The monster in the digital shadows: **why businesses need cyber insurance**

> *In the vast expanse of the online world, where every click, swipe and tap can open doors to both opportunity and risk, there lurks an insidious monster—cybercrime. It's a constant threat that preys on the unwary, exploiting vulnerabilities with cunning and precision and for businesses, it's not a matter of if they'll be targeted, but when - as Matthew Collins, Director at Chelmsford-based Ascend Broking Group, explains.*

CYBERCRIME is not merely a nuisance, it's a formidable threat that can wreak havoc on businesses of all sizes. In the UK alone, cybercrime cost the economy an estimated £21 billion in 2023, and the figures continue to rise.

32% of businesses in the UK have experienced security breaches or attacks, with medium and large businesses facing even higher odds. And with the average annual cost of cybercrime per victim estimated at £15,300, the financial repercussions of a cyberattack can be devastating.

Not only do they bring about financial or data loss, but a cyberattack leads to business interruption, damage to reputation and an erosion of trust from customers.

So, what types of attacks are out there?

From sophisticated hacking schemes to deceptive social engineering tactics, cybercriminals employ a myriad of techniques to infiltrate systems and exploit unsuspecting victims.

Here are some examples:

- **phishing attacks**
- **malware (viruses, ransomware, spyware)**
- **hacking**
- **identity theft**
- **online fraud**
- **denial-of-service (DoS) attacks**
- **cyberstalking**
- **social engineering**
- **insider threats**
- **data breaches**
- **BEC (Business Email Compromise).**

Quite a list! And it's a list that's growing all the time, as the monster at the door continually comes up with new ways to defraud your business. So, what do you need to know in order to protect it?

One of the most effective weapons in the cybercriminal arsenal is social engineering, a tactic used in almost 90% of all data breaches. Whether it's a seemingly legitimate email from your bank or a too-good-to-be-true offer, cybercriminals excel at manipulating human psychology to gain access to sensitive information. And, as the government acknowledges, combatting social engineering attacks is a top priority in the ongoing battle against cybercrime.

But the responsibility doesn't rest solely on the shoulders of authorities. Businesses must also take proactive measures to defend against cyber threats.

Businesses should consider:

- **implementing robust cybersecurity measures such as firewalls, antivirus software and intrusion detection systems**
- **regularly updating software and operating systems to patch known vulnerabilities**
- **educating employees about cybersecurity best practices, including how to recognise and report phishing attempts and other suspicious activity**
- **enforcing strong password policies and using multi-factor authentication**
- **securing network infrastructure with encryption and access controls to limit unauthorised access**
- **backing up data regularly and storing backups offline to mitigate the impact of ransomware attacks**
- **monitoring network activity for signs of unusual behaviour or unauthorised access**
- **Conducting regular security audits and risk assessments to identify and address potential vulnerabilities**
- **developing and maintaining an incident response plan to effectively respond to and mitigate the impact of cyberattacks.**

But what if, despite all best efforts and practices, your business falls foul of a malicious cyberattack? You can't close the door after the monster has bolted, so wouldn't it be advisable to have protection in place before it advances? This is where cyber insurance steps in!

Who needs cyber insurance? The answer is simple: everyone. Whether you're a small business or a multinational corporation, the threat of cybercrime looms large.

Cyber insurance is a vital lifeline in the fight against cybercrime. If your business uses technology in any capacity, cyber insurance is not just a wise investment, it's a necessity.

From data breaches to business interruptions, cyber insurance provides comprehensive coverage against the myriad consequences of cybercrime. By investing in this kind of insurance, businesses can arm themselves against this insidious monster and emerge stronger and more resilient in the face of digital threats.

Quite simply, you should consider obtaining cyber insurance if your business:

- **uses computers and email**
- **maintains a website**
- **stores digital records of customer or employee information**
- **conducts electronic payments or transactions**
- **relies on cloud storage or cloud-based services.**

Cyber insurance provides financial protection and support in the event of a cyber incident, covering costs associated with financial losses, data recovery, legal expenses, regulatory fines, business interruption and reputational damage.

As human error is often the weakest link in cybersecurity defences, with even the most vigilant employees falling victim to cleverly disguised phishing emails or other social engineering tactics, cyber insurance not only helps mitigate the financial fallout of such incidents but also provides access to resources and expertise to contain and limit the damage.

Cyber insurance also serves as a safeguard against the ever-evolving tactics of cybercriminals. As technology advances, so too do the methods used by cybercriminals to exploit vulnerabilities. A robust cyber insurance policy ensures that businesses are equipped to adapt and respond to emerging threats effectively.

But perhaps most importantly, cyber insurance offers peace of mind. Knowing that your business is protected against the unforeseen consequences of cybercrime can provide invaluable reassurance.

The online world may be fraught with peril, but with the right safeguards in place, businesses can keep the cybercrime monsters at bay. Cyber insurance is not just a precautionary measure, it's a strategic imperative in the ongoing battle against cybercrime.