Cyber Attacks:

A Growing Interruption Threat for Ministries

Natural disasters continue to be a primary cause for interruptions of church ministries; there is another concern on the horizon that is quickly developing into an equally devastating unnatural disaster: cyber attacks. As congregations continue to develop their reliance on computers, and digital storage of data, the potential risk of exposure to church records and finances grows with every passing day.

Although cyber attacks can cause interruptions to church operations, the good news is that ministries can take measures to mitigate this risk.

How Cyber Attacks Cause Interruptions

Hackers, thieves and other unauthorized parties have become adept at exploiting weaknesses in a ministry's computer system and operations. The threat can be through traditional hacking methods (computer access) or social interactions through programs such as email.

There are several types of attacks that have the potential to completely disrupt a church's ability to perform routine operations that include:

- Malicious programs that render a website unusable.
- Denial of service attacks that make your website inaccessible to church administrators and members.
- Viruses, worms or other malicious programs that delete critical information on a church's computer or other hardware.

Any of these events can present struggles that make it difficult for ministries to maintain their operations. Many smaller congregations may not have the staff available to detect the problem and then fix it, which only increases the length of an interruption.

Third-Party Interruptions

Your ministry can still be affected even if the cyber attack does not occur at your facility. If a church's accountant suffered an attack, for example, it could result in a threat to church funds and the ability to operate.

Although attacks on third parties are often out of your ministry's control, such an event could have a profound impact on how a congregation can operate and serve the people who rely on the ministry, and its services.

Ways to Prevent a Cyber Attack

Cyber security attacks are becoming so commonplace that a common belief in the cyber security world is, "It's not *if* you'll be a victim, but *when*." It is impossible to provide 100% protection against cyber attacks, but ministries can lower their chances of interruption by following a few suggestions:

- Only connect to the internet over a secure password-protected network.
- Do not click on links or pop-ups, open attachments or respond to emails from strangers.

- Create and document a formal risk management plan that addresses the scope, roles, responsibilities, compliance criteria and methodology for performing cyber risk assessments. This plan should include a characterization of all systems used at the organization based on their functions, the data they store or process, and their importance to the organization.
- Make sure all firewalls (programs to block access) and routers are secure and updated regularly.
- Create a cyber security policy that educates administrators, employees and congregants about the dangers of computer invasions and how to prevent them. The policy should be drafted for your ministry's specific needs.
- Download, install and update the software for your computer's operating systems and applications on a routine basis or as they become available.
- Start a strict password policy that has administrators and users change their passwords at least every 90 days.
- Limit users access to church data and information (limiting authority to install software).
- Obtain a cyber liability insurance policy.

If You Suspect An Attack Has Occurred

- If you have access to an IT department, contact them immediately. The earlier someone can investigate and repair your computer, the less damage to your computer and other computers on the network.
- Run a scan to make sure your system is not infected or acting suspiciously.
- If you find a problem, disconnect your device from the internet.
- If you believe you might have revealed sensitive information about your ministry, report it to the appropriate people within the organization, including network administrators. They can be on the alert for any suspicious or unusual activity.

How Cyber Liability Coverage Can Help

The standard commercial general liability (CGL) policy does not cover a loss to a ministry's operations (interruption) due to a cyber event. Cyber liability coverage is available to fill that void as an addition to that standard form.

If a church is unable to maintain normal ministry operations, cyber liability policies may help pay for expenses related to an interruption. The coverage may pay for:

- Lost income due to a cancelled event.
- Donations that would have been received had the event not occurred.
- Continuing operating expenses, such as utilities, that must still be paid despite operations ceasing
- Rented or leased equipment.

Cyber liability coverage may also protect a church from loss due to these types of events:

- **Data Breaches-** including costs for member notification, some legal costs and credit monitoring for those affected.
- **Damages to Third-Party Systems-** such as damages that occur when an infected email from your church damages or harms the system of a user or vendor.
- **Data or Program Loss-** due to a natural disaster or harmful activity (physical losses are usually covered under a different policy format).
- **Cyber Extortion-** this can include ransomware (a malicious program installed on a computer on your network) that prevents system access until a ransom is paid.

The interruption of church operations due to cyber attacks are fairly rare, but being unprepared for an attack can prevent a ministry from fulfilling their mission.

Please consult a licensed, qualified computer technician or other computer systems professional for specific advice on protecting your ministry.

INSURANCE BOARD
Partners in Protection