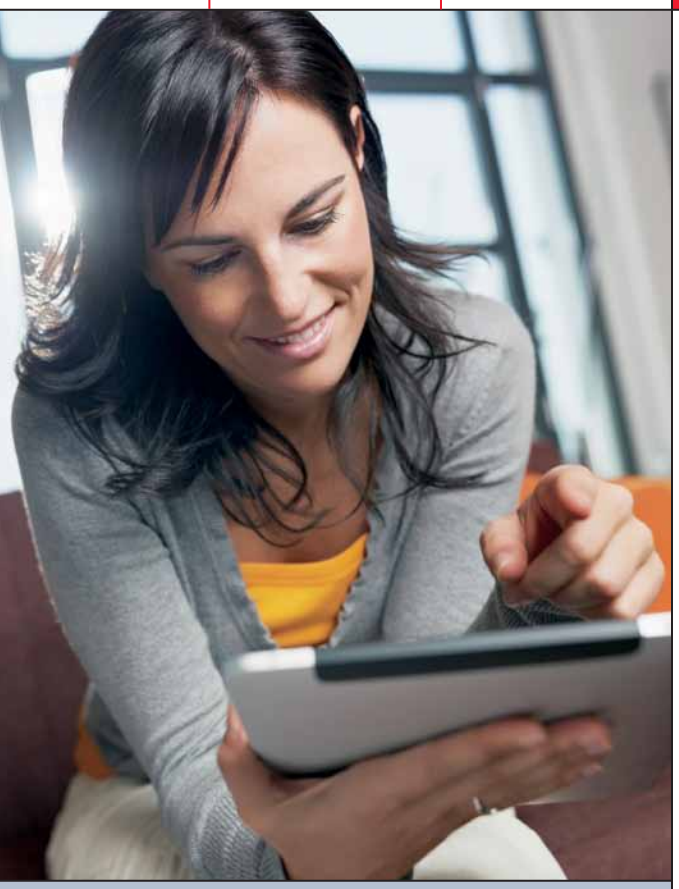
Risk Reporter

Winter 2014 | Vol. 13 issue 1

A quarterly publication by Church Mutual Insurance Company



Inside

Now get your quarterly *Risk Reporter* via email.

Sign up at *www.churchmutual.com/risk*.

Offering wireless Internet service for your congregation

Opportunities for ministry continue to grow as the technological landscape changes. Providing free wireless Internet can open many doors for a congregation and its members but not without risk.

"Wireless Internet is like air conditioning or sound reinforcement for a building. Although they're technically not required, they make almost any building a much more pleasant place to spend time," said Paul Clifford, owner and chief creative officer of TrinityDigitalMedia.com LLC and author of *Podcasting Church* and *Tweeting Church*. "Wireless Internet adds another dimension. It enables people with smartphones and tablets to access resources that could actually aid in your congregation's mission. It brings people in and encourages them to stick around."

Opening a wireless Internet network to your congregation or the general public can provide opportunities to serve the community in new and economical ways. Although the benefits are many, the congregation's leaders, in particular, should be aware of their exposure to the potential risks associated with the Internet access.

"One of the primary areas of concern when establishing a wireless Internet network is how the organization will protect itself and its members," Clifford said. "Congregations want to safeguard their own sensitive information and be protected against the actions of others using the network."

Security concerns are valid when providing wireless Internet to the public or congregation. Software could become infected with viruses or malware, or users could access and expose sensitive information.

In addition, a congregation faces liability concerns if a user knowingly or unknowingly uses the Internet connection provided to perform illegal and immoral acts that go against the mission of the organization. These concerns become even greater when youth members are involved.

"The risks associated with providing wireless Internet access are real, but the potential benefits for the congregation are tremendous," Clifford said. "It's important to address the risks and put a plan in place to ensure a safe and secure Internet experience for the congregation and the Internet users."

Minimizing risk

Minimizing risk is necessary when providing wireless Internet access to a congregation. One congregation that has accomplished effective policies to support wireless Internet usage is the Wisconsin Lutheran

(See Wireless Internet, Page 2)

cont.

(Wireless Internet)

Chapel in Madison, Wis. The chapel has implemented wireless Internet access as part of a comprehensive outreach program for college students.

The foundation of the successful student ministry at Wisconsin Lutheran Chapel is based on allowing students to use their facilities as a "home away from home," including free wireless Internet access and quiet spaces for studying.

"Keeping our data safe is paramount to being able to provide free wireless Internet to the local student population," said Matt Zuhlke, information technology coordinator for the Wisconsin Lutheran Chapel.

Zuhlke recommends that congregations begin by establishing a guest wireless network that is separate from their internal staff network.

"A separate guest network will help prevent unauthorized access to a congregation's data via the wireless network," Zuhlke said. "You also have the option to limit access to the guest network by requiring users to have a password to log in."

Password protection allows congregations to have additional control over who can and can't use the Internet access. You can restrict access to only congregation members — not visitors — or enforce age restrictions on the access.

"It also is important to take steps to manage the types of content guests can access when using the network," Zuhlke said.

Ask a networking expert or local IT network professional to configure the wireless router to allow web traffic only. This blocks access to other types of traffic, including file sharing services protecting the congregation from the possibility of users downloading pirated content.

"I also recommend using a web content filtering service to control the types of content guests can access. Router/firewall vendors, such as Juniper Networks and Cisco, will often offer content filtering as an add-on subscription service with their hardware products. Other companies, such as OpenDNS and Dyn, provide content filtering services that work to block access to undesirable content and protect Internet users from malware," Zuhlke said.

Taking these steps to set up a secure wireless Internet connection can prevent many of the risks associated with providing this free resource. However, in order to reduce the liability of the congregation in the event of improper use, an Acceptable Use Policy must be created.

Creating an Acceptable Use Policy

An Acceptable Use Policy helps minimize the risk a congregation faces when providing free wireless Internet services.

"The policy should clearly define the guidelines that must be followed when using a network connection provided by the congregation," Zuhlke said. "If you plan to offer wireless Internet, you need to have a policy established, and it should be displayed on the log-in page of the network."

Consider designating a staff member or qualified member of the congregation to act as a chief information officer who can work to establish the initial policy and then supervise usage of the network to ensure that any risks associated with providing wireless Internet are minimized.

An effective Acceptable Use Policy includes the following elements:

- Lists the contact information for the designated manager of the network.
- Outlines the types of usage that are prohibited (i.e., viewing pornography, gambling, illegal acts, downloading pirated content, installation of software, harassment, bullying, etc.).
- States the parental supervision requirements for minor children.
- Includes recommendations for staying up to date on anti-virus and anti-spyware software for any personal device using the wireless Internet network.
- Outlines expectations of online behavior in accordance with the mission of the congregation.
- Identifies consequences, such as loss of Internet privilege, if the guidelines of acceptable use are disregarded.
- Informs users that they are using an unsecured and public wireless network, and they should refrain from sharing sensitive or personal information.

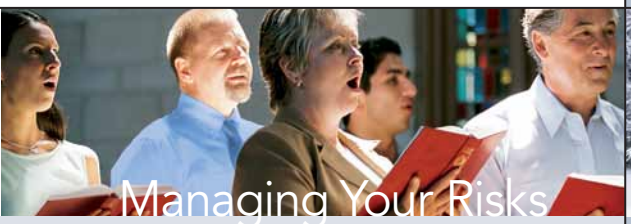
When creating an Acceptable Use Policy, keep in mind that other congregations can be a source of helpful advice. Ask an organization of a similar size and mission what they do to keep their congregation safe when providing wireless Internet.

"Remember that technology is constantly changing and so are the challenges associated with offering Internet access," Zuhlke said. "The person responsible for managing your wireless network needs to stay current on new security threats and usage trends. Any significant changes should be reflected in the congregation's usage policy and security measures."

Clifford notes that successfully implemented Internet systems share some basic characteristics.

"Make wireless Internet free and easy to use. Make sure that filtering and log-ins are not more restrictive than necessary and have a coherent usage policy," Clifford said. "Make sure you have wireless coverage everywhere in your congregation that people will use it and use the Internet as a tool for outreach whenever possible."

- **A sample Acceptable Use Policy** is available to Church Mutual customers at www.churchmutual.com/forms.



Managing Your Risks

Is your AED ready for an emergency?

Automated external defibrillators (AEDs) can be lifesavers if they are available for immediate use and in good working order.

According to the American Heart Association, hundreds of adults and children suffer sudden cardiac arrest every day in the U.S. The odds are that one may occur in your worship center, gym, fellowship hall or school. However, just having an AED in place and readily accessible is not enough — it must also be properly maintained, and you must have staff or volunteers trained to use it.

If you haven't looked at your AED in a while, now is a good time to check it over to make sure the device is in proper working order. It's very important to follow the manufacturer's recommendations for keeping the equipment ready for an emergency.

Usually, AED batteries need to be replaced every four years. Some AED pads have only a two-year shelf life, so be sure to check the manufacturer's recommendations.

A good place to start is to perform and document weekly checks to verify that each AED device is located in its designated storage spot, easily accessible and in good working order. A critical part of the status check is to make sure the battery is charged, and a supply of AED pads is available.

It is highly recommended that an AED log is kept for each unit to record the date and time it was checked. Any problems with the AED should be reported immediately to building/maintenance staff, so deficiencies can be corrected.

Congregations should designate key staff and volunteers — such as clergy, day care workers, ushers and choir members — so there are at least two AED trained people on site when the facility is in use. Designated volunteers and staff should complete a certified AED training course and keep current with their certifications.

To learn more about AED training courses, visit the American Red Cross website at www.redcross.org/take-a-class.

Edward A. Steele
Risk Control Manager

Seasonal Spotlight Winter

Keep boiler, furnace rooms clean and well maintained

Many congregations have storage issues. There are never enough closets or empty rooms to store all of the files, supplies, holiday decorations and other items that accumulate throughout the year. Although finding creative storage solutions is important, some areas are not safe storage options.

"Boiler and furnace rooms are designed with extra space to help keep the equipment running safely and efficiently," said Ernest Freeman, vice president of engineering at The Hartford Steam Boiler Inspection and Insurance Company in Hartford, Conn. "It's easy to want to fill this extra space with storage, but that can quickly become a fire hazard."

A fire in a boiler or furnace room can be ignited by an open flame or hot surface of the boiler and fueled by gas, oil, wood or other combustible items stored nearby. Combustible or flammable items should never be stored in the room, and nothing should be stored within 10 feet of the boiler or furnace equipment.

Signs of trouble

"Use your senses to help identify other signs that there might be potential fire hazards in the boiler or furnace room," Freeman said.

- **Sound** – Listen for loud noises coming from the heating system or fans. If the sound is noticeable or has changed since the last inspection, contact a maintenance professional immediately.
- **Smell** – Unusual odors are another sign of potential issues. Boiler rooms should be well-ventilated to avoid vapor concentrations. Sulfuric, sooty or smoky smells, as well as the smell of chemical compounds, such as chlorine or ammonia, can signify potential issues with airflow in the room.
- **Touch** – Excessive vibration or movement in the equipment and piping system can indicate pressure issues requiring maintenance. In addition, the equipment and piping should never feel hot to the touch (use a cloth when testing to avoid getting burned).

Equip the room

Boiler and furnace rooms should have self-closing fire-rated doors, fire-resistant walls and ceilings and smoke and fire detectors that are tested every six months.

"Don't rely on water for the fire extinguisher needs in a boiler or furnace room," Freeman said. "Keep a carbon dioxide or dry chemical fire extinguisher in the room."

- **For more information** about boiler and furnace room safety, visit www.churchmutual.com, select "Safety Resources" and click on "*Risk Alerts*."

Q|A

A Perspective

Collecting donations and offerings is a weekly, sometimes daily, responsibility for many congregations — and a role that is regularly entrusted to volunteers with little oversight or direction. Unfortunately, theft happens more often than many congregations realize.

Establishing a secure collection and handling process for donations is a simple way to protect one of your organization's most valuable assets. Risk Reporter spoke with Jack Cohn, treasurer for the Jacksonville Bible Church in Jacksonville, N.C., about the process they use to handle cash collections.

Risk Reporter: What security measures do you have in place to ensure the safe and secure handling of offerings?

Cohn: We ask our members to place their offering in a sealed envelope with their name and date written on the outside. Once the offering collection is complete, the money is immediately and directly transferred to the congregation office where the offering is counted. Knowledge of this location is limited to only those directly involved in the process.

Each collection is documented on a preprinted inventory balance sheet. The balance sheet accounts for every detail of the collection, including checks and cash denominations. The collection is counted twice by separate people, and the inventory balance sheet must be signed by both individuals. We perform this process after every collection.

Risk Reporter: Who is responsible for overseeing the collection process?

Cohn: My No. 1 rule for safe handling of the offering is that two people must be present at all times. We never allow a situation where only one person is handling the money — beginning with the collection of the offering during service through the deposit at the bank. Having two people present removes any suspicion and encourages accuracy.

Risk Reporter: What steps do you take to ensure safe storage of the money?

Cohn: After the documentation is complete, the cash is placed in a sealed moneybag and, ideally, immediately deposited at the bank. If that isn't possible, the money is stored in a safe that is kept in a locked office. Access to the safe is limited to only four people in our entire congregation.

If any additional accounting work is required before the money is deposited, a congregation elder or deacon must be present.

Risk Reporter: How is money securely transferred from your congregation to the bank?

Cohn: We try to deposit the money as soon as possible to minimize the risk of mishandling. If possible, we'll deposit the funds the same day as the collection. We also require that two people are present for the money transfer and deposit.

Risk Reporter: How do you recommend maintaining an organized accounting system?

Cohn: Beyond the inventory balance sheets we use to document collections, I recommend using accounting software that is specifically designed for congregations. Our system helps track all of our funds and budgets, making it easy to balance everything monthly. It is worth the investment and has helped us accurately monitor the flow of cash through our organization.

- Church Mutual offers a webinar on *Preventing Fraud and Embezzlement at Your Worship Center* available at www.churchmutual.com/safety; click on "Webinars."

Church Mutual INSURANCE COMPANY
Listening. Learning. Leading.®

Church Mutual Insurance Company | **www.churchmutual.com**
3000 Schuster Lane | P.O. Box 357 | Merrill, WI 54452-0357

Editor: Emilie M. Pierschalla | (800) 554-2642, Ext. 4120 | epierschalla@churchmutual.com
Risk Control Adviser: Edward A. Steele, CSP, ARM | (800) 554-2642, Ext. 4403 | esteele@churchmutual.com