Technology (NIST) Computer Security Resource Center.

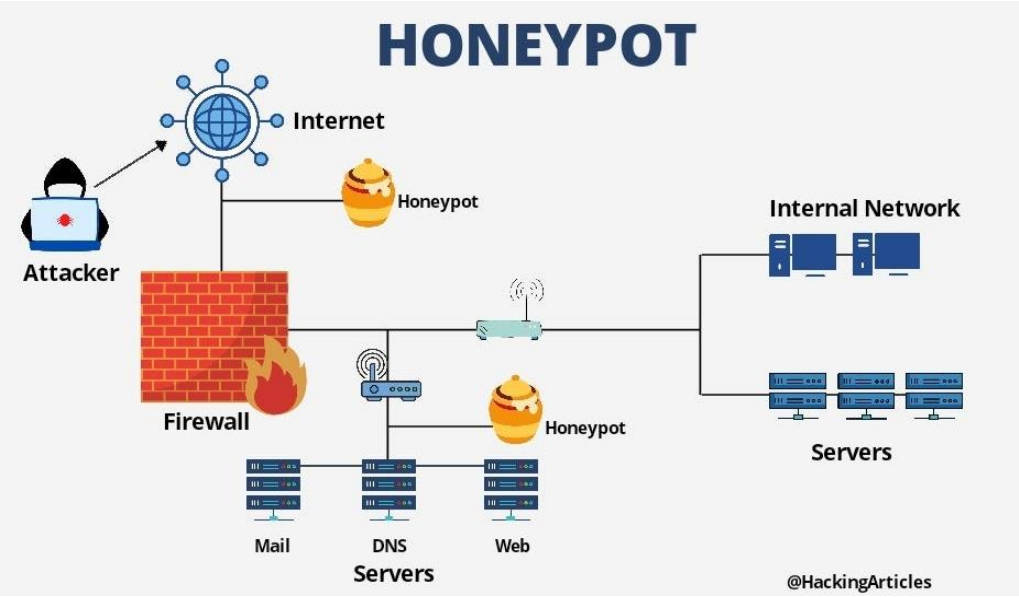
1. **Perform a risk assessment:** Knowing and understanding the value of what you are protecting will help to justify security expenditures.
2. **Create security policy:** Create a policy that clearly outlines the organization's rules, job roles, and responsibilities and expectations for employees.
3. **Physical security measures:** Restrict access to networking closets and server locations, as well as fire suppression.
4. **Human resources security measures:** Background checks should be completed for all employees.
5. **Perform and test backups:** Back up information regularly and test data recovery from backups.
6. **Maintain security patches and updates:** Regularly update server, client and network device operating systems and programs.
7. **Employ access controls:** Configure user roles and privilege levels as well as strong user authentication.
8. **Regularly test incident response:** Employ an incident response team and test emergency response scenarios.
9. **Implement a network monitoring, analytics and management tool:** Choose a security monitoring solution that integrates with other technologies.
10. **Implement network security devices:** Use next generation routers, firewalls and other security appliances.
11. **Implement a comprehensive endpoint security solution:** Use enterprise level antimalware and antivirus software.
12. **Educate users:** Provide training to employees in security procedures. One of the most widely known and respected organizations for cybersecurity training is the SANS Institute. Click here https://www.sans.org/about/ to learn more about SANS and the types of training and certifications they offer.
13. **Encrypt data:** Encrypt all sensitive organizational data, including email.

Behavior Approach to Cybersecurity

- Behavior-based security: Behavior-based security is a form of threat detection that involves capturing and analyzing the flow of communication between a user on the local network and a local or remote destination. Any changes in normal patterns of behavior are regarded as anomalies, and may indicate an attack.

Two behavior-based detection tools:

1. **Honeypot: A** honeypot is a cybersecurity tool designed to lure attackers by mimicking real systems, applications, or data. It acts as a decoy to attract malicious activity, allowing security teams to observe attacker behavior, gather intelligence, and detect intrusion attempts without putting actual assets at risk. Honeypots can also help identify vulnerabilities and improve overall threat detection and response strategies.



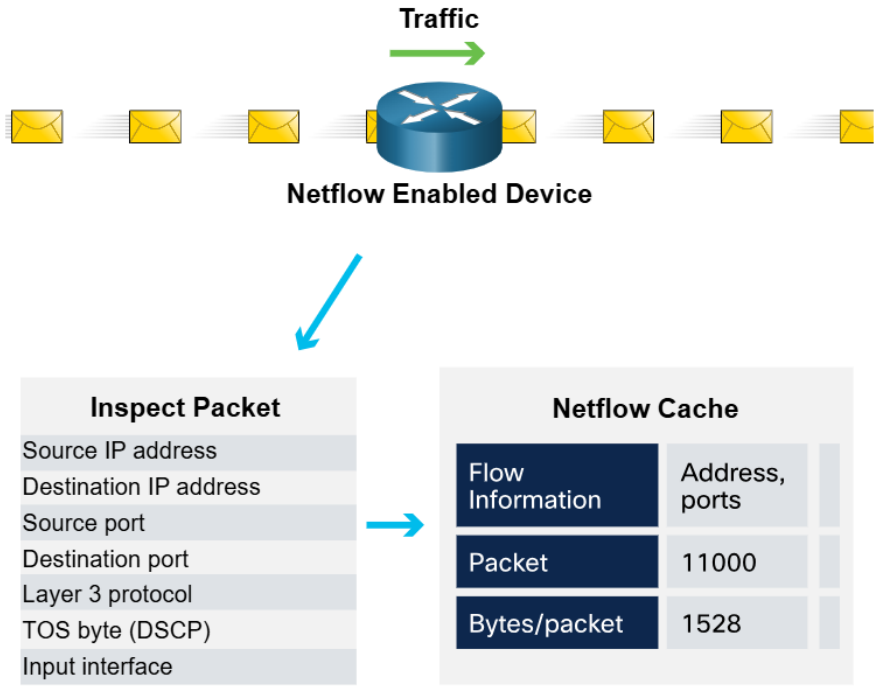
2. **Cisco's Cyber Threat Defense Solution Architecture:** This security architecture uses behavior-based detection and indicators to provide greater visibility, context and control. The aim is to know who is carrying out the attack they are performing and where, when and how the attack is taking place. This security architecture uses many security technologies achieve this goal.

NetFlow

NetFlow technology is used to gather information about data flowing through a network, including who and what devices are in the network, and when and how users and devices access the network.

NetFlow is an important component in behavior-based detection and analysis. Switches, routers and firewalls equipped with NetFlow can report information about data entering, leaving and traveling through the network.

This information is sent to NetFlow collectors that collect, store and analyze NetFlow data, which can be used to establish baseline behaviors on more than 90 attributes, such as source and destination IP address.



Penetration testing

Penetration testing, commonly known as pen testing, is the act of assessing a computer system, network or organization for security vulnerabilities. A pen test seeks to breach systems, people, processes and code to uncover vulnerabilities which could be exploited. This information is then used to improve the system's defenses to ensure that it is better able to withstand cyber attacks in the future.

The five-step pen test process.

1. **Planning:** The pen tester gathers as much information as possible about a target system or network, its potential vulnerabilities and exploits to use against it. This involves conducting passive or active reconnaissance (footprinting) and vulnerability research
2. **Scanning:** The pen tester carries out active reconnaissance to probe a target system or network and identify potential weaknesses which, if exploited, could give an attacker access. Active reconnaissance may include:
    i. Port scanning to identify potential access points into a target system
    ii. Vulnerability scanning to identify potential exploitable vulnerabilities of a particular target
    iii. Establishing an active connection to a target (enumeration) to identify the user account, system account and admin account.

3. **Gaining access:** The pen tester will attempt to gain access to a target system and sniff network traffic, using various methods to exploit the system including:
    i. Launching an exploit with a payload onto the system
    ii. Breaching physical barriers to assets
    iii. Social engineering
    iv. Exploiting website vulnerabilities
    v. Exploiting software and hardware vulnerabilities or misconfigurations
    vi. Breaching access controls security
    vii. Cracking weak encrypted Wi-Fi.
4. **Maintaining access:** The pen tester will maintain access to the target to find out what data and systems are vulnerable to exploitation. It is important that they remain undetected, typically using backdoors, Trojan horses, rootkits and other covert channels to hide their presence.
   When this infrastructure is in place, the pen tester will then proceed to gather the data that they consider valuable.
5. **Analysis and reporting:** The pen tester will provide feedback via a report that recommends updates to products, policies and training to improve an organization's security.

Impact Reduction

While most organizations today are aware of common security threats and put considerable effort into preventing them, no set of security practices is foolproof. Therefore, organizations must be prepared to contain the damage if a security breach occurs. And they must act fast!

The actions organizations should take when a security breach is identified.

1. **Communicate the issue:** Communication creates transparency, which is critical in this type of situation.

    i. **Internally,** all employees should be informed and a clear call to action communicated.
    ii. **Externally,** all clients should be informed through direct communication and official announcements.

2. **Be sincere and accountable:** Respond to the breach in an honest and genuine way, taking responsibility where the organization is at fault.
3. **Provide the details:** Be open and explain why the breach took place and what information was compromised. Organizations are generally expected to cover any client costs associated with identity theft services required as a result of a security breach.
4. **Find the cause:** Take steps to understand what caused and facilitated the breach. This may involve hiring forensics experts to investigate and uncover the details.

5. **Apply lessons learned:** Make sure that any lessons learned from forensic investigations are applied to prevent similar breaches from happening in the future.
6. **Check, and check again:** Attackers often attempt to leave a backdoor to facilitate future breaches. To prevent this, ensure that all systems are thoroughly cleaned, no backdoors remain, and nothing else has been compromised.
7. **Educate:** Raise awareness, train, and educate employees, partners, and clients on how to prevent future breaches.

"Don't forget, the impact of a security breach extends beyond the technical aspect of stolen data or damaged intellectual property. It can have a devastating effect on an organization's reputation!"

Risk management

Risk management is the formal process of continuously identifying and assessing risk in an effort to reduce the impact of threats and vulnerabilities. You cannot eliminate risk completely, but you can determine acceptable levels by weighing the impact of a threat against the cost of implementing controls to mitigate it. The cost of a control should never exceed the value of the asset you are protecting. The risk management process typically involves the following key steps:

1. **Identify Risks:** Continuously recognize potential threats and vulnerabilities that could impact assets or operations.
2. **Assess Risks:** Evaluate the likelihood and potential impact of each identified risk to understand its severity.
3. **Prioritize Risks:** Rank risks based on their assessed impact and likelihood to focus on the most critical ones.
4. **Implement Controls:** Select and apply appropriate measures or controls to mitigate, transfer, accept, or avoid the risks.
5. **Monitor and Review:** Continuously monitor risks and the effectiveness of controls, updating the risk assessment and management strategies as needed.
6. **Communicate:** Keep stakeholders informed about risks, mitigation efforts, and any changes in the risk environment.

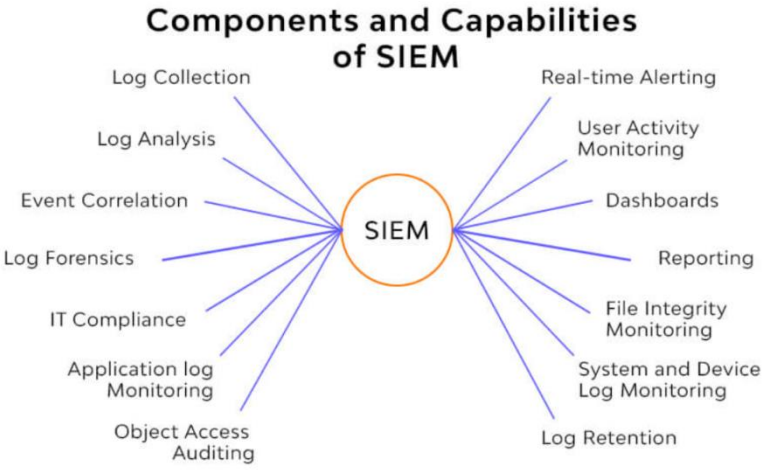
Tools used to detect and prevent security incidents.

There are a range of tools used to detect and prevent security incidents.

i. **SIEM** stands for **Security Information and Event Management**.: It's a tool that collects, analyzes, and correlates security data from across an organization's IT environment in real-time. SIEM helps to:

- Detect security incidents by identifying unusual or suspicious activity.
- Provide centralized logging and monitoring of security events.
- Generate alerts and reports to support incident response and compliance requirements.

SIEM systems play a critical role in helping organizations detect, investigate, and respond to threats quickly.



ii. **DLP** stands for **Data Loss Prevention**: It's a security tool designed to detect and prevent unauthorized access, use, or transmission of sensitive data outside an organization.

Key functions of DLP include:

- Monitoring data in use, in motion, and at rest.
- Enforcing policies to block or alert on activities that risk data leakage.
- Protecting confidential information like personal data, intellectual property, or financial records.

DLP helps organizations reduce the risk of data breaches and comply with regulations by keeping sensitive information secure.

Legal Issues in Cybersecurity

In order to protect against attacks, cybersecurity professionals must have the same skills as the attackers. However, cybersecurity professionals use their skills within the bounds of the law.

Personal legal issues

At work or home, you may have the opportunity and skills to hack another person's computer or network. But there is an old saying, 'Just because you can does not mean you should.' Most hacks leave tracks, which can be traced back to you.

Cybersecurity professionals develop many skills, which can be used positively or illegally. There is always a huge demand for those who choose to put their cyber skills to good use within legal bounds.

Corporate legal issues

Most countries have cybersecurity laws in place, which businesses and organizations must abide by. In some cases, if you break cybersecurity laws while doing your job, the organization may be punished and you could lose your job. In other cases, you could be prosecuted, fined and possibly sentenced.

In general, if you are unsure whether an action or behavior might be illegal, assume that it is illegal and do not do it. Always check with the legal or HR department in the organization.

International law and cybersecurity

International cybersecurity law is a constantly evolving field. Cyber attacks take place in cyberspace, an electronic space created, maintained and owned by both the public and private entities. There are no traditional geographic boundaries in cyberspace. To further complicate issues, it is much easier to mask the source of a attack in cyberwarfare than in conventional warfare.

The global society is still debating how best to deal with cyberspace. Country practice, opinio juris (a sense on behalf of a country that it is bound to the law in question) and any treaties drafted will shape international cybersecurity law.

"In addition to working within the confines of the law, you must also be able to demonstrate ethical behavior and act responsibly in your work. Let's consider an example."

Ethical Issues in Cybersecurity

Think back to the pen test you carried out for @Company. This test revealed that one of your colleagues, who started at the same time as you, was responsible for a data breach. You are thinking of not including this in your report as they might get in trouble.

- **Ask yourself the following questions to help you decide on the best course of action.**

  - ✓ Is it legal?
  - ✓ Does your action comply with @Company policy?
  - ✓ Will your action be favorable for @Company and its stakeholders?
  - ✓ Would it be okay if everyone in @Company took this action?
  - ✓ Would the outcome of your action represent @Company in a positive light in a news headline?

- How to answer
  - ✓ **YES:** If you are able to answer 'yes' to off those questions. Then it's likely to be appropriate to move forward with you action. However, it's important to remember that just because something is legal, it may not be ethical. In this case, while withholding the information from your pen test report is not illegal, it is not the ethical thing to do. The consequences of not reporting it could be devastating for @Company and its customers.
  - ✓ **NO:** If you response to any of those questions is 'no'. You should stoop and reconsider your actions, which could have serious legal ramifications for your and the organization. In this example, you are right to question your initial thoughts. Every new finding in cybersecurity must be reported to protect @company and its customers. Remember, always seek advice from your line manager or legal or HR representative to clarify in your action or behaviors might be considered unethical.

Here are some professional IT organizations that published Codes of Ethics to help guide employee actions and behaviors.

- **Information Systems Security Association (ISSA):** https://issa.org/code-of-ethics/
- CISCO: https://www.cisco.com/c/m/en_us/about/csr/esg-hub.html , https://investor.cisco.com/corporate-governance/code-of-business-conduct/default.aspx