

# CYBER RISK EXPOSURE SCORECARD

In recent years, cyber attacks have emerged as one of the most significant threats facing organizations of all sizes. When cyber attacks (such as data breaches and hacks) occur, they can result in devastating damage, such as business disruptions, revenue loss, legal fees, forensic analysis and member or employee notifications.

Instructions: Begin by answering the questions below. Each response will be given a numerical value depending on the answer. After completing all of the questions, total your score to determine your organization's level of cyber risk using the scale below.

YES = 5 points    UNSURE = 5 points    NO = 0 points

EXPOSURE	YES	NO	UNSURE	SCORE
Does your ministry have a wireless network, or do employees or members access your internal systems from remote locations?				
Does anyone in your ministry take church-owned mobile devices with them (either home or when traveling)?				
Does your ministry use cloud-based (off site) software or storage?				
Does your ministry have a "bring your own device" policy that allows employees/volunteers to use personal devices for ministry business or on your business network?				
Are employees/volunteers allowed administrative privileges on your network or computers?				
Does your ministry have critical operational systems connected to a public network?				
Does anyone use computers to access bank accounts or initiate money transfers?				
Does your organization store sensitive information that could potentially compromise your ministry if stolen?				
Does your ministry digitally store the personally identifiable information of employees or members? This can include government-issued ID numbers and financial information.				
Does your ministry participate in online giving?				
Does your ministry conduct business in foreign countries (including online)?				
Has your ministry ever failed to enforce policies around the acceptable use of computers, email the internet, etc?				
Can the general public access your building(s) without the use of an ID card?				
Is network security training for employees optional at your organization?				
Has your IT employee or professional ever failed to install antivirus software or perform regular vulnerability checks?				
Can employees use their computers or company issued devices without having to regularly update passwords?				
Can employees dispose of sensitive information in unsecured bins?				
Would your organization lose critical information in the event of a system failure or disaster?				
Can employees easily see what co-workers are doing on their computers?				
Has your ministry neglected to review its cyber security policies within the last year?				
Total Score				

**ESCALATED RISK: 55-100**

**HIGH RISK: 30-50**

**MODERATE RISK: 15-25**

**LOW RISK: 0-10**

