How secure are you, your systems and your information and data?

Rate each of these points of preparedness using the following scale:

Done/done consistently

Needs improvement or not consistently done

Item is not done or never done

Organizational Preparedness

○○○ We have a written cybersecurity policy.

○○○ We have a written internet use and access policy that provides examples of acceptable and unacceptable use.

○○○ We have a written physical security policy that addresses securing areas where computer equipment and/or sensitive information is held.

○○○ We have a written policy addressing the electronic storage and encryption of sensitive information on mobile devices such as laptops, tablets and phones.

○○○ Our cybersecurity policy addresses the use of mobile devices to access organization data.

○○○ Our cybersecurity policy addresses the immediate notification of a breach as required by the laws of our state.

○○○ Our cybersecurity policy includes an incident response plan.

○○○ Our cybersecurity policy has a process for notifying those impacted by a cybersecurity breach.

○○○ Our cybersecurity and internet use policies are reviewed annually to ensure they are up to date and address the needs of the organization.

○○○ Our cybersecurity and internet use policies are acknowledged annually by all with access to our computing systems/data.

○○○ Information that is critical to the operation of our organization is backed up regularly.

○○○ We have automated backups to the cloud or off-site for critical data and information.

○○○ Our policies and systems require changing passwords or pass phrases at least every three months.

○○○ Our cybersecurity policy requires strong passwords to include a combination of upper- and lowercase letters, numbers, symbols or special characters.

○○○ We utilize Multi-Factor Authentication (MFA) in addition to passwords or pass phrases.

○○○ We utilize a VPN for remote workers as an added layer of protection for our internal systems and data.

○○○ Our systems utilize role-based authority/permission levels to limit access to sensitive or critical data.

○○○ We conduct background checks on all persons with assigned security responsibilities or security sensitive functions such as money handling.

○○○ We conduct background checks on all persons that have access to our systems and devices.

○○○ Formal criteria are in place regarding what is acceptable within an individual's background to allow access.

○○○ Only approved individuals are allowed access to and use of systems and devices.

○○○ Visitor or guest registration (sign in/out) procedure with name badge and/or photo ID is required.

○○○ Social media is regularly monitored for potential issues/threats.

○○○ We have policies for disposing of old computer equipment that protect against data loss (shredding, wiping drives, etc.)

○○○ We have a Business Continuity Plan in place that addresses cyberattack.

○○○ We have obtained coverage for data breach protection.

How secure are you, your systems and your information and data? (continued)

Rate each of these points of preparedness using the following scale:

- Done/done consistently
- Needs improvement or not consistently done
- Item is not done or never done

IT Systems Preparedness

○ ○ ○ Our IT security personnel conduct regular systems checks to identify potential cyberinfections.

○ ○ ○ Our wireless network requires strong wireless authentication and masks the network name (SSID - Service Set Identifier) or location.

○ ○ ○ Our IT systems and devices automatically lock out accounts after three unsuccessful login attempts.

○ ○ ○ Our IT systems automatically log out after a pre-determined amount of time.

○ ○ ○ Our IT systems utilize firewalls and encryption to restrict access to the network and data.

○ ○ ○ Our IT systems utilize active system monitoring.

○ ○ ○ Our IT systems are reviewed and evaluated for vulnerabilities on a regular and scheduled basis.

○ ○ ○ All internet-connected systems are updated with the most current versions of software and apps.

○ ○ ○ We regularly review our technology to stay current and invest in upgrades.

○ ○ ○ Unused applications are deleted to reduce the risk of infection from malware or ransomware.

Staff Preparedness

○ ○ ○ All with access to our computers, mobile devices and systems have been trained to identify phishing, spear phishing, ransomware and other malicious emails.

○ ○ ○ We provide cybersecurity training upon hire and periodically throughout the year.

○ ○ ○ Our employees/volunteers have been trained in handling, protecting and disposing of sensitive information.

○ ○ ○ All staff, volunteers and other organization representatives have been trained on the cybersecurity policy and the responsibilities within it.

○ ○ ○ Our cybersecurity training emphasizes that passwords or pass phrases are never to be shared, written down or emailed.

○ ○ ○ Those with cybersecurity responsibilities have been trained and provided with procedures on how to respond to a cybersecurity risk or attack.

Facility Preparedness

○ ○ ○ We have an electronic security system (doors, windows) monitored by a central station.

○ ○ ○ Audible alarm systems are present and audible to exterior grounds.

○ ○ ○ We have security cameras placed in critical areas such as entries, hallways, areas of high occupancy and where valuables are stored or handled.

○ ○ ○ Our security system is inspected and tested annually by a licensed contractor.

○ ○ ○ All buildings are locked when unattended or unoccupied.

○ ○ ○ Formal and documented locking procedures are in place for office areas to safeguard financial or sensitive information.

○ ○ ○ Computing areas and equipment can be physically secured.

○ ○ ○ A key control policy or re-key policy is in place at the organization.

○ ○ ○ Waste paper containing sensitive information is shredded or disposed of through a document disposal vendor (secure bins).

Your results

The number of items rated **Done/Done Consistently**

▶ 0

40 OR GREATER

Your organization is well prepared. Continue to fine tune your security program.

39 TO **33**

Your organization has some security elements in place but there is opportunity to improve. Prioritize and complete items in the other columns.

32 OR LESS

Your organization's security program needs improvement. Action is needed to meet basic requirements.

Don't wait for a cyber threat to protect your information and data.
Risk Control Central can help identify your areas of greatest need and provide you with helpful resources.

PROTECTING
THE GREATER
GOOD®

Church
Mutual®
INSURANCE

The information contained in these materials is intended solely to provide general guidance on topics that may be of interest to you. While we have made reasonable efforts to present accurate and reliable information, Church Mutual Insurance Company, S.I. (a stock insurer)[1] and its affiliates disclaim all liability for any errors or omissions or for any actions you take or fail to take based on these materials. The information provided may not apply to your particular facts or circumstances; therefore, you should seek professional advice prior to relying on any information that may be found in these materials.

NAIC # 18767; CA Company ID # 2867-0

[1] Church Mutual® is a stock insurer whose policyholders are members of the parent mutual holding company formed on 1/1/2020. S.I. = a stock insurer.