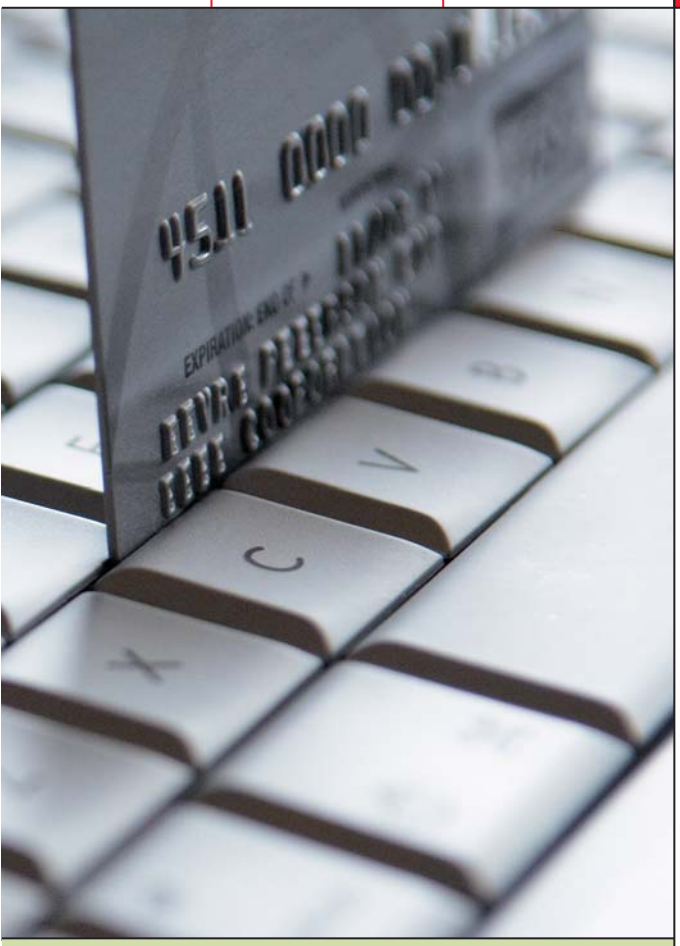
risk reporter

Spring 2008 | Vol. 7 issue 2

A quarterly publication by Church Mutual Insurance Company



Protecting precious personal information

More than 8 million U.S. adults were victims of identity theft in 2007, costing Americans roughly $49 billion. As the threat of identity theft grows, it is more important than ever for places of worship to re-evaluate their security procedures to protect the personal information of the organization and its members.

Information evaluation

Assessing and controlling identity theft risk begins with a personal information audit of all congregation papers and electronic files.

"Inventory all computers, flash drives, disks and paper files," said Beth Givens, director of Privacy Rights Clearinghouse, a nonprofit consumer information and advocacy organization in San Diego, Calif.

Review how personal information enters and leaves the organization and what type of information is captured and recorded. Create a document that identifies the different types of information the organization stores and how each is used. The list should include information categories, such as names, addresses, birth dates, Social Security numbers and driver's license numbers.

"Review the list and determine if all the information is vital to the organization," Givens said. "Properly dispose of unnecessary information categories and stop collecting it."

Reduce, regulate and protect

"Limit the amount of personal information collected to only what is absolutely necessary," said Sol Bermann, chief privacy officer for the state of Ohio's Office of Information Technology.

"A person's name, Social Security number and date of birth are the key elements for identity theft," Givens said. "Only keep this type of information as long as required and dispose of it securely when it is no longer needed."

"Paper documents are just as vulnerable as disks and computers," Bermann said. "Store all documents, files and computers in a locked file cabinet or a locked room."

Remind employees and volunteers not to leave sensitive files out and unattended.

(See personal information, Page 2)

inside

cont.

(personal information)

"Computers used to collect sensitive information should have a firewall and virus protection," Givens said. "The information also should be password protected and ideally encrypted for better security."

Employees should log out of computers when they are not in use. Regularly run anti-virus and anti-spyware software on computers and network servers. Store electronic files on computers without Internet or e-mail access.

The hiring process for personnel who will have access to this information is also important. Perform reference checks and background checks for these employees. Also, require employees to sign a confidentiality and security standards agreement.

"Restrict employee access to personal data to only what they need to know," Givens said.

Have access procedures in place for employees who might leave or no longer need access. At the very least, change or delete passwords and collect keys.

"Provide ongoing security training for employees," Givens said. "Use training sessions to educate staff about new security risks and discuss recent violations."

Document disposal

Properly disposing of sensitive information is just as important as storage. Once information is no longer needed, it should be disposed of in a way that it cannot be read or reconstructed.

Paper records, credit cards and even disks can be destroyed using a shredder.

"Invest in quality, cross-cut shredders and make them available in key areas of the organization," Givens said.

"Remember to place a shredder next to the photocopier and fax machine."

Disposing of computers and hard drives requires extra precaution because simply deleting sensitive files is not sufficient.

"Invest in a wipe utility program for computers that will overwrite the hard drive," Bermann said, "or use a company that specializes in disposing of computer equipment and files."

"Hard drives also can be physically destroyed by the organization or by a company specializing in data destruction," Givens said.

Detecting a security breach

It is important to have measures in place to detect a breach in security before it results in identity theft. Consider installing an intrusion detection system on computers housing sensitive information. In addition, monitor outgoing e-mails and traffic for signs of a violation.

"Be conscious of any change in the way a computer is running," Bermann said. "If the settings have changed or the data is displayed differently, this might signal a breach."

"Ask parishioners to inform the worship center if they become victims of identity theft, especially if it involves an account kept on file with the organization," Givens said. "If two or more individuals report identity theft, it could indicate a breach in security."

Develop a plan

When a security breach occurs, it is important to have a plan in place to respond to the incident, reducing the potential impact on the organization and members. Designate a team to review the security policies and develop and implement the response plan.

"Investigate security incidents immediately, assume the worst and act accordingly," Bermann said. "If a breach did occur, the first step is to notify those who are affected."

Consult with an attorney when developing the response plan. Many states have laws that identify who needs to be contacted and the time frame for when they must be contacted.

Identity theft coverage

Church Mutual now offers Identity Theft Case Management Service and Expense Reimbursement coverage at no additional cost with its multi-peril policies. This coverage protects your organization's leaders, combining identity theft insurance with valuable recovery services designed to help victims restore their credit history and identity records. For more information, contact your Church Mutual representative at (800) 554-2642.

Resources

- The Federal Trade Commission offers a detailed business guide to protecting personal information at www.ftc.gov.
- The National Crime Prevention Council also provides a guide to preventing identity theft available at www.ncpc.org.
- A checklist of responsible information-handling practices is available from Privacy Rights Clearinghouse, visit www.privacyrights.org/identity.htm.
- For more information on intrusion detection systems, visit www.sans.org.
- For security tips, quizzes and employee training information, visit www.OnGuardOnline.gov.

Managing Your Risks

Armed security

Although not a new problem, violence at worship centers is escalating and garnering more media attention than ever before.

Late last year, a gunman entered a church in Colorado Springs and shot and killed two members of the congregation before an armed security person at the church shot the gunman.

News of this incident was featured on the front page of many daily newspapers, and national news programs carried the story for days. Violence of this magnitude has occurred at worship centers before, but the media attention was never this intense. And no incident before this has ever convinced so many religious organizations to consider an armed security force.

During the last few months, Church Mutual has received numerous calls from customers looking for advice about arming their security team. The decision to approve taking deadly force at a house of worship is not easy. There are many issues an organization's leadership needs to discuss before making the decision.

To provide some guidance to our customers, Church Mutual assembled a panel of security experts to discuss the pros and cons of an armed security team at a worship center. Chester Quarles, professor of criminal justice at the University of Mississippi and author of *Crime Prevention for Houses of Worship;* Ron Aguiar, director of safety and security at Southeast Christian Church in Louisville, Ky.; Bob Klamser, a 24-year veteran in law enforcement in California; and Carl Jensen, assistant professor in the Department of Legal Studies at the University of Mississippi and retired FBI agent with 22 years of experience, agreed to provide their expertise on this issue.

Read the outcome of the panel's discussion and words of advice in Church Mutual's Risk Alert on armed security. It is found on our Web site, click on "Safety Resources," "Risk Alerts" and select "Armed Security."

The Risk Alert is not designed to sway your decision — just to provide the necessary information for you to make an educated decision.

Richard J. Schaber, CPCU
Risk Control Manager

seasonal spotlight

spring

Lock-in plans for safe overnight events

From movie nights to national conferences, congregations are finding enjoyable ways to integrate faith into the lives of their youth. One of the more popular activities is an overnight or "lock-in."

Through a fun-filled evening of activities, youth have the opportunity to share their faith with friends and worship in a casual environment. However, with this fun opportunity comes the responsibility to ensure the safety and well-being of each participant.

"Organized planning and open communication are keys to the success of an overnight or lock-in event," said Bethany Hannon, youth ministry director at Unity Palo Alto Community Church in California. "Once you've determined the event location and schedule, it is possible to manage any potential problems that might arise."

Adult supervision and facility layout are two essential areas to address during the planning process.

"We require at least two adults to supervise all events, regardless of participation," Hannon said. "However, the number of chaperones should be proportionate to the number of participants. We recommend at least one adult for every 10 teenagers and more for younger youth."

Additional chaperones of each sex should be available to accompany younger participants to restroom facilities.

Discuss appropriate behavior with chaperones, parents and participants before the event and require each participant to sign a contract for a "code of actions" in order to attend.

"Remind chaperones and participants of rules the night of the event," Hannon said. "Chaperones also should be responsible for conducting a head count once every hour."

It also is important that the location allows for separate sleeping quarters for girls and boys. In addition, at least two chaperones of the same sex should supervise each sleeping area.

Additional planning tips

- Require each participant to turn in a signed permission slip and medical release form with emergency contact information
- Develop an emergency response plan
- Keep at least one first-aid kit at the event site
- Chaperones should be trained in first aid and CPR
- Require all participants to have a parent or guardian provide transportation after the event
- At least one chaperone must remain until all participants have been picked up

q|a

A Perspective

Electronic payments and donations are increasingly popular for places of worship. However, many newcomers to online giving have questions about the risks and benefits associated with sharing personal information.

Risk Reporter spoke with Dave Montgomery, senior consultant at ServiceU, a company that provides electronic donation and payment software designed for organizations, such as worship centers, nonprofits, schools, universities, festivals and theaters.

Risk Reporter: How popular are requests for electronic-giving capabilities?

D. Montgomery: Very popular. ServiceU saw the volume of transactions processed increase 90 percent from 2006 to 2007. Donors are clearly doing more online giving now than in previous years. People also are increasingly comfortable with online giving, and it's an easy way to give even if you missed worship that week.

Risk Reporter: What are the advantages of electronic giving?

D. Montgomery: There are numerous benefits. For example, if someone misses a service, they can make a donation automatically online. For those who are committed to tithing, it's a simple way to make sure that donations are made on a consistent basis.

Risk Reporter: Is electronic giving secure?

D. Montgomery: Absolutely. In fact, electronic giving can be more secure than traditional methods. Many electronic-giving programs are designed to provide everything you need for online registrations and payments in a completely hosted solution — no programming required. This system is secure because no personal information is kept at an organization's office. It also allows donors to print receipts at their own convenience for tax purposes or budgeting.

For organizations still accepting checks, additional safety measures are required to secure account routing numbers, names, addresses, telephone numbers and even driver's license numbers printed on most checks.

Risk Reporter: What are best practices for securing personal information?

D. Montgomery: Ensure that the electronic-giving service is accredited and has the necessary credentials synonymous with secure transactions. For example, look for a service that is a Level One, the highest standard, with the Payment Card Industry (PCI). The PCI has six standards and 12 requirements for businesses securing personal information.The standards are: Build and Maintain a Secure Network, Protect Cardholder Data, Maintain a Vulnerability Management Program, Implement Strong Access Control Measures, Regularly Monitor and Test Networks and Maintain an Information Security Policy.

Risk Reporter: What tips can you share for starting an electronic-giving program?

D. Montgomery: Look for a company that not only fits the congregation's needs but is easy to set up and maintain, provides effective reporting options and has stringent security policies. The provider should house personal information off-site from the congregation to ensure maximum safety of sensitive credit card information. Then educate the congregation that electronic giving is available and that it is a safe, viable option.

Spring 08

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: Richard J. Schaber | (800) 554-2642 Ext. 4587 | rschaber@churchmutual.com