Cyberattacks in the healthcare sector

The number of organisations within the medtech and healthcare sector that have been targeted by cyber security threats continues to grow. Because of the sensitive nature of the healthcare industry, such attacks can be very damaging not only from a financial and organisational viewpoint, but also from a personal perspective.

The wealth of data in the form of patients' personal details held by hospitals and healthcare organisations makes them an obvious target for cyberattacks, but medtech innovators developing new technologies are also likely to be the focus of hackers looking to obtain commercially sensitive and valuable information.

The motivation behind cyberattacks can be varied, with some data stolen, particularly from large healthcare institutions, and ransomed for large sums, while other details are stolen with the specific intention of targeting individuals with scams and fraud. These attacks can be carried out by individuals, organisations and nation states.

Effects of cybercrime

The effects of such activity can be far-reaching and varied. Financial loss experienced by companies and health organisations may be the result of direct theft; the loss of commercially sensitive and valuable information; industrial monies paid out to hackers demanding ransom for the return of data; or fines issued by data protection agencies for security breaches in the storage of personal information.

Organisations who are the victims of cyberattacks may experience significant reputational damage, particularly if the breach is widely publicised. Such activity may also cause severe disruption to productivity if internal systems are compromised.

On a personal level cybercrime can have a damaging impact on individuals' physical and mental wellbeing as well as their finances, if it results in clinical treatments having to be cancelled or postponed or they become the targets of hackers because of identity theft.

Methods of attack

Many different methods are used to initiate cyberattacks. Some of the most common include malicious network traffic, whereby access to a system is achieved via an app or web service with the intention of carrying out malicious activity such as installing software to cause damage or disruption. Man-in-the-middle attacks occur when a device is manipulated to allow control by an unauthorised third party. System access can also be gained by 'phishing' exercises if users are persuaded to click on a link or upload pertinent data, allowing the hacker to gain entry.

Once access is gained the perpetrators may carry out various criminal activities including identity theft; scams relating to a patient's condition; medical device ransom where devices are shut down and reactivated only when payment is received; malicious disruption; commercial espionage; and theft of intellectual property.

The effect of Covid-19

The pandemic created an ideal opportunity for cybercriminals. During the first month of lockdown in the UK there was rise of approximately 400% in the number of scams. One of the reasons cited for this increase is that organisations were under intense pressure, resources were stretched and attention was very firmly on managing the immediate situation. Recognising this, cyber criminals were quick to take advantage. Organisations within the healthcare sector were an ideal target because of the importance and urgency of developments and innovations to help in the fight against COVID and the increase in the use of digital technology in the industry.

Minimising the risks

Cybersecurity should be a high priority for all organisations, especially for those holding sensitive personal data and valuable technological intelligence. Identification of risk through careful monitoring; good maintenance and prompt updating of software; strict adherence to device security; and effective training of those using the systems to recognise threats and understand the importance and sensitivity of data, can all go some way to minimising risk.