# The Need for Cybersecurity

- **Cybersecurity** is the ongoing effort to protect these networked systems and all of the data from unauthorized use or harm.
- On a **personal level**, you need to safeguard your identity, your data, and your computing devices.
- At the **corporate level**, it is everyone's responsibility to protect the organization's reputation, data, and customers.
- At the **state level,** national security, and the safety and well-being of the citizens are at stake.

- Your **online identity** is how you present yourself to others online. This online identity should only reveal a limited amount of information about you.

# CIA Triad

- CIA triad is a **guideline for information security** for an organization.
- **Confidentiality** ensures the privacy of data by restricting access through authentication encryption. Company policies should restrict access to the information to authorized personnel.
- **Integrity** assures that the information is accurate and trustworthy. Data must be unaltered during transit and not changed by unauthorized entities. Backups must be available to restore any corrupted data, and hashing can be used to verify integrity of the data during transfer.
- **Availability** ensures that the information is accessible to authorized people. Plans should be in place to recover quickly from natural or man-made disasters. Security equipment or software, such as firewalls, guard against downtime due to attacks such as denial of service (DoS).

# LastPass Security Breach (2015)


- The **online password manager, LastPass**, detected **unusual activity** on its network in **July 2015**. It turned out that hackers had stolen user email addresses, password reminders, and authentication hashes. Fortunately for the users, the hackers were unable to obtain anyone's encrypted password vaults.
- Even though there was a security breach, LastPass could still safeguard the users' account information. LastPass requires email verification or multi-factor authentication whenever there is a new login from an unknown device or IP address. The hackers would also need the master password to access the account.
- If the users and service providers both utilize the proper tools and procedures to safeguard the users' information, the users' data could still be protected, even in the event of security breach.
- LastPass users also have some responsibility in safeguarding their own accounts. The users should always use complex master passwords and change the master passwords periodically.
- The users should always beware of Phishing attacks. An example of a Phishing attack would be if an attacker sent fake emails claiming to be from LastPass. The emails ask the users to click an embedded link and change the password. The link in the email goes to a fraudulent version of the website used to steal the master password. The users should never click the embedded links in an email. The users should also be careful with their password reminder. The password reminder should not give away your passwords. Most importantly, the users should enable multi-factor authentication when available for any website that offers it.

# Vtech Security Breach (2015)

- The **high tech toy maker for children, Vtech**, suffered a **security breach to its database** in **November 2015**. This breach could affect millions of customers around the world, including children. The data breach exposed sensitive information including customer names, email addresses, passwords, pictures, and chat logs.
- A toy tablet had become a new target for hackers. The customers had shared photos and used the chat features through the toy tablets. The information was not secured properly, and the company website did not support secure SSL communication. Even though the breach did not expose any credit card information and personal identification data, the company was suspended on the stock exchange because the concern over the hack was so great.
- Vtech did not safeguard the customers' information properly and it was exposed during the breach. Even though the company informed its customers that their passwords had been hashed, it was still possible for the hackers to decipher them.
- The passwords in the database were scrambled using MD5 hash function, but the security questions and answers were stored in plaintext. Unfortunately, MD5 hash function has known vulnerabilities. The hackers can determine the original passwords by comparing millions of pre-calculated hash values.
- With the information exposed in this data breach, cybercriminals could use it to create email accounts, apply for credits, and commit crimes before the children were old enough to go to school. For the parents of these children, the cybercriminals could take over the online accounts because many people reuse their passwords on different websites and accounts.
- For parents, it is a wake-up call to be more vigilant about their children's privacy online and demand better security for children's products. For the manufacturers of network-connected products, they need to be more aggressive in the protection of customer data and privacy now and in the future, as the cyberattack landscape evolves.

# Equifax Security Breach (2015)

- **Equifax Inc.** is one of the **nationwide consumer credit reporting agencies** in the United States. This company collects information on millions of individual customers and businesses worldwide. Based on the collected information, credit scores and credit reports are created about the customers. This information could affect the customers when they apply for loans and when they are looking for employment.
- In September 2017, Equifax publicly announced a data breach event. The attackers exploited a **vulnerability in the Apache Struts web application** software. The company believes that millions of U.S. consumers' sensitive personal data were accessed by the cyber criminals between May and July of 2017. The personal data includes the customers' full names, Social Security numbers, birth dates, addresses and other personally identifiable information. There is evidence that the breach may have affected customers in United Kingdom and Canada.
- Equifax established a dedicated web site that allows the consumers to determine if their information was compromised, and to sign up for credit monitoring and identity theft protection. Using a new domain name, instead of using a subdomain of equifax.com, this allowed nefarious parties to create unauthorized websites with similar names. These websites can be used as part of a phishing scheme to trick you into providing personal information. Furthermore, an employee from Equifax provided an incorrect web link in social media for worried customers. Fortunately, this web site was taken down within 24 hours. It was created by an individual who use it as an educational opportunity to expose the vulnerabilities that exists in Equifax's response page.
- As a concerned consumer, you may want to quickly verify if your information was compromised, so you can minimize the impact. In a time of crisis, you may be tricked into using unauthorized websites. You should be cautious about providing personal information so you do not become a victim again. Furthermore, companies are responsible for keeping our information safe from unauthorized access. Companies need to regularly patch and update their software to mitigate exploitation of known vulnerabilities. Their employees should be educated and informed about the procedures to safeguard the information and what to do in the event of a breach.
- Unfortunately, the real victims of this breach are the individuals whose data may have been compromised. In this case, Equifax has the burden of protecting the collected consumer data while conducting credit checks because the customers did not choose to use the services provided by Equifax. The consumer has to trust the company to safeguard the collected information. Furthermore, the attackers can use this data to assume your identity, and it is very difficult to prove otherwise because both the attacker and the victim know the same information. In these situations, the most you can do is be vigilant when you are providing personally identifiable information over the Internet. Check your credit reports regularly (once per month or once per quarter). Immediately report any false information, such as applications for credit that you did not initiate, or purchases on your credit cards that you did not make.

# Types of Cyber Attackers

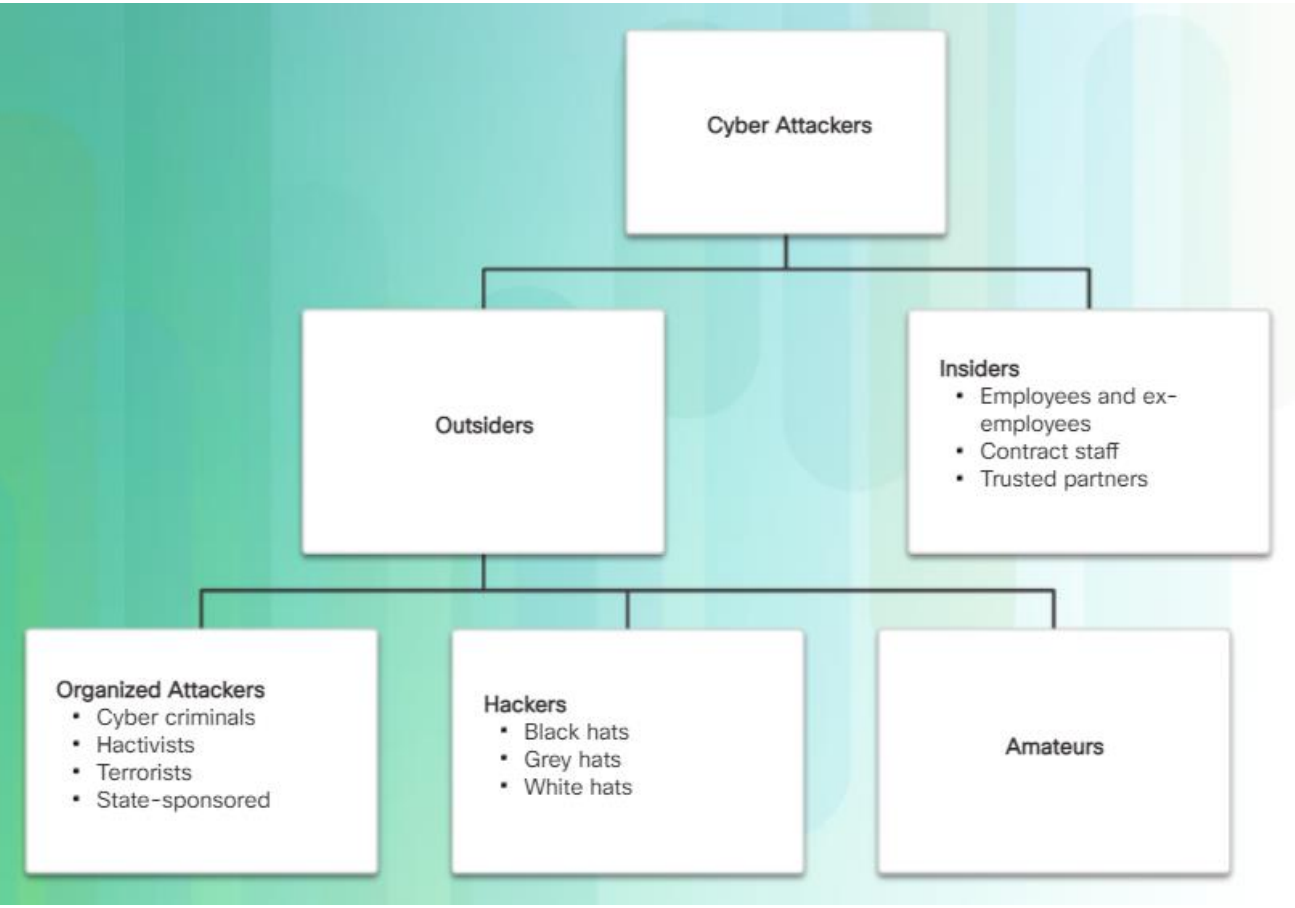
- **Amateurs**, also called script kiddies, often using existing tools or instructions found on the Internet to launch attacks.
- **White hat hackers** break into networks or computer systems to discover weaknesses so that the security of these systems can be improved. These break-ins are done with prior permission and any results are reported back to the owner.
- **Black hat hackers** take advantage of any vulnerability for illegal personal, financial or political gain.
- **Gray hat hackers** are somewhere between white and black hat hackers. They may find a vulnerability in a system and report the vulnerability to the owners of the system if that action coincides with their agenda. Some publish the facts about the vulnerability on the Internet so that other attackers can exploit it.

**Individuals**

- **Cyber criminals** are usually groups of professional criminals focused on control, power, and wealth. The criminals are highly sophisticated and organized, and they may even provide cybercrime as a service to other criminals.
- **Hacktivists** make political statements to create awareness to issues that are important to them.
- **State-sponsored hackers** gather intelligence or commit sabotage on behalf of their government. These attackers are usually highly trained and well-funded, and their attacks are focused on specific goals that are beneficial to their government.

**Organized hackers**

# Internal and External Threats




- Attacks can be originated from **within** an organization or from **outside** of the organization.
- **Internal threats** have the potential to cause greater damage than external threats, because internal users have direct access to the building and its infrastructure devices. Employees also have knowledge of the corporate network, its resources, and its confidential data, as well as different levels of user or administrative privileges.
- An internal user, such as an employee or contract partner, can accidently or intentionally; mishandle confidential data; threaten the operations of internal servers or network infrastructure devices; facilitate outside attacks by connecting infected USB media into the corporate computer system; accidentally invite malware onto the network through malicious email or websites
- **External threats** from amateurs or skilled attackers can exploit vulnerabilities in network or computing devices, or use social engineering to gain access.

# Cyberwarfare

- Cyberwarfare is an **Internet-based conflict** that involves the penetration of computer systems and networks of other **nations**.
- These attackers have the resources and expertise to launch massive Internet-based attacks against other nations to cause **damage or disrupt services**, such as shutting down a power grid.
- A nation can continuously invade other nation's infrastructure, steal defense secrets, and gather information about technology to narrow the gaps in its industries and military. Besides industrial and militaristic espionage, cyberwar can sabotage the infrastructure of other nations and cost lives in the targeted nations. For example, an attack can disrupt the power grid of a major city. Traffic would be disrupted. The exchange of goods and services is halted. Patients cannot get the care needed in emergency situations. Access to the Internet may also be disrupted. By affecting the power grid, the attack can affect the everyday life of ordinary citizens.
- An example of a state-sponsored attack involved the **Stuxnet** malware that was **designed to damage Iran's nuclear enrichment plant**. Stuxnet malware did not hijack targeted computers to steal information. It was designed to damage physical equipment that was controlled by computers. It used modular coding that was programmed to perform a specific task within the malware. It used stolen digital certificates so the attack appeared legitimate to the system.
- If the government cannot defend against the cyberattacks, the citizens may lose confidence in the government's ability to protect them. Cyberwarfare can destabilize a nation, disrupt commerce, and affect the citizens' faith in their government without ever physically invading the targeted nation.
- See video: Breaking Down Stuxnet.
- See video: Stuxnet: Anatomy of a Computer Virus.