**Threat actors and definitions**

[- [Instructor] In previous videos we covered what a hacker is, including the various types, and now we are going to get more in depth about various threat actors and what they mean. Let's start with defining what a cyber criminal is. Similar to regular run of the mill criminals you see in the movies or on TV, cyber criminals are not much different, except for their method of committing the crime. Cyber criminals still commit crimes, they just do it via digital means such as computers, mobile devices and the internet. They may steal personal and/or company data as a way to turn a profit or even exploit individuals or companies. Cyber criminals are not who you want to welcome into your networks or devices, though they are very good at finding and forcing their way in. You can't turn on the news nowadays without hearing of the latest data breach caused by these individuals or groups. A data breach as defined by Trend Micro, is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner. A small company or large organization may suffer a data breach. Stolen data may involve sensitive, proprietary or confidential information, such as credit card numbers, customer data, trade secrets, or even matters of national security. So just how do these cyber criminals get into a network and breach data? Unfortunately, there are a number of ways, but one we will define here is via an exploit. An exploit is when there is a digital flaw or vulnerability that a cyber criminal has discovered and they are able to leverage said flaw or vulnerability to gain unwanted access to networks, systems, software, and more. Think of it like a criminal going door to door until they're able to find a broken lock or an open window that allows them to go inside and gain access to things that they want to take, while cyber criminals usually don't reside within the company, there are other threats to consider that do. The term for this is insider threat, which is when someone within the company or organization has access to private or confidential information, and they share this information both willingly and unwillingly with threat actors. The reason it can be unwillingly is if the insider accidentally divulges information or access to information without even realizing. A way to circumvent accidental data leakage is through various processes, technologies and even training. The other side of insider threat is when it is conducted willingly and with intention. There are very things that may motivate someone to turn on a company or organization in such a way they would share a secret or confidential information, including but not limited to personal injustices related to pay, performance or even leadership. There are even instances where individuals may be approached and incentivized to divulge this information from someone outside of the organization that could use it for personal gain. Similar to the concept of a mole, an insider threat can wreak havoc on your company environment.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/threat-actors-and-definitions?autoSkip=true&contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)

**Technical risks**

[- [Instructor] You now know who the threat actors are, but do you know some of the tactics that they leverage? While companies are always implementing controls to protect against the bad guys, the bad guys are always trying to stay one step ahead. Let's dive a bit more into some of the methods the cyber criminals utilize to gain unwarranted access. First up is advanced persistent threat, also known as APT. According to Kaspersky, APT uses continuous clandestine and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences. They are stealth and may access a network and lay dormant for a while before they strike, or they may be in a network for months or even years, siphoning information undetected. Think of it like if your home had termites. You would assume your home was built to be safe from the risk, and once they were in, you likely wouldn't know before it was too late and the damage was done. A botnet is a group of computers or other internet-connected devices being controlled in unison to perform malicious acts. Botnets have also been referred to like zombies in that once they are infected, they no longer have a mind of their own but instead are being manipulated to perform specific tasks to take down others. The same is true for botnets. Once controlled, they may propagate viruses, malware, and even conduct DDoS attacks against others. Oftentimes, without the knowledge of the owner of said device. So what are these DDoS attacks that botnet can perform? DDoS, also known as distributed denial of service, is when a threat actor intentionally floods a server beyond its capacity to the point it essentially breaks and/or others can't access the site or service. Similar to when people try to call a phone number, but too many people are trying to also call at the same time, so they keep getting a busy signal. And they can't get through. However, the differentiator in this attack scenario here is that this is done with malicious intent. Malware is a term that is actually two words combined to create a new word, malicious software, AKA malware. Malware is software that is designed specifically with the intent of performing malicious tasks and wreaking havoc on computer systems by gaining unwarranted access, disrupting service, and even purposefully causing damage via viruses, Trojans, and more. A virus is a very specific version of malware that can self-replicate and spread. A computer virus is similar to a virus in people that can actually make them sick. The more things it comes in contact with that don't have the proper protection in place, the more it will propagate and infect, though the damage may differ. Though a virus is just one of many forms of malware, it is often the one we hear the most because it is the most common.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/technical-risks?contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)

**Threats that target the human element**

[- [Instructor] What about the human side of security? The human element is often the most exploited, but why and how do the cyber criminals do it? The first, most commonly leveraged method attacking the human element is social engineering. The best way to describe social engineering is to think of a puppet master pulling the strings on a puppet to get the puppet to do exactly what they want, when they want. Social engineering is the same. In that an attacker plays the role of the puppeteer, trying to manipulate the people who play the role of the puppet into divulging information or giving access to certain things that shouldn't be shared. And all of this is done for malicious purposes. This can be conducted in a number of ways, but we will cover some of the most common. Then we have phishing. Phishing is when an email is sent with malicious intent with the appearance of coming from a legitimate person or company. However, that is not the case. Phishing is named so because like with sport fishing, a malicious actor throws out a line, hoping that someone takes the bait by either replying to the email, clicking on a link or opening an attachment. Vishing while similar in nature to phishing is conducted over the phone instead of via email. A threat actor may contact you via phone and solicit personal or confidential company information with ill-natured intent. These attackers may pose as legitimate businesses or government organizations or may even play into your human instinct to want to help. Smishing is SMS or text message phishing. Have you ever received a strange text on your phone asking you to click a link to something you weren't expecting? This may have been a real-life example of smishing. Smishing may include a link to a malicious site or may request personal information that you wouldn't typically divulge via text. It is always important to be wary of all types of ishing attacks and stay up to date on the cyber criminals' tactics. Spoofing is just one mechanism that the bad guys may leverage in these types of attacks. Spoofing is where they make an email, call, or even text message appear as though it is coming from a trusted name, number, and or source. They do this spoofing or impersonating with the help of technology to look like trusted people or organizations with the hopes that the attack seems more believable and the receiver will fall for it and take the suggested action. Another threat vector that continues to grow year over year is ransomware. Ransomware is similar to how it sounds. When something is taken and a ransom is requested to get it back. But in this, the items that are taken or locked down are digital. And in order to gain back access, the cyber criminal request payment, typically in cryptocurrency.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/threats-that-target-the-human-element?contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)

**Apply cybersecurity terminology**

[- [Instructor] With limited time, we were unable to cover each and every definition and/or acronym within cybersecurity. However, it is my hope that you were able to learn a number of new concepts in a way that was easily digestible. Now that you've discovered the definition of a number of concepts you may or may not have heard before, I hope you are able to apply what you learned in your everyday conversations around cybersecurity, both at work and at home. If there were definitions not covered in this training or if there are definitions that you want to take a deeper dive into learning more about, I encourage you to check out the extensive catalog of cybersecurity training right here on LinkedIn Learning. There are many exceptional instructors that can help take you beyond just the definitions in a truly immersive learning experience. Also, make sure to check out the definition library in the Resources section of this training. This document will include the definitions we covered in this training and can serve as a hands-on reference for the definitions covered. And remember, always keep learning and never lose the passion to help make your workplace and the world a more secure place for all of us.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/apply-cybersecurity-terminology?contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)