When it comes to **cyber-crime,** no business is **'too small'**

While multinationals and larger firms will always remain in the cyber-criminals' crosshairs, small and mid-size enterprises (SMEs) can make much easier targets because, all too often, they are just not as prepared for a cyber-attack as their counterparts. They may also believe that they are just 'too small' for cyber-criminals to focus on when, in fact, it's this lack of awareness as a viable target that can make them more susceptible to cyber-crime.

Techinsure
part of the
clear group

Cyber-security breaches and changing work practices

Statistics released following the Cyber Security Breaches Survey 2021, commissioned by the Department for Digital, Culture, Media and Sport (DCMS), showed that four in ten businesses (39%) and a quarter of charities (26%) report having cyber-security breaches or attacks in the last 12 months.

Moreover, many UK businesses post-pandemic continue to use flexible working models, such as hybrid working, which present additional challenges to maintaining consistent cyber-security. So long as your customers have a workforce working remotely, and systems and data migrating to the cloud, they will face an increased exposure to security risks.

Why has exposure to cyber-incidents increased?

Your customers are at a greater risk of a cyber-incident because:

- More employees are working from home
- Changes to policies and working practices
- Staff potentially working outside company networks
- Companies more reliant on technology for their sales channels
- Employees becoming less vigilant, increasing the risk of an attack

What threats do your customers face?

Ransomware or extortion attack – this is when malicious software infects a customer's computer and effectively holds them to ransom by displaying messages demanding a fee to be paid for the system to work again.

Human error – is, for example, when an employee clicks on a suspicious link, leaves a laptop on a train, emails data to the wrong address or leaves company information vulnerable to theft or misuse.

Phishing – this is a type of social engineering attack used to steal data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message or text message.

Data hack – is an attempt to exploit a computer system or private network inside a computer, potentially allowing unauthorised access to/or control over computer network security systems for illicit purposes.

Zero-day attack – this is a recently discovered computer software vulnerability that hackers can exploit to attack your customer's computer systems until it is 'patched' or resolved.

How can we help your customers?

While the systems you are putting in place, and the services you provide, create a line of defence for your customer, no one is entirely safe from cyber-crime.

Techinsure can help your customers to understand and manage the risks that they face, by sourcing suitable solutions to address their needs and mitigate costs in the event of a cyber-attack or a data breach.

If you would like to discuss Technology Combined Insurance and your unique exposures, call us on **0333 043 1133** or email **techinsure@thecleargroup.com**

Techinsure
part of the cleargroup