Adventist Risk
Management® Inc.

CYBER
LIABILITY

This is a new era. Technology and the Internet have impacted the operations of today's business world. With these changes, cyber exposure has grown exponentially. In order to protect your institution's IT systems and clients' personal data, ARM has prepared this information sheet on some of the cyber risks you may be exposed to, and the solutions we can offer to minimize these risks.

Cyber Risks

Cyber risk exposures and related consequences are very real and numerous. They may include denial of service attacks and business interruption costs. As a result, an organization may fail to access it's own IT systems and lose substantial data processing time. Access to important data that may be mission-critical to decision makers could become unavailable.

WHAT ARE SOME OF THE CYBER RISKS YOU MAY BE EXPOSED TO?

- Breach of privacy (Release of Personally Identifiable Information e.g. social security number, names, address etc.)
- Cyber extortion (Data being held hostage unless you pay the blackmailer)
- Cybercrime (vandalism, sabotage of IT systems etc.)
- The risk of terrorism (use of IT systems to sabotage infrastructure such as power, communications, or water supplies etc.)
- The liability that may arise from network security breaches (legal suits, and compliance requirements etc.)
- The use of electronic media (such as online photos, music, videos and text messages)
- Use of intellectual property that belongs to others (e.g. copyrights, trademarks, patents)
- Technology errors and omissions (poor design or maintenance, or installations of systems)
- Colleges face the manipulation of student records or grades in the event of a data breach caused by hackers.
- Medical facilities are always facing the risk of data integrity to patient records.
- Illegal or unauthorized access to IT systems may result in fraudulent transfer of money using online payment instructions.
- A computer virus attack, for example, can damage the IT systems, including software, and corrupt the data in the system.

Solution

IDENTIFYING AND ANALYZING YOUR CYBER RISKS

The cost to recover or restore data that has been altered, destroyed, or deleted is not easily quantifiable. However, a risk management process can lead to the identification of specific cyber risks to which your institution is exposed. It can also help analyze the size of the risks and their impact to your organization's ministry.

CYBER RISK LIABILITY INSURANCE

Cyber risk liability insurance is a useful tool for mitigating the financial consequences of a potential data breach to IT systems. A cyber liability insurance policy for Churches may cover the Church as the first party. This means protecting the Church's own IT infrastructure should damage occur. The policy also has third party coverage that focuses on legal liability to others such as loss or exposure of your customers' private information. The summary below outlines the two coverage sections on the cyber liability policy:

THIRD PARTY (OTHER PERSONS):

CYBER LIABILITY COVERAGE

- Network Security
- Privacy Breach
- Internet Media

FIRST PARTY (INSURED/YOU):

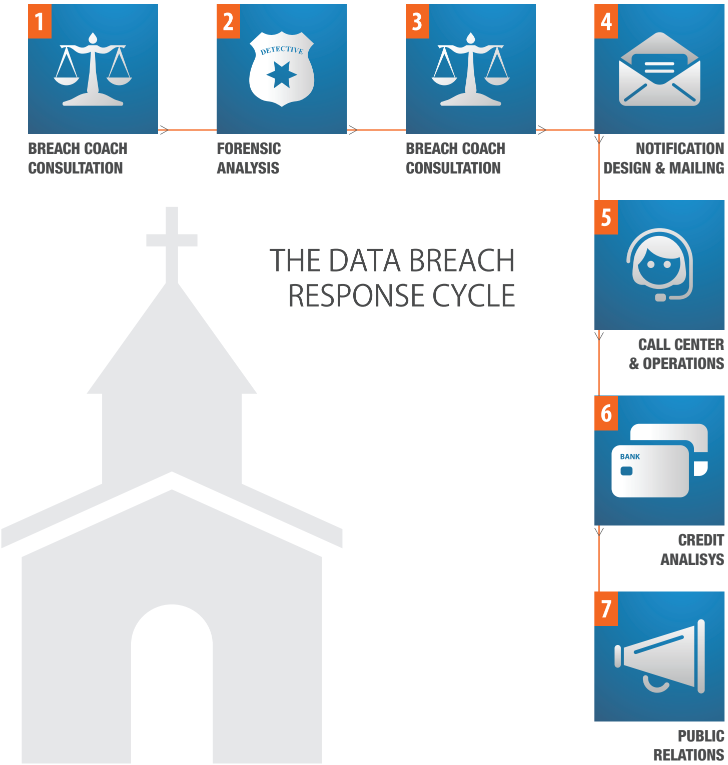
CYBER CRIME EXPENSES

- Regulatory Proceeding
- Credit Monitoring
- First Data Loss
- Network Business Interruption
- Network Extortion

When considering cyber risk, your organization must ask the following questions:

- What does our organization need to do to achieve its ministry in the age of technology?
- What tools or resources, such as IT systems, does our organization depend on?
- What financial or reputational cost could our organization face in light of a data breach or unavailability of IT Systems?

We encourage you to include cyber risk in your continuity planning and add a cyber liability policy to your insurance coverage. Please contact your Account Executive for more details and an application form. ■



THE DATA BREACH RESPONSE CYCLE

GLOSSARY:

CYBER: Meaning "computer," "computer network," or "virtual reality," used in the formation of compound words (cybertalk; cyberart; cyberspace).
DATA BREACH: A data breach is the intentional or unintentional release of secure information to an untrusted environment.
DENIAL OF SERVICE: A type of attack on a network that is designed to hamper or harm the network by flooding it with useless traffic.
FIRST PARTY: The insured organization or individual.
IT: Information Technology.
LIABILITY: A legally enforceable obligation.
MITIGATING: To make less severe, to prevent further damage.
NOTIFICATION: Security breach notification required by law in most states.
THIRD PARTY: An organization or a person other than the parties to the contract, for example, a customer whose data has been breached.
VIRUS: A segment of self-replicating code planted illegally in a computer program, often to damage or shut down a system or network.

Like us on
Facebook
adventistrisk

Follow us on
Twitter
@adventistrisk

Watch us on
YouTube
AdventistRiskMgmt

FOR MORE INFORMATION, SUBSCRIBE TO OUR SOLUTIONS NEWSLETTER AT:
www.adventistrisk.org