Decoding **cyber** insurance

As businesses grow and adopt further technology, the risk of cyber-related incidents likewise increases. We are all aware of external threats such as hackers, but human error is in fact one of the main reasons behind these incidents, whether it's through the loss of equipment, or a member of staff clicking on the wrong link.

We are aware of the enormous levels of stress business owners could be under at the time of an incident and there is a widely held belief that your MSP (Managed Service Provider / IT provider) may be able to help you in the event of a cyber incident.

Whilst your MSP is able to support you where they can in your hour of need, we are aware that being able to access the expert services needed is the single biggest advantage of a cyber policy.

- **Incident response including forensic & legal experts**
- **Notification expenses involved in a data breach/loss.**
- **Minimising reputational damage**
- **Data recovery costs and associated costs**
- **Business interrupt ion resulting from security breaches and system failures (financial costs/losses)**
- **Negotiating ransomware (Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid)**

Techinsure

part of the CLEAR GROUP

Decoding **cyber** insurance

Did you know that your MSP (IT provider) can help mitigate the risks and ensure you obtain the best possible solution from insurers?

Here are a few ways your MSP can help:

Train employees – To spot and manage phishing emails as well as understanding cyber risks. Note Training should always be ongoing.

Enable Multi-Factor Authentication (MFA) – When accessing your work computers/systems remotely especially on administrator accounts. (Also referred to as MFA. It is a 2 part authentication system).

Test your back-up system – It is unfortunately not enough to just have a back-up system. They need to be regularly tried and tested along with being up-to date.

Patch and update frequently – Ensure systems are up to date.

Close all unnecessary/unused ports – RDP remains the main point of entry in ransomware attacks and ultimately data filtration. When these ports are exposed to the internet, they offer a relatively effortless way for criminals to enter a network. Such incidents can be prevented by patching, MFA, disabling ports (unless absolutely necessary) and limiting port exposure to the internet. Open ports should be monitored regularly (ports are the way in which your computer is connected to the internet).

Incident response plan – A formal plan to follow in the event of an incident.

Questions, questions, questions!

In order to gauge your current level of risk management, insurers are required to ask a number of questions. For example, if you have a back-up system in place, they will need to know where this is stored, is it offline, off-site, and how often is the data backed up. Your MSP can assist with technical questions, and save you time when obtaining quotations.

You must bear in mind with any incident or potential incident, your Insurers need to be notified first and foremost.

For a no-obligation quotation, call our team on:

0333 043 1133

or email **cyberinsurance@thecleargroup.com**

Techinsure

part of the CLEAR GROUP