## Defining Cyber Security

In this video, we're going to be looking at what cybersecurity means. You may have come across a number of different terms which are used synonymously to mean the same thing. These might include information security, cybersecurity, and computer security. The reality is, there is a distinction. Cybersecurity relates to the security of any device which is connected to some form of network, such as the internet. Information security is wider than computer security because it relates to the security of any information, whether that be physical or held on a digital device.

Then you've got computer security, which relates to the security of any computing device. You'll see that there is some crossover between these different terms, and some people use them interchangeably. For our purpose, we're going to be referring to cybersecurity, as this encompasses most of the devices which are used in modern practice. Cybersecurity is often thought of as a technological solution or a range of technological solutions--

so things such as encryption. But the reality is, it's much more complex than this.

We have the human element as well. Humans intentionally or unintentionally can make things more difficult in terms of security. For example, if you consider user authentication, where passwords are known to be written down in plain sight due to the difficulty that the end user has in retaining that information. As a result, the mechanism itself becomes less secure. So you can see how challenging it can be around ensuring the security of a system. You should think of security as a cyclical process.

Prevent, detect, and respond is generally the stages within that process. Try to prevent any attacks. Try to detect any attacks which are happening or have happened. And then respond to those attacks, perhaps by incorporating more mechanisms or including things such as security training or policies which can also impact the security of a system. In approaching cybersecurity, generally an enterprise does this in a risk management form. That is, they identify their assets, such as a data set.

They determine the potential risks and threats which are posed to that--

so, for example, unauthorised access. And then they determine the kind of mitigation techniques that they want to implement to mitigate that risk. Obviously, any enterprise has a limited number of resources, whether that be money or space on servers--

those kind of things. As a result, they have to determine what is most important to them, and a risk management approach allows them to do this. People also impact the process. We need to consider the challenges around those aspects and the balance between the usability of a secure system versus the security of that system, and trying to get that balance right can be really difficult.

So overall, it's a very complex picture. To make it a little bit easier, generally in information systems, we look at security trying to maintain three properties, referred to as the CIA Triad. C stands for confidentiality, I for integrity, and A for availability. Generally, when we're talking about security of a system, these are the three properties that we're trying to maintain. Confidentiality is where information should be kept confidential from unauthorised parties. For example, if you visit your GP and have some medical issues documented, the doctor's surgery is required to ensure that that is kept confidential from unauthorised parties.

Integrity is where you want your data to be correct. You don't want someone to go in and amend that in an incorrect fashion. If we go back to the example of the GP surgery again, you wouldn't want somebody going in and changing your medication to something that it shouldn't be. So again, we're coming back to the idea of unauthorised parties changing information or accessing information that they shouldn't have access to. And finally, we have availability. The data should be available to legitimate users at a time which is expected to have access to.

One example of this could be a bank unexpectedly being hit by a denial of service attack. In which case, the end user would not be able to access their funds, which could cause some distress as well as obviously impact the bank's reputation, which is undesirable. There is a range of different terminology within the field of computer security or cybersecurity. These terms are important to know moving forward so that you can understand the terminology, and you're not getting distracted by that whilst building up your understanding of other areas.

One aspect is the bad actor or the threat actor, or perhaps sometimes the malicious actor or hacker--

although that tends not to be a term used within the field. It's more of a media term--

as well as just the attacker. This is an insider or an outsider. So that is someone who is legitimately part of the system or someone who is external to that who is trying to impose some form of harm on the system--

so to gain unauthorised access to a system that you shouldn't have access to.

You've also got the idea of malicious versus nonmalicious. Malicious is where someone sets out with the intent of causing harm, and nonmalicious is where someone unintentionally compromises the security of a system--

for example, writing down a password and storing it somewhere that can be easily found by someone who shouldn't have access to that. We've also got the idea of vulnerabilities, threats, and attacks. A vulnerability is a limitation of a system which opens it up to exploitation. A threat is something or someone which is constantly posing potential harm to an asset, such as a data set. And then you've got an attack. So this is an attempted exploitation of a particular vulnerability of a system.

You've also got the attack surface, which is the collection of all the different points of entry an unauthorised attacker could try to exploit. From there we have attack vector, which is typically referred to after an attack has taken place and is the particular path that the attacker has taken in order to gain unauthorised access. So you can start to see how we've got such a vast amount of terminology, but hopefully that gives you sufficient to start moving forward with the field. Another aspect to consider in cybersecurity is, of course, laws and regulations.

Within the UK, there are a number of laws and regulations which impact cybersecurity, specifically relating to computer crime and information security. Some of these include the Computer Misuse Act, the Serious Crime Act amendment which revised the Computer Misuse Act to affect more modern landscapes, and the Data Protection Act 2018, which is the UK implementation of GDPR. We won't go into these in depth here, but if that is something that interests you, there are loads of resources on the internet where you can find out a little bit more information on those.

But these obviously set out the requirements for aspects such as the security of information. Hopefully, you now have have built up some appreciation for the many different facets of cybersecurity and what a complex process it can be. We've tried to highlight the process and the fact that it's an iterative process that we continue to monitor and build on as needed. We've covered the fundamental properties which we try to maintain for the security of system; confidentiality, integrity, and availability.

We've covered key terminology, as well as introduced some of the regulations and laws which impact on security within the UK. You're now in a strong position to start to explore security in more depth. I hope you've enjoyed the video, and I'll see you next time.