Modern day robbery:
Will your practice survive a cyber-attack?

Lloyd & Whyte

What is a cyber-attack?

A cyber-attack is an intentional or malicious attempt to damage, leak or steal sensitive information from a computer network. This is usually achieved by attackers gaining unauthorised access to a system, or intercepting emails between practice team members.

Types of cyber-attacks include:

- Extortion - an attacker's threat to destroy a system or leak stolen information if ransom demands are not met
- Denial of service - the temporary or indefinite disruption of services after an attacker prevents legitimate users from accessing the system
- Phishing - the malicious disguise of hacking, leading victims to believe that links or personal data queries sent to them via email have come from a trustworthy contact
- Theft of electronic funds - the interception of communications, allowing a hacker to gain unauthorised access to a bank account or the victim's bank details.

How could your practice be affected?

It's easier to believe that an attack won't happen to you, which is probably why only 27% of businesses in 2018 opted for a formal policy that covered their cyber security risks. Yet government research has revealed that, between 2017 and 2018, nearly half of UK businesses suffered a cyber-attack.[1]

If your practice is targeted in a cyber-attack and sensitive data is leaked or stolen, it's possible that the everyday running of your practice is going to be disrupted. At worst, disabled access or damage to your system could bring patient care to a halt completely.

How common are these attacks?

Out of the five most likely global risks expected in 2019, two of them are data theft or fraud and cyber-attacks.[2]

In this digital age, advanced methods of hacking and electronic theft leave systems exposed to the dangers of cyber. No matter the size of a practice, the problem lies in its technological vulnerabilities - many of which, attackers are happy to exploit.

Although IT security serves to protect a system from these vulnerabilities, the determination of attackers can go beyond the usual protective barriers. If this is the case, Cyber Insurance ensures that your practice is protected if it is targeted. But before anything, it's important to think about ways in which you can prevent an attack.

Can these attacks even be prevented?

Not every single attack is preventable, but to keep your practice as secure as possible, you can receive guidance on cyber security by following the Cyber Essentials scheme*. This is a platform for government-approved advice, which outlines security basics such as keeping a secure internet connection, controlling access to your patient data and regularly updating your software.

> "Out of the five most likely global risks expected in 2019, two of them are data theft or fraud and cyber-attacks."

Raising awareness about the threats posed by a cyber-attack is also a good idea. Educate staff about good practice with regard to data handling, and make sure they are aware of email and telephone scams. As well as that, share communications from the Information Commissioner's Office about cyber developments.

*Cyber Essentials scheme: www.cyberessentials.ncsc.gov.uk

Turn over for: Examples of cyber-attacks/events & areas of cover. >>>

What can Cyber Insurance do for your practice?

For the times when prevention isn't enough, Cyber Insurance can help you in the aftermath of an attack.

Here are some key areas of cover:

Type of attack / event	How could Cyber Insurance help?
Cyber extortion	Covers costs of the ransom, reinstatement of data and restoration of IT systems
Network failure	Covers income lost and additional expenses
The theft of patient information	Press coverage from media experts on behalf of practice
Network / privacy breach	Covers notification and legal costs in the event of third party data breaches

A few examples of cyber-attacks…

Ransom & cyber extortion:

At a private practice, a hacker gains access to the healthcare system and corrupts the patient data. This sensitive data contains the home addresses, contact details and medical records of patients. The hackers contact the practice and demand a ransom of £30,000. They say they will decrypt the data in exchange for the ransom money.

If this happens to you, will you know who to call?

Invoice fraud:

A practice pays an invoice of £15,000 to their usual medical supplier, and confirms this via email. The medical supplier contacts the practice, telling the manager that they haven't yet sent the invoice. They soon find out that a fake invoice had been sent to the practice, and the money had been paid to the hacker's bank account.

How will you cope in this situation?

Do you assume that it's your own fault?

Fraudulent bank transfer:

At a mixed practice, the manager receives an email from an employee stating that their bank details have changed. The manager authorises this. When payday comes, the employee asks the manager why they haven't yet received their wages. The manager refers to the employee's email, but the employee denies ever sending such an email. They soon discover that the email system had been intercepted by a hacker, and the employee's wages had been transferred straight into the hacker's account.

What happens next?

How will you compensate for this loss?

Have a back-up plan

For advice on arranging Cyber Insurance, contact us today:

Call: 01823 250760 ■ Email: info@lloydwhyte.com

Visit: www.lloydwhyte.com/aopcyber

In proud partnership with

Association of Optometrists
Affinity Partner

Insurance Brokers
Chartered

*[1]Department for Digital, Media & Sport - Culture Cyber Security Breaches Survey 2018. Based on a survey of 1,519 businesses.
*[2]World Economic Forum - Global Risks Report 2019 (14th Edition).