ZURICH®

Church safety solutions

February 2007

Special points of interest

- Computer threats
- Making sense of risk reduction
- Lessons of loss–learn from others that have been there

Inside this issue

Next month!
Ladder safety and working on elevated surfaces

Computer security–are you at risk?

Protecting computer systems from theft of financial records, personal information and preventing access to inappropriate Web sites should be a part of any church's risk protection strategy. First, the church administrative business committee should consider implementing a process to evaluate and monitor access to church computers. Access to computer systems should be controlled through use of unique login id's and passwords. The church administrative business committee should also consider appointing a member of the congregation or board of trustees to function as a computer system administrator. This person can help provide oversight to the protection of church records and systems and help ensure

frequent password changes are required at least every three months. Where possible, computer users should be assigned to a single workstation. Allowing free access, though well intended, can compromise the computer system's anti-virus protection. Ask your appointed

(Continued on page 2)

Don't fall victim to computer hacking

The moment you make your church's Web site accessible through the Internet, it is possible that you have unintentionally provided the world a window into your local network and confidential information. Church Web sites are often a target for anti-Christian attacks. Some computer hackers may be content with simply altering your site's home page by replacing it with obscenities, while others steal your entire database of financial information and church member directory. Essentially, there are three basic concerns for Web site security including identity theft, Web site vandalism and eavesdropping Internet data. There are a number of ways for church administrative committees to minimize potential for hacking that include both administrative controls and oversight, as well as engineering the system's design and anti-virus software to look for and isolate attempts to gain unauthorized access from both external and internal sources.

(Continued on page 3)

Computer security–are you at risk? *(continued)*

Don't leave confidential information out on the desk.

system administrator or computer service provider to ensure the system's antivirus protection software is current. Churches should establish a policy of appropriate use of church computer systems and further restrict user access to inappropriate Web sites, chat rooms, personal e-mail services and free access Web spaces.

Why is antivirus software necessary?

There are over 55,000 known viruses. Each year businesses lose an estimated $13 billion in damages related to virus attacks. More sobering, over 250 new viruses appear each month. Churches that fail to use and update antivirus software are at risk of a complete loss of data or possibly allowing hackers access to personal information. Churches should assess their current antivirus software and ensure it is robust enough to meet the full spectrum of threats associated with the demands of the system. If you use the antivirus software that came with your PC, it may only be a consumer version lacking the full range of protection offered by a business version.

What additional steps can I take to protect my computer system?

- Don't allow users to give out e-mail addresses to people they don't know.
- Don't open attachments from messages sent by unknown sources.
- Ensure the antivirus software detection runs in real-time to prevent viruses from being copied to your hard disk.
- Only browse the internet using secure Web connections.
- Use an antivirus software program that has the ability to detect and eliminate viruses embedded in ActiveX and Java.
- Don't use floppy disks of unknown origin.
- Use the Ctrl-Alt-Delete locking function of the computer when leaving the workstation unattended to prevent others from gaining access to your computer.
- Don't record passwords and make them accessible to others.
- Don't leave confidential information out on the desk.

Risk reduction makes sense

Why should churches bother with controlling risk?

After all, isn't that what insurance is for? Isn't a church supposed to be focused on their ministry? Of course, but the two go hand-in-hand and allow churches to focus on there primary mission.

Consider the following argument. If church leadership fails to take into account the risks associated with opening their doors to the community, they could fail to serve the purpose of their existence. Think of the costs associated with repairing a building following a storm or the adverse actions that could result from internet theft or vandalism. Rather than expanding the ministry, church communities may find themselves financially burdened paying for losses.

The purpose of managing risk is to provide for the continued success of the organization. The least expensive means of controlling insurance costs is to prevent the loss from ever happening.

When church leadership becomes involved in protecting people and property, they will enable the ministry to fulfill its primary mission to the community.

Don’t fall victim to computer hacking *(continued)*

Hackers have shifted their focus to exploiting security products, which is why it is important to create a system with layered firewall protection to restrict external access. The system provider should be able to provide a variety of choices to meet everyone’s budget. Computer system data should also be backed up daily to ensure the most current version of data is maintained. System administrators should also investigate using a business version of antivirus software rather than solely using the preloaded home-user versions of the antivirus software.

Unless flaws are fixed quickly, hackers can potentially gain access to data being backed up by organizations using such programs. There is also an increase in vulnerabilities in software that power devices for moving traffic around the Internet, such as routers and switches. Peer-to-peer file-sharing programs for trading music online continue to be carriers of spy ware and malicious “bots,” computer code that can commandeer personal computers. Instant messaging and playing digital media are also considered to be at risk applications.

First, oversight. Trust, but verify. One of the surest ways to prevent internal information theft or inappropriate use of computer systems is to ensure system usage is controlled and monitored by more than one person. Giving one person sole responsibility for computer security can spell disaster if that person ever leaves the organization.

Ensure financial records, banking information, payment information, payroll and financial statements are protected from unauthorized access.

Churches should build into their policies and procedures a written security policy for acceptable computer use. This security policy should succinctly lay out the organization's policies with regard to:

- Who is allowed to use the system
- When they are allowed to use it
- What they are allowed to do (different groups may be granted different levels of access)
- Procedures for granting access to the system
- Procedures for revoking access (e.g. when an employee leaves)
- What constitutes acceptable use of the system
- Remote and local login methods
- System monitoring procedures
- Protocols for responding to suspected security breaches
- Use of filters to reduce access to unauthorized software
- Caution related to unprotected wireless networks

One of the surest ways to prevent internal information theft or inappropriate use of computer systems is to ensure system usage is controlled and monitored by more than one person.

Lessons of loss

Church employee prosecuted for computer access theft

A former employee of a church in Alabama was sentenced to one year and six months in federal prison without parole and was ordered to pay $12,300 in restitution to the church for computer access theft.

The defendant was employed as the church's system administrator. The church business manager discovered a financial discrepancy on the books. While investigating, it was discovered that $500 was missing from a services account. The local police department ran background checks on all church employees that had access to church records and discovered a felony conviction against the church computer system administrator not reported on his job application. The administrator was released from his position because he lied on his application.

That Saturday, while working in her office, the church business manager was suddenly logged off her church computer and found she could not log back on. All accounts on the network had been disabled and could not be accessed.

Church leadership was unaware the former computer administrator had connected to the church via remote access from his own personal laptop computer. During his trial, the former computer administrator admitted he established a remote connection to the church and had used the unauthorized access to initiate a program that locked out or disabled every user of the system with the exception of his own account and the administrator's account.

The computer invasion was highly disruptive to the operations of the church. Full access to the system was not restored for three months, costing the church over $5,000 to hire consultants to repair the network and re-establish account access.

The former church computer system administrator pled guilty to unauthorized computer intrusion. This case was investigated by the Federal Bureau of Investigation and prosecuted by the Assistant U.S. Attorney.

Preventive steps to consider:

- Ensure oversight through the church administrative or business committee.
- Conduct background checks on individuals who will have access to church computer systems.

References

Zurich Services Corporation Risktopics

United States Department of Justice Web site

http://www.cybercrime.gov/cccases.html

http://www.us-cert.gov/cas/tips/

http://kids.getnetwise.org/

If you have any questions, please send them to:

churchsafety.solutions@zurichna.com

Zurich Services Corporation

1400 American Lane, Schaumburg, Illinois 60196-1056
800 982 5964 www.zurichservices.com

Zurich Services Corporation
Risk Engineering

Because change happenz℠

ISO 9001:2000
Quality-Assured Solutions Provider

(01/07) 06-4154

ZURICH®