Cyber Risk Exposure Scorecard
Offices

Offices are full of networks and devices that can help communicate, streamline operations and reduce costs. However, many employers don't realize the extent of their cyber risks. Even though most offices have necessary safeguards in place, hackers can sell target your systems with social engineering schemes, data stolen from third parties, and a growing cyber attacks list. Even 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 lawsuits and a tarnished reputation.

Since the potential loss from a cyber attack is so high, no office can assume their systems are completely safe. It would help if you also considered cyber liability insurance a critical component to your risk management program.

QUESTIONS	YES	NO	UNSURE	SCORE
Does your organization have a wireless network, and do you let employees or visitors access it?	☐	☐	☐	
Do you allow employees to use their personal devices (e.g., laptops, smartphones, and tablets) in the office?	☐	☐	☐	
Does your business have offices in more than one location?	☐	☐	☐	
Can employees access your office's servers or data remotely?	☐	☐	☐	
Does your office have a website or mobile app used to collect or track personally identifiable information such as email addresses, phone numbers, or IP addresses?	☐	☐	☐	
Does any software at your office require an update?	☐	☐	☐	
Has your office ever failed to screen visitors or service providers to ensure they can't access unauthorized areas?	☐	☐	☐	
Does your office use a third-party vendor for data storage, payment processing, or online marketing?	☐	☐	☐	
Has your office ever failed to confirm that your third-party vendors use sufficient data protection procedures?	☐	☐	☐	
Does your organization allow employees to use company-owned devices on insecure Wi-Fi networks?	☐	☐	☐	
Can any of your employees access administrative privileges on your network or devices?	☐	☐	☐	
Does anyone in your office use computers to access bank accounts or initiate money transfers?	☐	☐	☐	
Does your office store sensitive information, such as financial reports, customer data, or strategic roadmaps the could potentially compromise you if stolen?	☐	☐	☐	
Has your office ever failed to enforce policies around the acceptable use of computers, email, the internet, or other cyber-related topics?	☐	☐	☐	
Is network and cyber security training for employees optional at your office?	☐	☐	☐	
Has your office ever failed to train employees to recognize social engineering scams?	☐	☐	☐	

Cyber Risk Exposure Scorecard
Offices

QUESTIONS	YES	NO	UNSURE	SCORE
Does your business operate in the Europe or store any data the could happy to the European Union's General Data Protection Regulation (GDPR)?	☐	☐	☐	
Would your office lose critical information in the event of a system failure or other network disaster?	☐	☐	☐	
Can employees or visitors access your office outside your regular business hours?	☐	☐	☐	
Has your office neglected to review its data security or cyber security policies and procedures within the last year?	☐	☐	☐	
TOTAL SCORE				

ESCALATED RISK: 55-100   **HIGH RISK: 30-50**   **MODERATE RISK: 15-25**   **LOW RISK: 0-10**