

Cyber risk exposure questionnaire

Whatever the size of your company, you probably depend on electronic systems to help run your business. It might be selling online, using office applications and email. In some cases, your whole business might be IT systems driven. When cyber attacks (such as data breaches and hacks) occur, they can result in devastating damage, such as business disruptions, revenue loss, legal fees, a permanently tainted reputation, and more.

If it's been a while since you reviewed your arrangements, you could be leaving your business exposed to risk. Have a look at our questionnaire below.

Instructions

Answer the questions below and give each response a numerical value depending on the answer:

- **Yes:** 5 points
- **No:** 0 points
- **Unsure:** 5 points

After completing all of the questions, total your score to determine your organisation's level of cyber risk

- **Low risk: 0-10**
- **Moderate risk: 15-25**
- **High risk: 30-50**
- **Escalated risk: 55-100**

Exposure	Yes	No	Unsure	Score
1. Can your employees or customers access your internal systems from remote locations? Do you have a wireless network?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2. Do any of your employees travel or work from home with company-owned mobile devices (eg, laptops, smartphones and USB drives)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3. Does your organisation use Cloud-based software or storage?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4. Does your organisation allow employees to use their own personal devices for business use or on a company network?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5. Are any employees allowed access to administrative privileges on your network or computers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6. Does your organisation have critical operational systems connected to a public network?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
7. Does anyone in your organisation use computers to access bank accounts or initiate money transfers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
8. Does your organisation store sensitive information (eg, financial reports, trade secrets, intellectual property and product designs) that could potentially compromise your organisation if stolen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

9.	Does your organisation digitally store sensitive information? This could include government-issued ID numbers and financial information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
10.	Is your organisation part of a supply chain, or do you have supply chain	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
11.	Does your organisation conduct business in foreign countries, either physically or online?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
12.	Has your organisation ever failed to enforce policies around the acceptable use of computers, email, the Internet, etc?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
13.	Can the general public access your organisation's building without the use of an ID card?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
14.	Is network security training for employees optional?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
15.	Can employees use their computers or company-issued devices indefinitely without updating passwords?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
16.	Has your IT department ever failed to install antivirus software or perform regular vulnerability checks?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
17.	Can employees dispose of sensitive information in unsecured bins?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
18.	Would your organisation lose critical information in the event of a system failure or other network disaster?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
19.	Can employees easily see what co-workers are doing on their computers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
20.	Has it been more than a year since your organisation reviewed its data security or cyber security policies /procedures?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Total score					

Unfortunately, no organisation is immune to the impact of cyber-crime. As a result, cyber liability insurance is an essential component to any risk management programme. Get in touch with Adam Jeffs via adam.jeffs@marshcommercial.co.uk or [07748 647673](tel:07748647673) to see how he can help you.

Source Zywave – Cyber Risk Exposure Calculator

This is a marketing communication.

Marsh Commercial is a trading name of Jelf Insurance Brokers Ltd, which is authorised and regulated by the Financial Conduct Authority (FCA). Not all products and services offered are regulated by the FCA (for details see marshcommercial.co.uk/info/terms). Registered in England and Wales numb 0837227. Registered Office: 1 Tower Place West, London EC3R 5BU. FP20.068c

