HOW IS YOUR BUSINESS DEALING WITH THE CYBER THREAT?

CHAMPION
insurance brokers

HOW WOULD YOU REACT IF:

1. You came into work and were told that someone had breached your system and accessed your data. What would you do?

2. Someone hacked your business and started putting out messages on social media. How would you stop them and repair the reputational damage?

3. You switched on your computer and there was no response, except for a ransom demand. Who would you call, and would you pay? What would you say to your customers and employees?

4. Cyber criminals accessed your banking passwords and transferred funds out of your business bank account.

FACT:

"In 2017 45% of all businesses were hit by at least one cyber attack with average costs for UK businesses ranging from £25,000 for smaller businesses and £385,000 for companies with 1,000 employees or more."

Source: Hiscox Cyber Readiness Report 2018.

THE DIFFERENT TYPES OF CYBER CRIME

Cyber crime is getting increasingly sophisticated and takes many forms including:

Phishing or social engineering is an attempt to dupe your business into transferring funds to criminals as a result of fraudulent emails purporting to come from employees, directors, customers or suppliers.

Whaling is an attempt to land a big fish, such as a CEO, with a sophisticated scam, such as paying a large sum for a fake acquisition.

Hacking is where a hacker gets into your business files or server and gains information.

Cyber extortion is where a hacker enters your computer and disenables your business files, demanding a ransom, usually in Bitcoin, to reinstate them.

Denial of Service (DoS) Attack is an attempt to bring a website or network to a standstill by flooding it with data requests.

Virus is a small program designed to cause trouble by gaining access to your device, it usually self-replicates after hooking into your system.

Malware is a general term for malicious software, such as WannaCry and NotPetya. It can include ransomware, spyware, worms and Trojans.

E-Theft is where cyber criminals breach your systems and steal funds from your bank account.

FACT:

"According to Action Fraud the cost of phishing attacks to UK businesses in 2016-2017 was £32,200,000 and is the third most common way that criminals defraud a company."

WHAT IS CYBER INSURANCE?

There's a lot of confusion about cyber insurance, why it might be needed and what it actually covers.

To start with, ask yourself which part of your business is not reliant on a digital system. If a cyber attack meant this was the only functioning part of your business, what could you do?

The answer is, probably, not much.

That's what cyber insurance is for, to keep your business running in a world operated by digital systems and increasingly threatened by cyber attacks. It also provides protection for your company if it is held accountable for allowing your customer data to be compromised.

WHAT DOES CYBER INSURANCE DO?

If your business is reliant on digital systems, you face significant financial, operational, reputational, legal and regulatory risks without cyber cover.

A cyber insurance policy can be tailored to your business's individual risk profile, providing cover against:

- hackers stealing or encrypting data and demanding a ransom to release it
- fines and penalties you may occur if you are assessed as being non-compliant with the new GDPR rules
- viruses that paralyse systems, and the income lost while they are being restored
- accidental loss of data, followed by legal action brought against you by those parties affected
- your business bank account being targeted by hacking or phishing
- lost income or additional expenses incurred as a result of downtime after a data breach

CORE COMPONENTS OF CYBER COVER:

Cyber insurance is constantly evolving but a good cyber policy will include some or all of the following covers:

Breach costs

The cost of removing the hacker or virus/malware, notifying affected customers, offering credit monitoring and bringing in forensic teams.

Damage to data or programming

The cost of restoring affected data or security programmes.

Network failure

Covers business interruption losses arising as a result of breach or network failure.

Cyber extortion / ransomware

The costs of any extortion or ransomware payments associated with the attack.

E-Theft

To indemnify you after funds have been stolen from your bank following a breach of your systems.

Network security, privacy and confidentiality liability

Covers your liability if you are sued by affected customers, vendors or employees in the event of a data breach.

Regulatory

Legal costs incurred if you have to comply with regulatory action taken as a result of a breach.

Multimedia liability

Breach of copyright, libel or slander, plagiarism or defamation if you are sued as a result of information appearing on multimedia channels, such as Twitter, Facebook or websites.

Cyber Terrorism

Losses caused by individuals, groups or governments acting for political, religious or ideological purposes, causing disruption of your computer systems.

Payment card industry

Fines incurred due to failure to properly follow PCI security standards.

MYTHS SURROUNDING CYBER COVER:

We back-up on the Cloud, so our systems and data are secure.

When it comes to data, there's no such thing as secure. For example, data was wiped from one of Google's data centres in Belgium after the local power grid was struck by lightning four times. Some customers permanently lost access to their files. Google said it was totally responsible for the outage and urge customers to back-up their back-ups.

I'm covered under my existing insurance.

Most existing insurance policies do not cover the full range of cyber threats. For example, an employee notices their corporate Twitter feed is broadcasting pro-ISIS propaganda. It's been hacked by an ISIS affiliate. Luckily, the company has cyber insurance, and a team of forensic experts is called in. They are able to restore the security of the client's website, email system and Twitter feed.

Cyber cover is expensive.

Not taking out cyber cover could also be expensive. For example, in a cyber attack, 100,000 customer records are compromised. You have to write a letter to each one, advising of the situation. (After such a data loss, you can't email.) At 70p per first class stamp, that's £70k, before you even look at legal costs. When all costs are tallied up, the average cost per lost record is £110. You are also fined for breaching the new GDPR legislation.

I'm an SME. It wouldn't be worth anyone's while to attack my business.

SMEs have few processes and are particularly vulnerable to human error. For example, an employee responds to an apparently genuine email request from a trusted source for confidential employee tax records and other information. Hackers have 'spoofed' the 'From' line of the email and it is fraudulent. The employee responds in good faith, clicking the malicious link and sending the names, addresses, employment status and tax records for every employee to the hacker's email account.

My business doesn't hold customer data, such as names, addresses or banking information.

A Denial of Service (DoS) attack could paralyse your website and a 'ransomware' attack could lock your system until a release fee is paid. For example, an employee clicks a link in an apparently innocent email, releasing a virus that encrypts over 12,000 company files. Hackers demand £3,000 in exchange for decryption. The virus is impossible to remove and the company has to pay. In addition, they can't trade during the breach.

CONTACT:

If you require any further information about our products or services please contact us on 03330 430 430.

Telephone: 03330 430 430

Email: info@champion-insurance.co.uk

www.champion-insurance.co.uk


CHAMPION
insurance brokers