Cyber Security Trends to Look Out For in 2019

Due to the nature of the industry, Cyber Security evolves at an incredibly fast pace. Technologies such as AI and VR which seemed so futuristic just a few years ago are being executed in everyday technology today.

The overlying reason for the fast pace of the industry is the arms race between cyber criminals on one hand and governments and business' on the other. More sophisticated and advanced cyber threats and attacks are emerging daily. As a result, our cyber security professionals must keep relentlessly defending our data and infrastructure trying to keep ahead.

On top of this, new legislations such as GDPR place importance on the protection and sharing of our personal data, encouraging business' to prioritise cyber security and spend more to help the company, thus helping the industry to mature.

With all this in mind, here are our top cyber security trends to look out for over the coming year.

Crypto - theft

As 2017 saw the boom in crypto currencies, 2018 saw the increase in crypto - theft. With this still relatively new form of currency comes an abundance of cyber threats. As crypto - currencies are traded online, through untraceable and anonymous ways, they are particularly attractive to cyber criminals. According to the cyber security company Carbon Black, roughly $1.1 billion worth of crypto currency was stolen in the first half of 2018. So if 2018 is anything to go by, we will likely see a increased trend of crypto - theft.

Multifactor Authentication will gain wider adoption

After global companies and e-commerce sites such as Amazon have adopted this new technique to protect their users data, multifactor authentication is becoming increasingly popular. Through the simple adaptation of two forms of identification to log into an account, the security of this account has drastically improved.

AI will be used to benefit security solutions

With companies such as Darktrace achieving global success, companies of a similar vein are likely to follow suit. As the number and range of threats continue to grow, it is clear that AI can be a successful tool to help counter them. Given the spread of AI in general at the corporate level, it will continue to grow in the security segment as well.

Biometrics will continue to replace passwords

With Apple's Iphone continuously using fingerprint recognition and face recognition, the use of biometrics instead of passwords has become increasingly mainstream. Due to the efficient and secure nature of this technology, companies (predominantly financial companies) are researching and testing how this can benefit themselves and their customers and clients.

IoT will continue to be a major source of vulnerability

Products such as Amazon's Alexa and Google Home, are beginning to become a common household item. However, as many are aware, the security of these products are often poor and the amount of personal data they hold is unsettlingly high. As a result, until the security and protection of these devices dramatically increases, they will remain a major source of vulnerability within homes and companies.