FACT SHEET

HAMILTON FRASER Cosmetic INSURANCE

Protecting the things that matter most

Why are cyberhackers attacking cosmetic practitioners?

We're all familiar with news stories reporting cyber-attacks on banks and big businesses - but cosmetic practitioners should not underestimate the interest online criminals might have in their businesses, or the chaos a cyber incident could cause.

Over the last few years, there have been several troubling reports of cosmetic surgeries and clinics being targeted by hackers, stealing or encrypting patient information with malware in order to blackmail for a ransom.

For example, the Susan M. Hughes Centre, a provider of aesthetic medicine and cosmetic surgery services in the US, discovered ransomware had been installed on its computer system in August 2016. Over 11,000 patients were impacted. Fortunately, the centre had a backup system in place which ran whilst action was taken to isolate the incident, and an external cybersecurity firm has since conducted a forensic investigation.

Closer to home, information was stolen in 2014 from servers belonging to the Harley Medical Group, which operates 21 clinics across the UK. Extracted from a website enquiry form, the theft involved up to 480,000 potential clients' contact details and the procedure they were interested in. A statement from the company made it clear that the criminals' motive was to extort money from the Group. The attack not only breached security but raised concerns that such sensitive private information could also be used to blackmail individuals.

In 2014, the FBI estimated that the extortionists behind one particular strain of ransomware, named CryptoLocker, extorted $27 million in blackmail money from victims in just six months. Expensive and disruptive for any business, digital extortion is particularly worrying for clinics and organisations which store patient records including drug histories and health information, as it could seriously disrupt operations and even damage patient health.

FACT SHEET

HAMILTON FRASER Cosmetic INSURANCE

Protecting the things that matter most

"If you have patients, you are going to panic way quicker than if you are selling sheet metal," points out Stu Sjouwerman, CEO of the security firm KnowBe4. So what can you do to protect your establishment from this wave of cyber-crime?

- **Knowledge is power** – Ignorance about the risks cyber-attackers pose to clinics, and failing to focus on cyber-security and training, contributes towards making establishments easy targets.
- **Back it up** – Back up your data, and do it regularly – every day is best. Being threatened with not being able to access your company records is less of a worry if you've got a copy of everything from the day before.
- **Watch where you click** – Never open suspicious emails or links, and watch out for fake adverts. Train staff to right click on email attachments and scan for malware before opening, whilst installing ad blockers on your internet browsers can thwart "malvertising".
- **Take security measures** – Use a security product, make sure your Wi-Fi and business networks are kept private, and keep Java, Flash and other plug-ins up to date to avoid hackers exploiting known weaknesses.
- **Suspect an attack?** – Here's what to do. Immediately disconnect all company computers from the corporate network, disable Wi-Fi and Bluetooth on all machines, and halt all network operations to prevent the malware spreading. A pre-prepared action plan will ensure business operations can continue as best as possible, so it's a good idea to write one before anything happens.
- **Have a contingency plan** – Whilst Business Interruption insurance might offer some protection for your organisation against loss of profits, dedicated Cyber Liability insurance can include specific benefits such as covering cyber ransoms, legal costs, compensation paid due to lost data, and more.

Call us on 0800 63 43 881 to find out more.

For more resources and advice, please go to our website
www.cosmetic-insurance.com