Cyber-attacks are on the increase

During this moment in time, it is more critical than ever before to ensure you have the correct and adequate IT protection in place. Criminal activity is varied and can have a massive impact on your business and to your service users and their families.

Many businesses assume that they have transferred their liabilities and risk when their data is in a cloud provider's hands. In most cases this is not the position and there is little protection in terms of liability with your cloud providers. As recently as July 2020, The National Trust became one of the latest victims to issue a data breach alert, after cloud computing service Blackbaud was attacked. The growing cyber-attack has so far also affected charities such as Sue Ryder, Young Minds as well as dozens of Universities.

Although Blackbaud have said the data compromised did not include bank account or payment card details, a source has told the BBC that in some cases it involved donors' details including:

- Names, ages and addresses.
- Car licence details.
- Employers.
- Estimated wealth and identified assets.

During a webinar we recently hosted, a question was raised regarding mitigating the need for cyber protections due to cloud based services being purchased. Provided that you have systems, policies and procedures in place to keep data secure, using the cloud as a backup option is suitable and provides benefits to re-instate data and potentially defeat ransomware demands, which are increasing.

Certain things that you may need to consider when using a cloud-based service, however, include:

- Who has the access and authority to modify backups?
- How secure are your backups, could a ransomware attack overwrite previous backups, have you ensured your cloud provider keeps multiple versions of backed up data?
- What support will your cloud provider provide in the event of an attack?
- Will your cloud provider accept responsibility for attacks via their systems?
- Do you have client or other service providers software on your systems, is this clear to your cloud provider and are there any additional terms or restrictions from a third-party perspective?
- Does your cloud provider have multi-factor authentication to protect backups?

Such steps should assist to mitigate the risk of ransomware and other cyber-attacks. It is essential that you manage data as securely and as closely as you would if this was stored on your own systems. There are also Information Commissioner and GDPR issues around data that is sensitive or personal that is then made public: this is still your risk and liability.

Insurance protections

Cyber insurance can help protect your business against a range of cyber threats and exposures, including cybercrime, data breaches and system interruption.

Top activity areas for cyber-criminal include:

- Ransomware
- Phishing
- Data leakage
- Hacking
- Insider threat

Cover can now be purchased to protect against GDPR breaches, as part of a cyber protection policy.

Towergate Insurance – Insurance Partners of National Care Forum
Towergate Insurance is the preferred insurance provider of National Care Forum and offers members focused business advice and support in relation to your insurance protection as well as risk management solutions.

We work with specialists in the insurance and risk management sectors to ensure we have a variety of products to offer the care sector to assist your business when it needs it most.

To find out more, you can get in contact with your dedicated Towergate representative, Richard Hearn on 07977 491 586. Alternatively, you can email richard.hearn@towergate.co.uk