

# Risk Reporter

Summer  
2014

Vol. 13  
issue 3

A quarterly publication by Church Mutual Insurance Company



## Protecting against cyber liability and data breach

Data breach is one of the fastest growing crimes in America. For victims, it's a painful and costly problem. When information is stolen that compromises identities and financial security, victims can be left wondering what they can do to regain not only their assets, but their peace of mind.

Risk Based Security Inc. reports that in the first four months of 2014, there were more than 300 publicly disclosed data breaches in the United States, resulting in the compromise of more than 51 million records.

Data breach occurs when someone steals personal or financial information. Unfortunately, data breach doesn't just happen to a person. It also can happen to congregations. Business identity fraud is a growing problem that can affect any entity. If an organization's Federal Employee Identification Number is stolen, websites and other data can be misused.

Consequences of data breach and identity theft can destroy the very foundation that congregations are built upon. Learning how to avoid information risk and protect the members of your congregation is paramount.

"Churches of all sizes can be victims of a malicious data breach or a simple unintentional data loss accident," said Tom Widman, president and CEO of Identity Fraud Inc., a corporation that provides a variety of identity crime-related solutions to help protect people and businesses against identity crimes and data theft. "Luckily, there are cost-effective resources available that can help control the risk and impact of a breach."

### The information you use could be stolen

To operate smoothly, many organizations collect personal information about members that might include email and mailing addresses, phone numbers and even family and medical histories.

"Our church collects contact information that is provided voluntarily for various purposes," said Karen Kubiak, director of communications at Elmbrook Church in Brookfield, Wis. "Many of our programs and events for children and adults are registration-based so we maintain that registrant information in our database. We also provide year-end giving

(See Cyber liability, Page 2)

## Inside

### Seasonal Spotlight

*Guidelines and screening help keep volunteers safe*

### Managing Your Risks

*Ladder Inspection Checklist and safety posters*

### QIA

*Risk Reporter talks with Harry Shuford about filing claims promptly*

Now get your quarterly  
**Risk Reporter** via email.

Sign up at [www.churchmutual.com/risk](http://www.churchmutual.com/risk).



## ( Cyber liability )

statements to those who have contributed financially to the church.”

Larger organizations also might be in a position to retain the financial data of members by encouraging automatic contributions through regular account transfers or online payments.

“While this is an easy and convenient way of providing support, protecting this account information and maintaining the security of the website is an added layer of responsibility for the organization,” Widman said.

Storing financial data can be extremely dangerous and could create the opportunity for a data breach that would have negative consequences on not only the members, but the business identity or the organization as well.

### Consequences of data breach

In the event of a data breach in which members are victims of identity theft, the congregation can be held liable, resulting in large fees or penalties. The congregation also would be responsible for all costs associated with communicating the damages to members, as well as the costs associated with offering recovery assistance.

When an organization’s business identity is stolen, criminals can take actions using the congregation’s data that are illegal, immoral or financially detrimental. A thief could steal information about the organization that could lead to total financial corruption, extreme legal ramifications or worse.

The consequences can be dire when an organization experiences a data breach. In the worst case scenario, a breach could cause an organization to be stripped of its assets. The organization would then be forced to shut down.

“Once the credit record of a congregation is damaged, charitable contributions are siphoned away or the bank account is emptied, there is little recourse for recovery,” Widman said. “Given the financial consequences of a breach, no organization can afford to ignore information risk.”

### Creating a data security procedure

One of the best measures you can take to protect your congregation’s business identity and your members against identity theft is to enact a data security procedure.

“Ideally, data needs to be kept off the Internet (in a place) where people with malicious intent can’t find their way to it,” said Paul Alan Clifford of TrinityDigitalMedia.com LLC. “That’s not always possible, so having a good security procedure in place is a must.”

To create a data security procedure, organizations must address the following concerns:

#### ■ Information storage

Review the types of personal and financial data that are collected. Consider how this information is stored

and which staff members or volunteers have access to it.

#### ■ Data classification

Classify your data. Some data might be perfectly acceptable to have designated as public use, such as member names or email addresses. Other data, such as financial data or medical histories, should be kept classified for key personnel only.

#### ■ Computer protection

Ensure your computer antivirus program is installed and up-to-date. Software, such as Norton™ AntiVirus or McAfee® can go a long way in protecting computers from hackers.

#### ■ Computer networks

Encrypt your computer network to protect information that is sent. Consider using programs, such as SensiGuard or AutoKrypt.

#### ■ Security vulnerabilities

Scan your system for security vulnerabilities. Programs, such as Rapid7 or Nessus are a good place to start.

### What to do if your congregation is a victim of identity fraud

Protecting your organization from data theft is not enough. A complete risk management plan also should include a response plan.

“As part of the risk management plan, congregations should consider how they would respond to a breach, including who can help manage the thorny issues of breach response and the financial impact of the incident,” Widman said. “A proper breach response can help prevent a bad situation from turning catastrophic.”

If your congregation is a victim of data theft, respond quickly and professionally. Notify your members of the situation as soon as you have all of the information. You also might consider offering free credit monitoring or identity recovery assistance to help your members.

Lastly, identify ahead of time a professional who can help manage your recovery from identity fraud. Contact your insurance company or a legal representative to learn what resources they have available to assist your congregation in the event of a data breach. Although a large number of organizations experience a data breach event every year, there are easy and inexpensive ways to protect your congregation.

Church Mutual offers its customers optional Cyber Liability insurance and data breach services through Identity Fraud Inc. and its business partners.

■ **For more information** about preventing cyber crime, visit [www.churchmutual.com/cyber](http://www.churchmutual.com/cyber).



## Managing Your Risks

### Ladder Inspection Checklist and safety posters

An analysis of workers' compensation and liability claims involving Church Mutual customers showed that ladder-related, slip-and-fall accidents were a major loss driver. During calendar years 2009-2013, employees, volunteers and guests were involved in more than 870 ladder accidents costing upwards of \$13.8 million. Injuries to maintenance workers were responsible for the biggest share of the workers' compensation claims and associated dollar losses.

Trimming trees, painting, repairing roofs and changing light bulbs are just a few of the tasks that often require using a ladder. Because ladders are used frequently, it's easy for employees and volunteers to overlook potential hazards when using them.

To help address the proper use of ladders and related safety concerns, Church Mutual developed a new brochure entitled **Ladder Inspection Checklist**. The brochure outlines five key steps for using ladders safely:

- Choosing the right ladder
- Inspecting the ladder
- Correct set up
- Climbing and descending
- Using safe work practices

The brochure includes four tear-out copies of the *Ladder Inspection Checklist*. There also are four *Danger — Damaged Do Not Use* tags that can be attached to a defective ladder to warn others about its condition and to indicate it is out of service.

Six new safety posters were added to the risk control resources available to Church Mutual customers. These posters provide helpful tips for employees and others about preventing back injuries, kitchen accidents, strains and sprains and slips and falls on walking surfaces and from ladders. Also, information on making ergonomic adjustments to computer workstations is covered in one of the posters. To view, download or print copies of these and other safety resources, please visit [www.churchmutual.com](http://www.churchmutual.com).

Edward A. Steele  
Risk Control Manager

# Seasonal Spotlight

### Guidelines and screening help keep volunteers safe

Congregations often rely on volunteers to help tackle a wide variety of projects ranging from routine facility maintenance to emergency repairs. However, neglecting to clearly communicate volunteer expectations and responsibilities can open the door to serious injury and potential liability.

"Volunteers are generally more than willing to assist in any way possible, but that doesn't necessarily mean they are capable of doing the work," said Shari Ilsen, director of engagement at VolunteerMatch, a company that connects nonprofit organizations with volunteers. "Organizations have a responsibility to ensure a proper fit between project duties and a volunteer's capabilities."

#### Establish a volunteer manager

"Coordinating volunteer labor requires a central point person to ensure the process runs smoothly and safely," Ilsen said. "Appoint a volunteer manager who can oversee the planning and supervision of volunteers."

The volunteer manager is responsible for handling all aspects of volunteer labor within the organization, including screening potential volunteers, managing a volunteer database and reviewing projects to determine the scope and type of labor required.

"The volunteer manager needs to understand the skills and expertise available from the volunteer workforce and help appropriately match volunteers to projects," Ilsen said. "The manager also needs to recognize when it might be more cost effective or safer to hire professionals."

#### Develop a plan for every project

"Any project that requires volunteer labor should begin with a project plan that clearly establishes project guidelines and expectations," Ilsen said.

The project plan should identify any physically demanding work or specialized skills required, as well as how many volunteers are needed, the amount of time desired, and any special training or equipment required to keep volunteers safe.

"The plan also should include a description of the ideal volunteer candidate," Ilsen said. "This description identifies the expertise, physical ability and knowledge needed to assist with the work."

#### Screen volunteers

Volunteers should complete an application form that includes contact information, birth date, social security and driver's license numbers, previous work or volunteer experience, physical limitations, specialized training, first aid or CPR certification and insurance information.

If the volunteer is going to work with children, make sure a detailed background check also is performed.

- **For more information** about volunteer safety, visit [www.churchmutual.com/safetyresources](http://www.churchmutual.com/safetyresources).

# Q A

## A Perspective

*When an injury, accident or disaster occurs at the workplace, filing an insurance claim often is not your first priority. However, it is important to file a claim within 24 hours of an incident to receive the best care and protection for your employees and property. Risk Reporter spoke with Harry Shuford, chief economist at the National Council on Compensation Insurance (NCCI), about the importance of filing claims promptly and what is at stake when this process is delayed.*



### **Risk Reporter: Why is timely filing of an insurance claim so important?**

**Shuford:** Prompt reporting of an insurance claim is essential to effective risk management, as well as a fast claims handling and recovery process. Claims should be reported within 24 hours of an incident or one business day. You also need to file the claim within the time frame required by your state to avoid paying a fine. Remember that even minor incidents and injuries need to be reported.

In the case of injury, prompt reporting is essential in trying to limit the severity of an injury and in expediting recovery and an early return to work. For property claims, timely reporting can help reduce the potential for further damage.

### **Risk Reporter: What types of costs increase when there is a delay in reporting a claim?**

**Shuford:** A delay of any kind can mean additional property damage or injury resulting in additional costs. For example, a delay in reporting an injury often means a delay in proper treatment and that could result in additional medical problems and costs. For instance, a back strain that goes untreated could cause disc degeneration, spinal fusion and chronic pain.

For an employer and its workers' compensation insurer, a delayed claim can mean higher medical and indemnity costs, as well as the possibility of increased scrutiny by workers' compensation and workplace safety regulators.

### **Risk Reporter: Why is it especially important to file workers' compensation claims promptly?**

**Shuford:** Workers' compensation was created to protect workers and their families. Filing a claim promptly helps to minimize pain and suffering, eases anxiety, limits the possibility of permanent disability and expedites the return of an injured worker to work and earning a paycheck. Late reporting delays treatment and interferes with the objective of workers' compensation, which is to secure the best possible outcomes for injured workers and their families.

### **Risk Reporter: What is the importance of return-to-work programs for injured employees? How do they work?**

**Shuford:** Research suggests that extended time away from work is detrimental to a worker's future earnings potential. Early return-to-work programs enable injured workers to avoid these unfavorable outcomes by resuming gainful employment prior to their being physically able to return to their previous jobs. These interim jobs typically involve modifications to their previous assignments to accommodate any physical and medical limitations. Although early return-to-work programs are designed to offer financial, medical and emotional recovery for injured workers and their families, they also help enhance the relationship between the worker and the employer.

- **For more information** about filing timely insurance claims, visit [www.churchmutual.com](http://www.churchmutual.com), click on "Claims Center" and select "Importance of Prompt Claim Reporting."