**What is cybersecurity?**

[- [Instructor] Cybersecurity may be called a number of things including Information Security, Computer Security and even just Cyber InfoSec among some others not mentioned. According to Digital Guardian, cybersecurity refers to the body of technologies, processes, and practices, designed to protect networks, devices, programs, and data from attack, damage or unauthorized access. As the use of technology and data continues to grow exponentially, so does the need for protecting the technology and the data. That is where cybersecurity comes in. Cybersecurity doesn't just apply at work though, it also applies in your personal life, on your personally owned devices such as computers, cell phones, and even other IoT devices that are being brought into your home. As technology continues to advance, so to do the associated risks. Multiple layers of defense and continuous awareness and training around these risks are imperative in order to create safety and security on networks and devices. We will cover a number of technologies leveraged in cyber to protect people, data, and organizations. Additionally, we will look at some of the positions within cybersecurity teams, and even to find some of the threat actors that are looking to infiltrate our data and use it for malicious purposes. We will also break down some of the policies, processes, guidelines, and frameworks that are put into place to create a better understanding of what needs to be done in order to keep data, information, and assets secure in the first place. In this training, we have aligned the terminology we will define similarly to the definition provided at the beginning of this video. We broke down the training into three segments, people, processes, and technology, which is often coined as the three pillars of cybersecurity. As the saying goes, you don't know what you don't know. However, this course will help change all of that. Whether you are in security, IT, HR, finance, or anywhere else, understanding some of the basic terminology within the cybersecurity field will allow you to take a huge step forward in playing your part in helping to secure your organization. So, let's get started.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/what-is-cybersecurity?autoSkip=true&contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)

**People, process, and technology**

[- [Instructor] First up is people. The people pillar includes a number of elements, from the way the teams are structured to the way the companies protect the human element and even who the adversaries are that you must protect against. Next up is the process. When people hear processes, they tend to assume documentation. And while that is right, there is a lot more that goes into the process pillar in security, including, but not limited to, specific technical controls to protect the company, its assets, and its people. And finally, we will cover technology. Technology is the most well-known pillar within cybersecurity, which isn't surprising, as cybersecurity needs technology as much as technology needs cybersecurity. Within this pillar, we will cover security best practices and controls, as well as define some of the more recent technological advancements. Though most of the definitions were able to fit within the scope of the three pillars, there was still a large area that we had to define outside of people, process, and technology. That is the threat actors and their methods of executing attacks. As attacks continue to grow, so does the need for cyber security in all its forms, including people, process, and technology.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/people-process-and-technology?contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)

### Security awareness and leadership

[- [Instructor] As technology continues to advance and processes and requirements continually change, one thing remains constant, and that is the people. While advancements in technology have taken some of the human aspect out of the equation, there is one that will never be able to be replaced, and that is the end user. The term, user, is utilized often in security, and is defined as a person or group of people that operate within your business environment including but not limited to operating computers, systems, applications, networks, and more. This term is typically used to describe employees in a more technical sense, and is often associated with a username, login name, or screen name. Let's take a look at the leadership. Usually, though not always, within a security organization, there will be a CISO or CSO that leads the security team. The difference between a CISO and a CSO is that CISO stands for chief information security officer, and means that the team consists of just logical and technological security positions and areas of focus. Whereas the CSO stands for chief security officer, and usually means that this group is all-encompassing of security, including both logical and physical security within the respective groups. Many times under the CISO or CSO security umbrella is a dedicated area to protect the human element. Typically, this falls under the name of security awareness, though it may be named a few other things, such as security training, security education, security culture, and even human risk officer. Security awareness is a person, group, or team that focuses on awareness, training, communications, and education for the employees of the organization. Their goal within the program is to help make the employees more knowledgeable of the risk, both they and their organization face, as well as what to do if they are faced with those risks. Their end goal is to create a more security-minded environment and risk-averse culture. While a security awareness person, team, or group is essential to any successful security program, this team can't be everywhere to train everyone. One approach to help expand their awareness efforts is to create a network of extensions of the security team, which is often called security champions. Other terms used interchangeably include security ambassadors, partners, or liaisons. A security champion is someone in a company that volunteers their time to help create a more secure environment as well as helps develop a two-way pipeline between security and other groups, regions, and organizations within a company. While there are many positions, teams, and individuals we didn't list that make up the people side of security, the three we did cover all can work together in a business or organization to accomplish one goal, securing the company and its assets and data.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/security-awareness-and-leadership?autoSkip=true&contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)

### Red vs. blue vs. purple teams

[- [Instructor] What makes up a security team, and how are the people categorized? Oftentimes there is a red team, a blue team, and sometimes even a purple team. Let's take a deeper dive into the makeup of a security team and how they may be categorized. Typically, one will hear red team versus blue team when threat exercises are being conducted within their organization or their environment. Let's break down exactly what red and blue teams look like, as well as what a newer group, labeled purple team, means as well. In the most simplest of terms, a red team is the group that attacks. Usually, this is done via third-party penetration test, or via social engineering, or even vulnerability scanning. This is conducted without the blue team being aware that the test is even occurring. The purpose of the red team is to find vulnerabilities in areas that are susceptible to attack, should a real one occur. The findings from such tests are then leveraged to harden the environment along with bettering any existing policies and technologies to create a higher level of security within the organization. Since the red team's job is to attack, the duty of the blue team is to defend. The blue team understands the company's network, tools, and policies, and works to ensure they all work together to protect the company and its assets. The blue team constantly monitors for abnormalities, and if/when they are detected, they work to mitigate the presented issues. The blue team also focuses on the human element of security by conducting social engineering simulations to test users. Many people have heard the term red versus blue team, but did you know there's a newer definition of a purple team? while the red team attacks and the blue team defends, the purple team is a combination of both red and blue coming together to work as one team. The red team needs to disclose their methods of infiltrating a network or company to the blue team so they can be better prepared for potential future attacks, and the blue teams can divulge how they defended against any vulnerabilities they discovered. This is a true lessons learned exercise that aligns practices from both sides to share their findings, and in turn strengthen the security of the team and its security tactics.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/red-vs-blue-vs-purple-teams?contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)

### Who are the adversaries?

[- The word criminal is a familiar term which means someone participating in nefarious behavior. So now let's align that with cybersecurity and then what we get is a cybercriminal, which is an individual that is conducting this malicious behavior via computers, networks, and even the internet. There is a high likelihood that you have heard the term hacker used most frequently when describing the bad guy. However, that term has many meanings beyond just the negative connotation so often associated with it. What you may not know is there are variety of different hackers, including black hat, white hat, and gray hat hackers. Let's start with the good guys or the white hat hacker. These are the people that look for vulnerabilities and exploit them for the purpose of reporting them to be fixed. Therefore, what they do, while it may seem questionable, is actually done with good intent. You may hear white hat hackers referred to as ethical hackers. They are often employed by an organization to find their areas of exploit before the bad guys do. The opposite of black is white and the opposite of ethical is unethical and this is exactly how a black hat hacker would be described in the most simple of terms. Black hat hackers find vulnerabilities for their own gain, whether it be money, fame, notoriety, or something else. They illegally go around security controls to find vulnerabilities and exploit them before a company can discover what has been done. These are the cybercriminals companies are working to protect themselves against. When you think of a Venn diagram and one circle is black, the other is white, and in the middle where they overlap, would then be the gray. This is a good visual demonstration of what a gray hat hacker is. They are somewhere in between white and black. They may hack into networks to find vulnerabilities without permissions, which is technically illegal. But then, instead of leveraging what they found for their own personal gain, they would report it to the company to help them out in the end, which is a gray area, hence the name. So the next time you hear the word hacker, remember that it doesn't always have the negative connotation that is typically tied to it. As we defined here, there are hackers that are good, bad, and everything in between.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/who-are-the-adversaries?contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)

### Understanding privacy

[- [Instructor] Another aspect of the human element of security is privacy and understanding how to protect your own information. Privacy in the purest sense means freedom from or protection of something. But how does that apply in terms of cybersecurity? Privacy, as related to cybersecurity, is the protection of your information. The main questions around privacy are usually what information of mine is being collected and stored? How is my data being used? And who has access to my data and can share it? Personally identifiable information, or PII, is information that is directly related to an individual that may be used to identify them. This can be broken down into two areas: sensitive, and non-sensitive PII. The best way to describe non-sensitive PII would be to think of it as information that is easily searchable or accessible to anyone should someone go looking. A simple internet search could provide such information on an individual. This includes but is not limited to your name, your birthday, and even your gender. While this information is not worrisome, if anonymized and accessed independently, it can be used to link other information and tie back to an individual, and that is where it becomes an issue of privacy. Since non-sensitive PII is easily accessible information, sensitive PII is information that should not be searchable or easily accessed. Someone should not simply be able to search for this information online and easily find it. For example, you probably don't want your personal medical information easily accessible to the public. So that is sensitive information. This breaks down into a number of categories that include but are not limited to Social Security number, passport and driver's license information, and even credit card and medical information as well. Many new laws and regulations have been implemented to help keep companies accountable for protecting this information. There is a certain expectation of companies to protect our information on our behalf. However, even with regulations and laws in place, it is imperative that individuals take their own privacy and PII, both sensitive and non-sensitive, and hold it in high regard to help add an extra layer of protection against information loss and exposure. You can do this by thinking before you share information, questioning why information requested is needed, removing any social media content that is no longer necessary, and updating your privacy settings, as well as searching your name regularly, and where you can, opting out or removing your information to make it private.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/understanding-privacy?contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)

### Understanding processes and documentation

[- If you're in a high stake situation you're going to want to know exactly what to do and have somewhat of a playbook to follow, right? That's the kind of stuff that makes processes and documentation so important. In addition to all the lower stake situations you may encounter where you need to leverage this information as well. Processes are when you take certain actions to get a defined end goal. In security, having the right processes in place ensures that people know what actions need to be taken in order to achieve the same set of results, like securing the company and its assets. CIA stands for confidentiality, integrity and availability and is a well known model within cyber security. Confidentiality is the work done to keep data secure within the company environment. Integrity equates to trusted, which means the data is reliable and verified. And finally, availability means that the data is available to authenticated users as needed. Another well known area of process is policy. And it is often hard for people to distinguish when a policy is needed versus a procedure, standard or guideline. For example, policies are usually broad in general and don't need updating nearly as often. Whereas procedures are more detailed, step-by-step instructions that may need more frequent updating as requirements change. A policy is defined as a formal statement that needs to be followed by a defined audience. This is usually high level, and doesn't go into the weeds with details. A procedure on the other hand is a detailed document with step-by-step instructions on how to comply with the related policy. Typically, a policy is written first to define the statement and the procedure follows with much more description on the rules to follow to achieve the statement within the policy. Standards also accompany a policy and may be related to an industry standard or an internal company defined technology standard. A policy will determine whether the standard is mandatory or voluntary as well as which groups need to follow the standard. A guideline sets itself apart in that it provides general guidance related to the policies, procedures and standards. It is often more generalized and spelled out in more layman's terms to assist various audiences that the policy may not specifically apply to, but may need knowledge of. While a company will develop their own internal policies, procedures, standards, and guidelines, there are also state and federally mandated cyber security controls and frameworks. These frameworks provide detailed instructions for how to maintain a secure environment and many companies, even if not mandated, will strive to align their requirements with various industry controls and frameworks as best practice. Some of the most well known are GDPR, HIPAA and PCI. After the documentation is in place, you will need to test implementation to verify everything is being followed properly. This is called a security audit. It can be managed internally or externally. This audit is a deep dive into the documentation to confirm that the organization is adhering to the requirements they have established regarding policies, procedures, standards, and guidelines.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/understanding-processes-and-documentation?contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)

### Technical controls

[- [Instructor] Have you turned on the news lately only to hear of the latest company that has experienced a breach? To prevent these types of incident, cybersecurity teams implement controls within their environment so they don't become the next company that you read about in the news. Let's take a deeper look into some of the controls that may be included within the policies, procedures, standards and guidelines. First up is access control, which can be described as who you give permission to allow within your environment. When you think of access control from a physical security perspective, you may think of employees with badges that permit certain people access to the building. And then once inside, the individual may even be prohibited access to certain areas within. This is the same for logical access control. Users are given rights to your network and applications and may be restricted to certain areas. One way to define such access is through an administrative account, which allows for elevated or privileged access. People that are assigned elevated access should only be done so on a need-to-have basis, which leads up to least privilege. Least privilege is when users are given only the minimum access needed in order to complete their required job functions. This is imperative to ensure that people don't end up accessing areas of the network or data that they shouldn't be able to access and doing something with that data or out of negligence or even maliciously. Just as you wouldn't want someone to physically access your data center, you also don't want someone to access your data on your network. So how do you determine what access you have to the network? First, you need to authenticate. Authentication is how you verify who a user is and what all they should have access to. As with physical security being tied to what access you have within a building, your logical access is usually tied to a username. Beyond the username, a user must also know the password as well as possibly even knowing how to get beyond any multi-factor authentication parameters that may be in place. A password is a set of letters, numbers, characters, or a phrase that only you should know that will allow you access to a system when paired with the associated username. Multi-factor authentication, or MFA, or even two-factor authentication is an extra layer of security beyond just a username and password. MFA can be verified based on something only you know, you have or you are. An example of something you know would be an answer to a security question, such as your favorite restaurant, or your mother's maiden name. Something you have would be something such as a security token or a badge. And something you are could be your fingerprint, retina or face. While there are other ways to utilize MFA, these three are the most common.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/technical-controls?contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)

### Secure practices, terms, and exercises

[- [Instructor] Technology is often the most talked about and most considered side of security. Let's walk through a few definitions of terms often used when describing how to secure environments. First up is encryption. Think of encryption as a secret code that one needs to decipher in order to understand the true meaning or gain access, and more specific to security, it is data, such as passwords, messages, and even payment information. A good visual for this is to think of encryption like a decoder ring toy. You have a message that you want to get to your friend, that you don't want anyone without the decoder ring to understand. So it becomes a secret message. This is the same with encryption. In that once encrypted, only the right people with the right technologies can decrypt the content. Most companies will require encryption of secret or confidential files, especially if being shared outside of the company. However, not everything is encrypted by default. If something is not encrypted, it is known in the industry as cleartext. Often you'll hear cleartext when someone is referring to finding or storing of passwords. To refer to the previous decoder ring example, this would be like sharing a secret message but forgetting to put it in secret code. So anyone that finds your message would be able to read it and use the information. Computer or digital forensics is when a person or team is tasked with uncovering information on a system or network, usually for the purpose of a court case or investigation. Computer forensics can be thought of almost as detectives looking into evidence in a case. Just as detectives in a real case would look through physical evidence, computer forensics is tasked with looking through digital evidence. These teams often deploy a lot of tools to recover data or pull it as needed. Some of these tools may even include description techniques if data needed has been encrypted. Next step is penetration testing. A good way to think of this is similar to how car manufacturers intentionally crash their cars with dummies inside in order to find any issues or flaws so they can build their cars to be more safe. In cybersecurity, penetration tests are done by a network to find flaws or vulnerabilities in a controlled environment before cyber criminals find them and exploit them. Findings from such tests allow networks and environments to be hardened in order to create more security.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/secure-practices-terms-and-exercises?contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)

### Network controls

[- [Instructor] When you think of your own personal people network, it is typically people with a common interest that you communicate with in order to help you complete tasks or leverage to gain something from and vice versa. When you use a computer such as in a work environment, you are communicating and sharing information via your company's network. A network is a set of computers that leverage the same set of resources and are able to communicate due to a set of common technologies. A virtual private network, or VPN, is almost like a tunnel you can turn on and off when connected to a public network. This tunnel, when turned on, serves as a way to encrypt data being transmitted, which in turn is an extra layer of security when utilizing public wifi. Your company may require use of a VPN in order to access certain information within your company environment. When you consider the physical security of a company building, one layer of security that may be in place is a security guard. This guard is there to monitor people coming into and out of a building, and verify they have the correct permissions to be there, usually by looking at their badge credentials. A firewall serves a similar purpose in digital means by monitoring both incoming and outcoming traffic on a network and not permitting access if access is not authorized. Just like criminals can find ways around physical security controls, cyber criminals have been known to exploit firewalls in order to gain access into the network as well. Utilizing VPNs and firewalls are one way to protect yourself and your data, but there are a number of others. While we can't cover them all, we will define a few. Next up is antivirus. One can think of antivirus similar to when someone goes to the doctor, either because they are not feeling well or just as a wellness checkup to ensure everything is in order. The doctor will do a scan and check your body, and if something is found, notify you, and perhaps make recommendations to help fix the issue. Antivirus is similar, and that it is placed on a device with the purpose of scanning the device, either automatically or on demand for malicious malware and viruses, notifying the user of what has been found, and even sometimes giving advice for how to remedy the issues that were discovered. When it comes to securing a network and/or devices, there is no one size fits all, and the amount of tools and technologies out there is enumerable. We only covered a minuscule amount of what can be done to create a secure environment. So I encourage you to continue to research additional methods for protecting yourself and your information.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/network-controls?contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)

### Advancements in technology

[- [Instructor] So often, it is said, "Save that to the cloud," or "That is in the cloud," but what does in the cloud really mean? According to Microsoft, Cloud computing is the "delivery of computing services, including servers, storage databases, networking, software, analytics, and intelligence over the internet to offer faster innovation, flexible resources, and economies of scale." Next is Artificial Intelligence, or AI. As humans, we are able to think and make intelligent decisions, as it is human nature to be able do so. AI is when computers, robots, and machines have the ability to make decisions in a humanlike way, because they have been designed in such a way to mimic human thought processes. These technologies are programmed in a way to align with human intelligence, but taking it further is complicated. As Inc put it, "While AI can learn the 'how' to just about anything better than a human, it does not have the curiosity to ask 'why.'" And that is the true differentiator between human and artificial intelligence. Similar to AI is machine learning. And just as humans can learn so they develop new skills, so can machines. Machine learning is part of AI, and it leverages data to develop, learn, and grow over time. Just as we as students go to school to learn based on curriculum we are given, machines are also taught based on very specific information they are given. According to IBM, "Machine learning is a branch of artificial intelligence and computer science which focuses on the use of data and algorithms to imitate the way humans learn, gradually improving its accuracy." As defined by Investopedia, "A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend." A defining feature of cryptocurrency is that they are generally not used by any central authority, rendering them theoretically immune to government interference or manipulation. There are many types of cryptocurrency with new ones being added, which include Bitcoin, Ethereum, and Litecoin. While cryptocurrency continues to grow, it is also an area of contention and has not been as widely adopted as some may have anticipated.](https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/advancements-in-technology?contextUrn=urn%3Ali%3AlyndaLearningPath%3A650398af498eb8976fcc93ca&resume=false)