Risk Reporter

Special Edition
for Places of Worship, Camps and Conference Centers

Fall/Winter 2015 | Vol. 14 issue 4

A quarterly publication by Church Mutual Insurance Company

Be aware

October is National Cyber Security Awareness Month

Protect your reputation from cyber crime

Make active assailant emergency planning a top priority

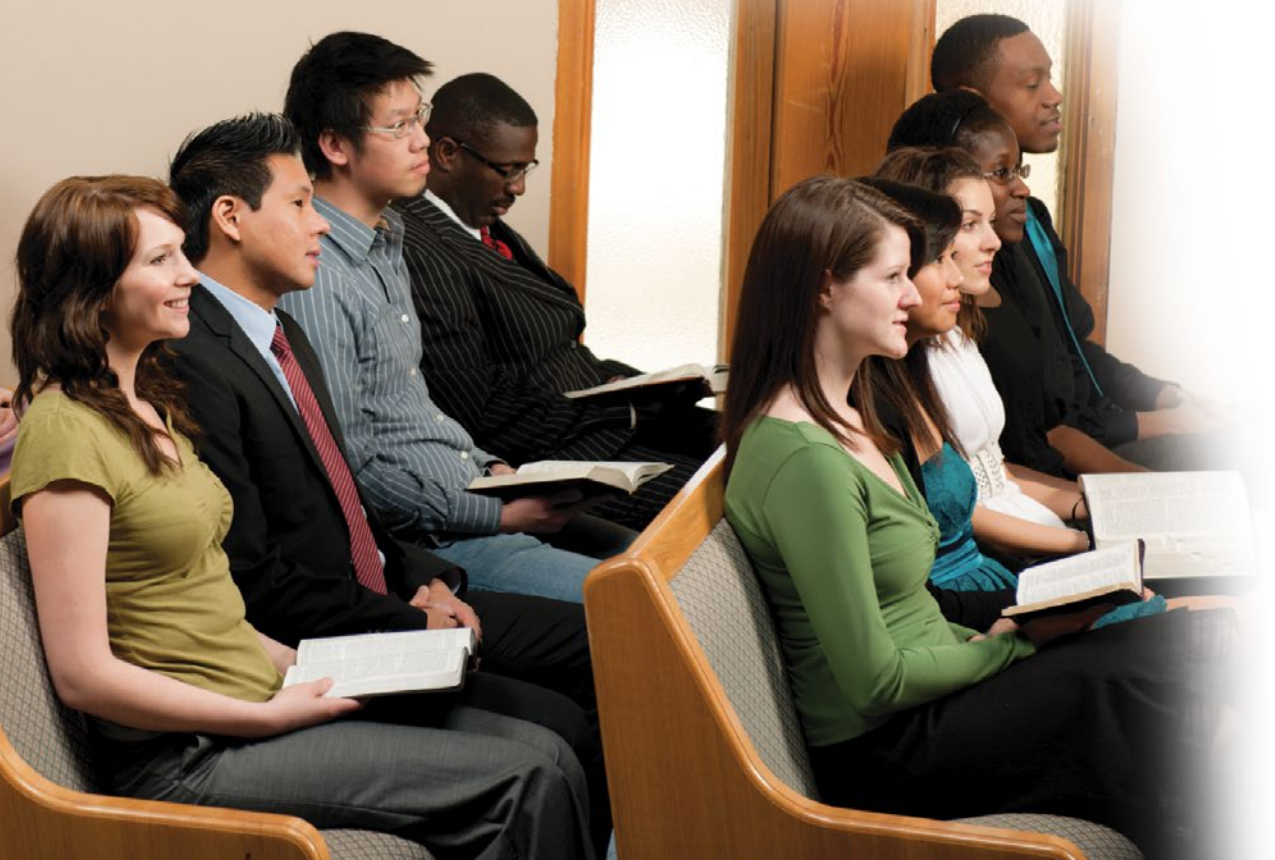
Take action to prevent child sexual abuse

Be prepared

Active assailant emergency planning for faith-based organizations

"Active shooter is a term used by law enforcement to describe a situation in which a shooting is in progress, and both law enforcement personnel and citizens have the potential to affect the outcome of the event."
— FBI 2014 Report

Today's religious leaders are keenly aware of the risk of violent attacks against faith-based organizations. As events over the last several years have shown, no faith community is immune. Attackers could focus their attention on individuals, locations or events. Victims might be targeted because of their religion, ethnicity, political or social views, or simply because they were in the wrong place at the wrong time. Perhaps worst of all, the chaotic, unexpected nature of such attacks can leave people feeling fearful and anxious in the very places where they would hope to feel treasured and safe.



There are specific actions your organization can take now to enhance security while continuing its larger mission of service to individuals, families and the greater community.

First, ensure emergency readiness

Put the right people and systems in place

Security and insurance professionals can work with you to assess key systems — lighting, backup power, alarms, fire suppression, security cameras, fencing and gates, doors, locking systems, etc. — as well as emergency policies and procedures. They can also work with you to ensure that employees and volunteers are properly screened before being hired.

Consider adding armed security

It's best to contact local law enforcement and seek out legal counsel before hiring armed security. In general, current or former law enforcement officers offer better training, skills and experience than private security company employees — but background checks should be used to screen and select specific individuals.

Then, focus on active assailant situations

Plan in advance

- Plans should incorporate facility lockdown and evacuation procedures, shelter-in-place locations, methods of communication during an incident and when buildings and grounds are safe.
- Address access and communications for the disabled or other special populations.
- Share your organization's plans with law enforcement and first responders prior to an emergency.

Train people to respond appropriately

There are three basic responses to an attack: RUN, HIDE or FIGHT. People can run away from the attacker, find a secure place to hide where the attacker cannot reach them, or overcome and incapacitate the attacker in order to survive and protect others from harm. As an event continues, those under attack could use more than one option.

It's natural for people under attack to be startled and to hesitate out of disbelief or denial. Use drills and training to teach people to respond immediately to an attack. The faster people respond, the faster they can get to safety.

Special considerations

In an active assailant incident, individuals must react swiftly, often without stopping to help the wounded. Members of faith communities might find this difficult, but doing so can save lives. You might find it useful to schedule a time for your congregation to meet and discuss such concerns. Congregants, staff members and volunteers might find it comforting to realize that their entire faith community is thinking how best to deal with a difficult situation.

Prepare for post-event management and intervention

Once a scene is secured, first responders will work with your staff members to transport the injured, interview witnesses and initiate an investigation. Your organization should have an emergency response team in place to help law enforcement, rescue workers, victims, family members and staff members. Post-event planning should also address communications with the media and the public.

Make sure you're covered

Your Church Mutual insurance agent can help you plan for the worst while hoping for the best. If you have questions about liability or coverage related to active shootings or other emergencies, contact your agent directly. For assistance with safety planning, contact our Risk Control Consulting and Research Center at (800) 554-2642, ext. 5213, or riskconsulting@churchmutual.com.

For help screening job applicants and volunteers, we recommend our corporate partner Trusted Employees. Contact the company at trustedemployees.com or (877) 389-4024.

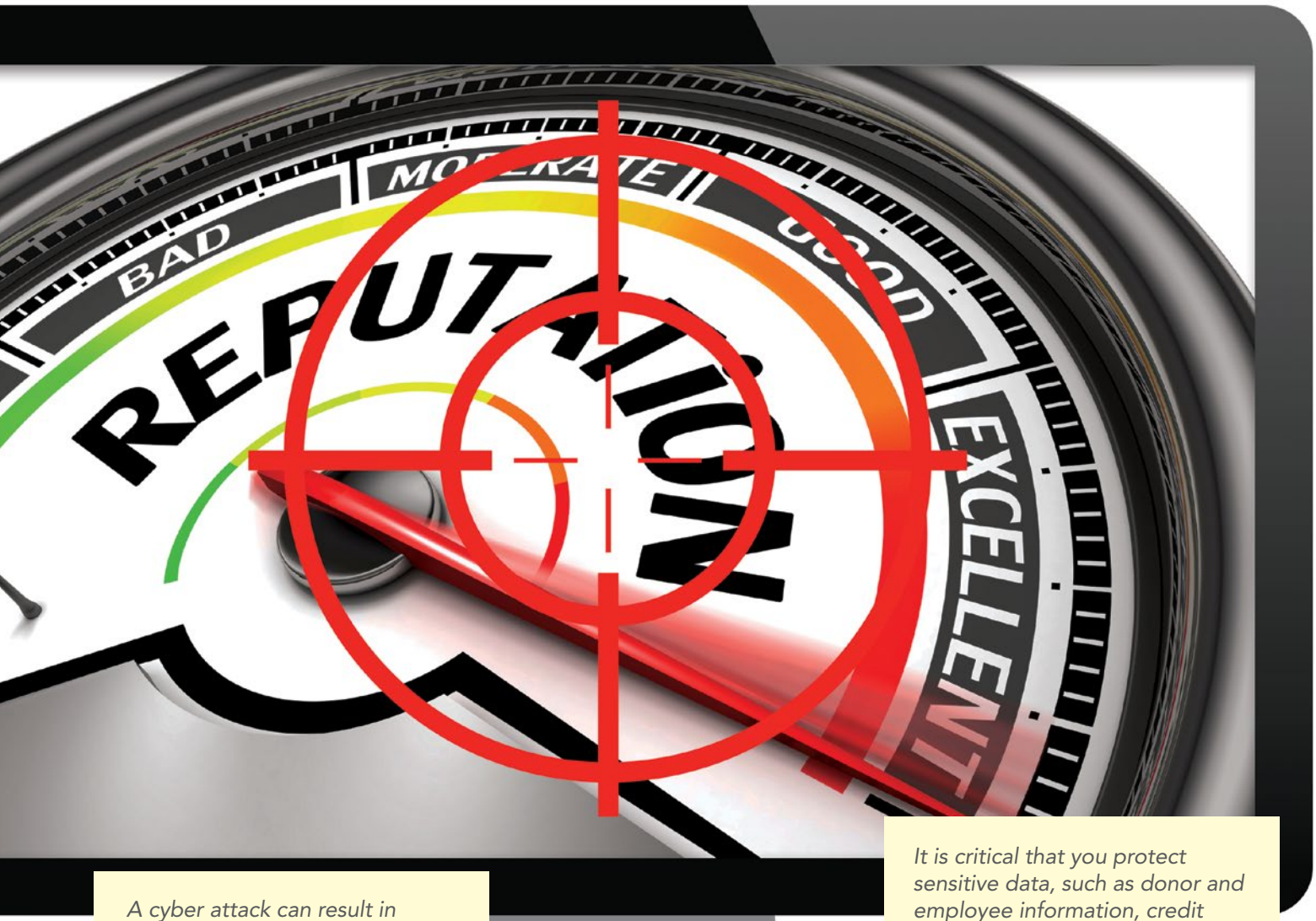
PROMOTING AWARENESS

- Ask congregants to report suspicious behavior
- Ensure confidentiality so people feel safe about reporting
- Make sure staff know how to respond to any reports or concerns
- Train staff members and volunteers to spot and respond to potentially risky situations

Be aware

A cyber attack can result in devastating reputational damage

As your organization becomes more dependent on the Internet as a primary channel for doing business, storing congregant and employee information and conducting both personal and business interactions, your risks of becoming a primary target for a cyber attack increase.



A cyber attack can result in not only financial loss but also loss of confidence and contributions, reduction in camp and conference participation and reputational damage.

It is critical that you protect sensitive data, such as donor and employee information, credit card numbers, and even medical information about members, attendees and employees.

> "We now live in a world that is more connected than ever before. The Internet touches almost all aspects of everyone's daily life, whether we realize it or not. Recognizing the importance of cyber security to our nation, October has been designated as *National Cyber Security Awareness Month.*"
>
> — U.S. Department of Homeland Security

Understanding the real costs of a cyber attack

It is almost impossible to predict the probability of a cyber attack and the costs associated with the loss and mitigation of it, but understanding the overall real cost of an attack can help inform your security strategies, investment decisions and insurance protection.

Direct costs resulting from cyber crime

In considering the consequences of cyber crime, you must take into account direct losses to individuals as well as your organization. The costs of responding to cyber crime include compensation, regulatory fines, costs associated with legal or forensic issues, and possible payments to victims of information/identity theft.

Indirect costs associated with cyber crime

Indirect costs include such factors as reputational damage to your facilities, personal damage to employees and members, loss of confidence in your ability to conduct cyber transactions and reduced revenues because of decreases in contributions or camp and conference participation.

The costs of preventing cyber crime

There are very real costs associated with cyber security, which could require implementation of protection and detection methods, heightened physical and technological security, cyber crime insurance, changes to ensure compliance with regulatory and/or industry standards and employee training. These costs, however, are both foreseeable and far more controllable than the costs of suffering a cyber attack.

Special considerations

The trust and confidence of your members, attendees and employees is a cornerstone of your success. The greatest obstacle to cyber security for most faith-based organizations could be a perception that they are not vulnerable because of their size or their mission. That isn't true. Cyber criminals search for the easiest and most vulnerable targets — and there continues to be a dramatic rise in cyber attacks on small organizations.

Stay ahead of cyber threats

Protecting your organization against cyber attacks requires continued investment in technology, education and training. You will need to maintain an ongoing focus on policies and processes to stay ahead of cyber criminals — and protect your congregation, your staff members and your organization's standing in the community.

We're here for you

Our cyber crime liability insurance and protection services focus on your protection and include prevention education, coverage for both electronic and paper data loss or theft, identity theft and post-loss data recovery.

For assistance, contact your agent directly, visit churchmutual.com or contact our Risk Control Consulting and Research Center at (800) 554-2642, ext. 5213, or riskconsulting@churchmutual.com.

For help screening job applicants and volunteers in order to reduce the possibility of internal threats, we recommend our corporate partner Trusted Employees. Contact the company at trustedemployees.com or (877) 389-4024.

Follow industry best practices – create a culture of security

- Monitor applications with access to data
- Establish role-based access controls
- Collect detailed logs and report data
- Use only strong passwords and change default passwords
- Maintain security patches and updates
- Utilize user activity monitoring
- Develop and enforce policies on mobile devices and remote access
- Implement an employee cyber security training program
- Enhance background screening of all staff and volunteers
- Implement measures for detecting compromises
- Develop a cyber security incident response plan

Be alert

Preventing child sexual abuse in youth programs

From daycare programs to summer camp, children's choir to youth sports, active programs for families and children are a welcome, even essential, part of modern worship. Unfortunately, youth activities can also provide prime opportunities for child sexual abusers to target and gain access to victims.

Disclosure Among Victims

- Not all sexually abused children exhibit symptoms.
- Disclosures [of abuse] often unfold gradually and could be presented in a series of hints.
- If they are ready, children might then follow with a larger hint if they think it will be handled well.
- Disclosure of sexual abuse is often delayed; children often avoid telling because they are either afraid of a negative reaction from their parents or of being harmed by the abuser.

Source: "Raising Awareness About Sexual Abuse: Facts and Statistics" The U.S. Department of Justice, NSOPW

Addressing the problem

While child sexual abuse may be an uncomfortable topic, it is important for faith leaders to tackle the problem head-on. An abuse scandal connected to a house of worship or other faith-based operation can have devastating effects:

- Damaged reputation
- Loss of public trust
- Loss of members and financial support
- Unexpected legal expenses
- Lawsuits brought by victims and their families

Taking steps to prevent child sexual abuse can help protect your organization as well as the children and teens entrusted to your care.

Making the decision to act

Faith communities might hesitate to discuss child sexual abuse in the mistaken belief that prevention might be difficult or costly, might lead the public to believe a problem already exists or because of fears that abuse will be discovered.

Leaders need to educate themselves, staff members, volunteers and congregants about the benefits of prevention:

- Well-defined youth-protection policies could reduce liability.
- Uncovering problems sooner rather than later might limit negative impacts.
- Thirty-five percent of child sexual abusers were abused themselves, so prevention can break the cycle.

Perhaps, most importantly, preventive measures can support a faith community's mission to serve and protect all of its members.

Key components of a prevention plan

The Centers for Disease Control (CDC), working in concert with experts in the field, has identified six key components of prevention programs for youth organizations. These components are not separate "steps" but rather facets of an integrated and cohesive approach.

- Careful screening of applicants for any staff or volunteer positions involving contact with children and youths.
- Detailed policies and guidelines for adult-youth and youth-youth interactions.
- Safe physical environments that limit opportunities for abuse.
- Empowerment of employees and volunteers to monitor/report abusive behavior or breaches of policy.
- Defined responses to abuse allegations or suspicions, including: reports to authorities; restriction or suspension of alleged abusers; and restorative practices to support victims, their families and others.
- Training to help employees, volunteers and youths understand abuse.

This overview is based on the CDC handbook *Preventing Child Sexual Abuse Within Youth-serving Organizations*, which is available for download at cdc.gov.

Let us help

Please feel free to contact Church Mutual with any questions about liability or insurance coverage related to child sexual abuse, youth programs, etc. For assistance, contact your agent directly, view youth safety videos at churchmutual.com/videos or contact our Risk Control Consulting and Research Center at (800) 554-2642, ext. 5213, or riskconsulting@churchmutual.com.

If your organization needs help screening job applicants and volunteers, please contact our corporate partner Trusted Employees at trustedemployees.com or (877) 389-4024.

WARNING SIGNS OF POSSIBLE ABUSERS

Keep an eye out for adults or older children who display these behaviors:

Personal space

- Ignore social, emotional or physical boundaries
- Refuse to let children set limits on interactions

Sexual behavior and conversation

- Use sexual language to describe, tease or insult children
- Mistake gestures of friendship or affection as being sexual in nature
- Minimize harmful or hurtful behaviors when confronted

Relationships with children

- Turn to children rather than adults for emotional or physical comfort
- Share inappropriate personal or private confidences with youths
- Secretly interact with children or teens through games, texting, emails, phone calls, etc.

Church Mutual Insurance Company
Listening. Learning. Leading.®

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

Editor: Amy M. Kimmes | (800) 554-2642, Ext. 4529 | akimmes@churchmutual.com
Risk Control Advisor: Edward A. Steele, CSP, ARM | (800) 554-2642, Ext. 4403 | esteele@churchmutual.com

Risk Reporter

Fall/Winter 2015 | Vol. 14 issue 4

A quarterly publication by Church Mutual Insurance Company

Church Mutual Insurance Company
3000 Schuster Lane
P.O. Box 357
Merrill, WI 54452-0357