10 TIPS:

To help prevent

a Cyber attack

1. Backup Data

Backup data frequently with the backups stored off the insured's premises and not connected to the insured's network.

2. Staff Training

Ensure all staff have frequent cybersecurity training so they are aware of the potential risks.

3. Firewall & Anti-Virus Protection

Use operating systems with embedded firewalls and anti-virus protection software (such as Windows or MAC OS X), or run separate commercially licensed firewall or anti-virus protection software.

4. Never pay Ransom

Its not always wise to pay a ransom as you are not able to determine where the money will go (i.e funding terrorism without knowing) or if the hacker will repeat this attack.

5. Mobile Device Encryption

Protect your data with encryption including mobile phones, laptops and other portable devices.

6. Credit Card Storing

Do not store your credit card details on websites – do not keep them saved on notes or documents on computer system.

7. Password Protection

Keep passwords strong and secured and set up two factor authorisation (2FA).

8. Third Party Vendor Management

Any requests to alter supplier and customer details including bank account details, independently verified with a known contact for authenticity.

9. Two Person sign-off

Ensure that at least two members of staff authorise any transfer of funds, signing of cheques and the issuance of instructions for the disbursement of assets, funds or investments.

10. Incident Response Plan

Have a well-planned approach to addressing and managing a cyber attack to help respond to, and recover from network security incident.

DUAL