CYBER-RISK EXPOSURE SCORECARD -

OFFICES

TURNER
INSURANCE GROUP

Office networks and devices can help with communication, streamline operations and reduce costs. However, many employers don't realise the extent of their cyber-risks. Even though most offices have basic safeguards in place, hackers can still target your systems with social engineering schemes, data stolen from third parties and a growing list of cyber-attacks. Even one cyber-exposure can put your financial information, intellectual property or strategic plans at risk. You also need to protect your customers' and employees' personal information, as a data breach can lead to damaging legal action and a tarnished reputation.

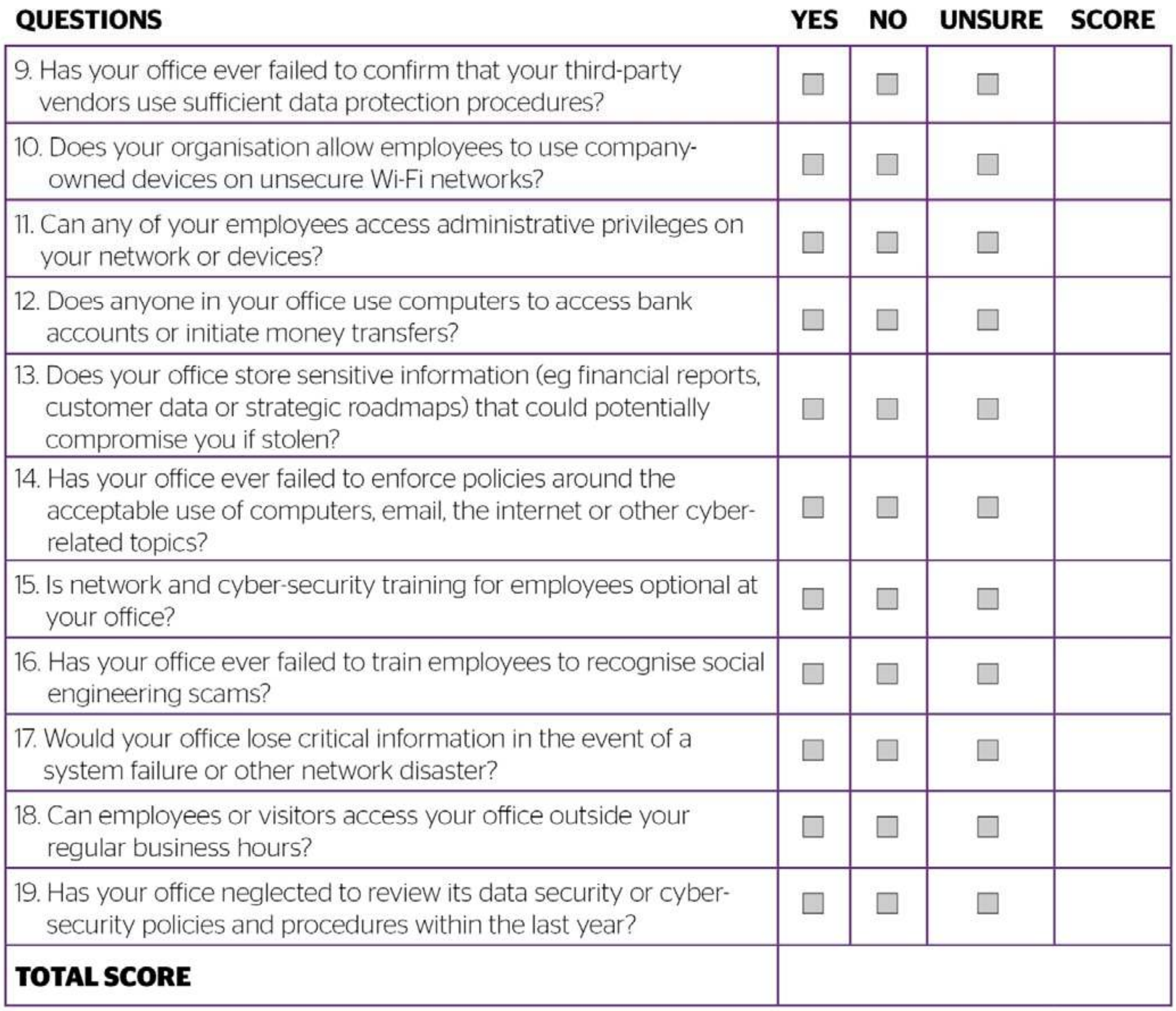
Since the potential loss from a cyber-attack is so high, no office can assume that their systems are completely safe. You should also consider cyber-liability insurance as a key component to your risk management programme.

Instructions: Begin by answering the questions below. Each response will be given 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 office's level of cyber-risk using the scale below.

QUESTIONS	YES	NO	UNSURE	SCORE
1. Does your office have a wireless network, and do you let employees or visitors access it?	□	□	□	
2. Do you allow employees to use their personal devices (eg laptops, smartphones and tablets) in the office?	□	□	□	
3. Does your business have offices in more than one location?	□	□	□	
4. Can employees access your office's servers or data remotely?	□	□	□	
5. Does your office have a website or mobile app that's used to collect or track personally identifiable information such as email addresses, phone numbers or IP addresses?	□	□	□	
6. Does any software at your office require an update?	□	□	□	
7. Has your office ever failed to screen visitors or service providers to ensure they can't access unauthorised areas?	□	□	□	
8. Does your office use a third-party vendor for data storage, payment processing or online marketing?	□	□	□	



QUESTIONS	YES	NO	UNSURE	SCORE
9. Has your office ever failed to confirm that your third-party vendors use sufficient data protection procedures?	□	□	□	
10. Does your organisation allow employees to use company-owned devices on unsecure Wi-Fi networks?	□	□	□	
11. Can any of your employees access administrative privileges on your network or devices?	□	□	□	
12. Does anyone in your office use computers to access bank accounts or initiate money transfers?	□	□	□	
13. Does your office store sensitive information (eg financial reports, customer data or strategic roadmaps) that could potentially compromise you if stolen?	□	□	□	
14. Has your office ever failed to enforce policies around the acceptable use of computers, email, the internet or other cyber-related topics?	□	□	□	
15. Is network and cyber-security training for employees optional at your office?	□	□	□	
16. Has your office ever failed to train employees to recognise social engineering scams?	□	□	□	
17. Would your office lose critical information in the event of a system failure or other network disaster?	□	□	□	
18. Can employees or visitors access your office outside your regular business hours?	□	□	□	
19. Has your office neglected to review its data security or cyber-security policies and procedures within the last year?	□	□	□	
TOTAL SCORE				

Low risk. Contact Turner Insurance Group to confirm: 0-10

Moderate risk. Contact Turner Insurance Group to confirm: 15-25

High risk. Contact Turner Insurance Group to confirm: 30-50

Escalated risk. Contact Turner Insurance Group to confirm: 55-95