Cyber Risk Exposure **Scorecard**

In recent years, cyber attacks have emerged as one of the most significant threats facing organizations of all sizes. The internet and other network operations have created risks that were unheard of less than a decade ago. When cyber attacks (such as data breaches and hacks) occur, they can result in devastating damage, such as business disruptions, revenue loss, legal fees and forensic analysis and customer or employee notifications.

It is important to remember that no organization is immune to the impact of cyber crime. As a result, cyber liability insurance has become an essential component to any risk management program.

Instructions: begin by answering the questions below. Each response will be given a numerical value depending on the answer.

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

After completing all of the questions, total your score to determine your organization's level of cyber risk using the scale below.

Exposure	Yes	No	Unsure	Score
1. Does your organization have a wireless network, or do employees or customers access your internal systems from remote locations?				
2. Does anyone in your organization take company-owned mobile devices (e.g., laptops, smartphones and USB drives) with them, either home or when traveling?				
3. Does your organization use cloud-based software or storage?				
4. Does your organization have a "bring your own device" (BYOD) policy that allows employees to use personal devices for business use or on a company network?				
5. Are any employees allowed to access administrative privileges on your network or computers?				
6. Does your organization have critical operational systems connected to a public network?				
7. Does anyone in your organization use computers to access bank accounts or initiate money transfers?				
8. Does your organization store sensitive information (e.g., financial reports, trade secrets, intellectual property and product designs) that could potentially compromise your organization if stolen?				
9. Does your organization digitally store the personally identifiable information (PII) of employees or customers? This can include government-issued ID numbers and financial information.				
10. Is your organization part of a supply chain, or do you have supply chain partners?				
11. Does your organization conduct business in foreign countries, either physically or online?				
12. Has your organization ever failed to enforce policies around the acceptable use of computers, email, the Internet, etc.?				
13. Can the general public access your organization's building without the use of an ID card?				
14. Is network security training for employees optional at your organization?				
15. Can employees use their computers or company-issued devices indefinitely without updating passwords?				
16. Has your IT department ever failed to install antivirus software or perform regular vulnerability checks?				
17. Can employees dispose of sensitive information in unsecured bins?				
18. Would your organization lose critical information in the event of a system failure or other network disaster?				
19. Can employees easily see what coworkers are doing on their computers?				
20. Has your organization neglected to review its data security or cyber security policies and procedures within the last year?				

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

Total Score: