

# 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.

<b>1. Your ability to trade</b>	<b>What would happen if you are not protected?</b> 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?	<input type="checkbox"/>
		1.2 Is delivery of goods / services to your patients dependent on digital systems?	<input type="checkbox"/>
		1.3 Do you operate a website that provides you with an income?	<input type="checkbox"/>
		1.4 Do you have a process in place if your website is successfully attacked / corrupted?	<input type="checkbox"/>
		1.5 Do you have a process in place if your website is attacked but the attack is not successful?	<input type="checkbox"/>
		1.6 Is your payroll dependent on a digital system?	<input type="checkbox"/>
		1.7 Is your supplier-invoicing process dependent on digital systems?	<input type="checkbox"/>

<b>2. Your data</b>	<b>What would happen if you are not protected?</b> Loss or theft of patient or employee information.	2.1 Do you keep patient or employee information electronically?	<input type="checkbox"/>
		2.2 Are patient credit card or bank details kept on your system?	<input type="checkbox"/>
		2.3 Are these details encrypted?	<input type="checkbox"/>
		2.4 Do you have an IT policy in place regarding the handling of this type of data?	<input type="checkbox"/>
		2.5 Do you have a Privacy policy in place governing your collection of private data?	<input type="checkbox"/>
		2.6 Do you back your data up regularly?	<input type="checkbox"/>
		2.7 Do you permit your data to leave your system eg do you store it in the cloud?	<input type="checkbox"/>
		2.8 Do you have a contract with the third party that clearly defines what they can and cannot do with your data?	<input type="checkbox"/>
		2.9 What would you do if the third party's system went down?	<input type="checkbox"/>

<b>3. Your money</b>	<b>What would happen if you are not protected?</b> 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?	<input type="checkbox"/>
		3.2 Do you update security software as soon as advised?	<input type="checkbox"/>
		3.3 Are there automated checks and audit trails built into your financial systems?	<input type="checkbox"/>
		3.4 Do new supplier bank details need the approval of your Financial Director?	<input type="checkbox"/>
		3.5 Are monthly used twice in this sentence on funds leaving the business's account?	<input type="checkbox"/>

<b>4. Your reputation</b>	<b>What would happen if you are not protected?</b> 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?	<input type="checkbox"/>
		4.2 Would you know what to do if your social media were hacked?	<input type="checkbox"/>
		4.3 Do you have a contract in place with a PR agency who would support you if you were attacked?	<input type="checkbox"/>
		4.4 Do you have an incident response plan for cyber attacks?	<input type="checkbox"/>

**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 proud partnership with



[www.lloydwhyte.com/aopcyber](http://www.lloydwhyte.com/aopcyber)  
 01823 250760 • [info@lloydwhyte.com](mailto:info@lloydwhyte.com)

