Cyberattacks: How care providers can protect themselves.

General

Use **risk assessment tools** to assess cyber risks & implement strategies to counter cyberattacks.

Regularly **review** & **refresh cyber awareness training** to keep the risks in the forefront of employees minds.

Always use **strong and secure passwords**. Consider investing in a password manager.

Look at obtaining **Cyber Essentials (NCSC) accreditation**.

Purchase **Cyber Insurance** to mitigate loss & protect against the financial & reputational impact, Cyber incidents can have.

Software

If using a 'Software as a Service' (SaaS) platform, check it has a **high level of cyber security**.

Check the terms & conditions of your Cyber Insurance policy if your SaaS suffers a breach.

Always keep your **anti-virus software up to date** and ensure it is running on all your devices.

Ensure that **software** is **updated** as often as possible across all devices.

Check with all suppliers to ensure their **cyber security procedures** are as robust as yours.

Smartphones, tablets and laptops

Use **strong and secure** passwords. Web browsers should suggest strong passwords.

Keep all of your device's **Operating System up-to-date.**

Make your staff aware that **banks & other organisations will never call to request password information** or ask them to transfer money.

Always connect to **secure WiFi.** If connecting to public WiFi be careful not to share sensitive data.

Be aware of suspicious downloads. There are malicious COVID-19 Apps which trick users into downloading malware.

howden specialist insurance brokers

QCS Quality Compliance Systems