Understanding of cyber security and risk of exposure or loss resulting from a cyber-attack or data breach in your business including malware attack and ransomware.

What is Cyber Security?

There are lots of great things that come with having access to the world wide web. However, there have been problems with the virtual world that have arisen over time. One of these is cyber attacks.

Cyber attacks can happen at any point in time, to anyone and they are not only a risk to information, data and security; but they can also be a financial issue too.

This is where cyber security can help. The idea of cyber security is that individuals and organisations take charge of reducing the risk of facing a cyber attack. It covers a range of devices, essentially any that can get online and is there to ensure that the chance of a cyber attack is as low as possible.

Why is Cyber Security Important?

As we have already covered, cyber attacks can happen when you least expect them. This is why cyber security is important. It safeguards all types of data and ensures that it doesn't get into the wrong hands.

This ensures health information, information that will identify a person, intellectual property, personal information and also any government information too. It covers a wide range of sensitive data.

Whilst it can't always stop a cyber attack, what it can do is formulate a plan which will offer a response to attacks and try to lessen their impact.

The risks associated with cyber activity

Whilst much of the activity you have online is going to be positive; there is always a chance that something will go wrong and you will be faced with an issue. There are lots of different issues that can arise, however, here are some of the most common risks associated with cyber activity.

- Ransomware
- Phishing
- Hacking
- Data Leakage
- Insider Threats

These all happen in a different ways and can have a different impact on your business or you as an individual.

What are the Different Types of Cyber Security Threats?

We have already looked at some of the different types of cyber security threats, however, let's take a look at them in more detail and also learn more about some of the other threats out there that you can come across.

Advanced persistent threats (APT)

An advanced persistent threat is a sophisticated and sustained cyber attack which allows an intruder to infiltrate a network, completely undetected. They can then steal a variety of sensitive data, although this will often happen over a prolonged period of time rather than in a one-off attack.

Distributed denial of service (DDoS)

We all know how irritating it is if we cannot gain access to a website that we need. The very idea of distributed denial of service is to cause this form of annoyance. The attackers will cause a flood within a server, made up of internet traffic. This internet traffic will then block other users from being able to access the services and sites that they need. Causing an issue not only for the users but also for the businesses too.

Malware attack

Malware is one of the most commonplace forms of cyber attacks. They cover a variety of different programmes that are malicious in their nature (hence the name). They are delivered and installed onto the systems and servers, more often than not to the end-users. They are designed to cause maximum harm to the singular computer, the server that it runs on or a more extensive computer network. More often than not, malware will be used to obtain data that can be used for financial gain.

Man-in-the-middle attack (MitM)

As the name suggests a man-in-the-middle attack is a cyber-attack where the threat puts themselves in the middle of two parties. This will often be the end-user and the business-owned application too. The actor, the middle-man, will use their position to intercept any communications that run between them and therefore also the data that is exchanged. This data can then be used either to hack the end-user or perhaps to make purchases using their financial information.

Password attacks

If a password is used to access a website or an app, then there are hackers out there who try to find out how they can guess them and then use them to gain entry to a variety of apps and secure websites. Password attacks can come in a variety of forms, they can be brute-force attacks, stuffing with credentials, dictionary attacks and password spraying.

Ransomware

Ransomware is a specific form of malware. It is designed to stop a user from being able to access files that they need on their network or computer. It does this by encrypting the files and the information that it contains and then asking the user, or the network owner to pay a ransom in order for the decryption key to be given to them.

Social engineering attacks

In social engineering attacks, the attacker will use manipulation to essentially fool the user to give out sensitive and confidential data that they can then use to their advantage. This will often be targeted at people who are more vulnerable and therefore are going to be easier to trick.

Software supply chain attacks

In a software supply chain attack, the cyber attacker will use their attack method to infiltrate the network of a business or organisation. They will then send out a code that is malicious in its nature and the business or organisation will then send it out to their customers, unknowingly. This code will then be able to gain access to the data of the customer.

What are the three pillars of cyber security?

In order for cyber security to work and to offer protection of the data for the end user and the original user it needs to follow the three pillars of cyber security. These are people, processes and technology.

People

The people pillar is where there is often the highest risk. This is where human errors occur and where misjudgements can also be made. These will then cause a cyber attack to be able to be successful and cause a harmful impact on the end user and the business or organisation too.

Processes

A process is what will ensure that the people who use the system are going to do the right thing. They are set up to provide the guidance and training that these people can then use to help them to be successful in protecting themselves and their organisation from any threats.

Technology

If you want to be able to manage a cyber attack risk, then you are going to need to rely on technology. However, it is not all about investing in the most expensive technology to do the job, it is more about knowing how best to use it to protect yourself.

Information security model

Not everyone is going to be an expert in cyber security, which means that they are going to need to have help to work out what approaches are going to be the right ones for them to take. This is where an information security model can help. These outline how security should be organised and how it can be governed to give the best security possible.

There are three main aspects of this model to keep in mind. Availability, confidentiality and integrity.

Availability

Availability means that any key information should be accessible to the parties that are able to access it and that need to access it. The key aspect

of availability is to maintain the hardware within the cyber set-up and to ensure that technical infrastructure and systems that will display the information.

Confidentiality

The term confidentiality means that certain information is kept private and is recognised as being sensitive. This means that unauthorised access is not allowed and that it should have a low chance of getting into the wrong hands. The nature of the data will often change the level of confidentiality that is needed to be applied.

Integrity

Integrity ensures that the data is kept accurate and consistent as it moves through all the channels. It must not be changed or altered throughout the process.

Risk protection and reduction

It is great to have so many different devices that are now able to help us to connect to the internet and keep us mobile. However, with all these devices, comes a variety of issues that are going to need to be addressed.

Computers

For computers, the main aim is to protect the computer system. This means that they are not going to be harmed in any way, used in a way that is unauthorised and also protected from theft too. More often than not a computer will be password protected and it may also be placed in a spot that is out of site.

Laptops

Laptops are more mobile than computers, which brings about another risk; theft. Laptops that contain sensitive information should always be password protected (all laptops really can benefit from this) and many can be encrypted for log too. Laptops should also be protected when they are out and about, it is a good idea to carry them in a bag and always have them with you when you are out and about with them.

Network devices

One of the best defences that we have against cyber attacks on network devices is to ensure that they are password protected. You want to remind users what makes for a proper password and also encourage things such as two-factor authentication.

Smartphones

Smartphones should always be password protected, either by Face ID, fingerprint scanning or with an access code. Passwords should not be stored on the phone where someone can gain access to the information and then use this to log into apps.

Tablets

Much like smartphones, tablets will also need to have access protection on them as they are mobile and portable too.