Cyber Security Self-Assessment

Find out which areas of cyber security presents the biggest risk to your practice. Ask yourself the following questions and evaluate how you feel about the results.

1. Your ability to trade	**What would happen if you are not protected?** Denial of service attacks on your systems - resulting in your business being unable to meet commitments to employees, suppliers or patients.	1.1 Do you communicate with patients electronically?	Select:
		1.2 Is delivery of goods / services to your patients dependent on digital systems?	Select:
		1.3 Do you operate a website that provides you with an income?	Select:
		1.4 Do you have a process in place if your website is successfully attacked / corrupted?	Select:
		1.5 Do you have a process in place if your website is attacked but the attack is not successful?	Select:
		1.6 Is your payroll dependent on a digital system?	Select:
		1.7 Is your supplier-invoicing process dependent on digital systems?	Select:
2. Your data	**What would happen if you are not protected?** Loss or theft of patient or employee information.	2.1 Do you keep patient or employee information electronically?	Select:
		2.2 Are patient credit card or bank details kept on your system?	Select:
		2.3 Are these details encrypted?	Select:
		2.4 Do you have an IT policy in place regarding the handling of this type of data?	Select:
		2.5 Do you have a Privacy policy in place governing your collection of private data?	Select:
		2.6 Do you back your data up regularly?	Select:
		2.7 Do you permit your data to leave your system eg do you store it in the cloud?	Select:
		2.8 Do you have a contract with the third party that clearly defines what they can and cannot do with your data?	Select:
		2.9 What would you do it the third party's system went down?	Select:
3. Your money	**What would happen if you are not protected?** Phishing attacks i.e: you transfer money to a criminal rather than a supplier as a result of a fraudulent email.	3.1 Do you use temps in your finance team?	Select:
		3.2 Do you update security software as soon as advised?	Select:
		3.3 Are there automated checks and audit trails built into your financial systems?	Select:
		3.4 Do new supplier bank details need the approval of your Financial Director?	Select:
		3.5 Are monthly used twice in this sentence on funds leaving the business's account?	Select:
4. Your reputation	**What would happen if you are not protected?** Spoof websites or attacks on your social media accounts, but more importantly, loss of patient trust if you fail to respond confidently to any of the above.	4.1 Do you regularly check for spoof websites, e.g. Google Alerts?	Select:
		4.2 Would you know what to do if your social media were hacked?	Select:
		4.3 Do you have a contract in place with a PR agency who would support you if you were attacked?	Select:
		4.4 Do you have an incident response plan for cyber attacks?	Select:

Mostly Yes

To the questions you answered Yes; does that give you confidence or concern?

Did you answer yes more than you anticipated?

If answering yes gave you concern, then you need to speak to an insurance broker as soon as possible.

Some Yes / Some No

Look at each section and see if you have more Yes answers than Nos for that section. Where is the biggest risk to your practice? Where do you need the most protection?

Share this self-assessment with your broker to get a cyber policy that fits your practice.

Mostly No

Answering mostly No means one of two things; your practice is either a low risk or is ill prepared for a cyber attack.

If you fall into the latter, you need to take action now. Now you know where your risks are, you know what action to take.

In partnership with

BMA

www.lloydwhyte.com/bmacyber

01823 250580 • info@lloydwhyte.com

Lloyd & Whyte