

CYBER RISK EXPOSURE SCORECARD

Instructions: Begin by answering the questions below. Each response will be assigned a score depending on the answer.

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

Your score will determine your organisation's level of cyber risk.

In recent years, cyber attacks have emerged as one of the most significant threats facing organisations 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 organisation is immune to the impact of cyber-crime. As a result, cyber liability insurance has become an essential component to any risk management programme:

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

TOTAL SCORE

ESCALATED RISK: 55-100

MODERATE RISK: 15-25

HIGH RISK: 30-50

LOW RISK: 0-10



556 Leeds Road, Outwood, Wakefield, WF1 2DX
01924 871111 - insurance@wtj.co.uk - wtj.co.uk