How secure are the computer systems at your church or office?
Church IT Security Essentials

Hackers and others are always seeking vulnerable targets that can be easily infiltrated. Have you given any thought to how secure the computer systems are at your church or school office? Utilizing several easy steps will create a safety net around computer systems and the information contained on them.

Continue reading...

Em português

Fire Safety Webinar

September 21st 2:30 pm EDT

When the Alarm Sounds

By Arthur F. Blinci,
VP Chief Risk Management Officer at Adventist Risk Management, Inc.

SPACE IS LIMITED

Reserve your Webinar Seat Now at:
https://www1.gotomeeting.com/register/246700025

You hear them coming, with sirens and lights -- those selfless servants and heroes, the men and women who we call fire rescue personnel. This coming month (October) our safety focus is on fire prevention awareness. Learn how you can help make your church and school a fire safe facility. The actions you take today, may save a life - when the alarm sounds.
Title: When the Alarm Sounds
Date: Sunday, September 21, 2014
Time: 2:30 PM - 3:30 PM EDT

BAD THINGS COME FOR THOSE WHO WAIT.

Insurance industry statistics show that delays in claim reporting causes difficulty in resolving claims and increases the cost.

24/7 HOTLINE: (888) 951.4276
CLAIMS@ADVENTISTRISK.ORG

Copyright © 2014 Adventist Risk Management, Inc. All rights reserved.
You are receiving this email because you opted in at our website or someone signed up on your behalf. If you did not sign up for this list or wish to discontinue receiving correspondence from Adventist Risk Management, Inc., please click on the ‘UNSUBSCRIBE’ link.

Our mailing address is:
Hackers and others are always seeking vulnerable targets that can be easily infiltrated. Have you given any thought to how secure the computer systems are at your church or school office? Utilizing several easy steps will create a safety net around computer systems and the information contained on them. A discussion on computer security can go into great detail regarding the various aspects to protect technology. This doesn't do much good if it is all talk and no action is taken. Without knowing a starting point it can be easy to become paralyzed to take action. Let's look at computer security from a vulnerability point of view.

Your church members can be scammed simply by access to your church member list. You may not consider that there is anything of much importance on the local church computers. However, you may be surprised how the information that is there can be used in a variety of bad ways when accessed by people with malicious intent. Your church members can be scammed simply by the church member list falling into the wrong hands. For example, using the church members list, which includes phone numbers and addresses, a criminal can contact church members to sell goods and services that may not even exist. However, when these perpetrators know and use names of other church members, it lends them credibility.

How can you help prevent this? Start by using a firewall. Never connect your computers directly to the DSL or cable modem. There are many types of firewalls and just as many price ranges for them. Talk to your church IT department or ask others what they use to provide even basic intrusion protection for church computer(s). Don't use the default credentials. Be sure to change the passwords using 10 or more digits that include numbers, upper and lower case letters, and special characters if you can.

Is your firewall the only way someone can gain access to your computers? A wireless network is one of the most vulnerable connections to your church computers. Anyone using your wireless connection can gain access to the same information as described above. It is also possible for users to access inappropriate content using your wireless and possibly even store this content on church computers potentially leaving you liable.

How can you help to prevent this? Start by using two separate wireless networks, one for church business and one for your church congregation. Many affordable access points now come with the capability to provide both a business and guest network connection for wireless users. Also, be sure to change all wireless passwords on a regular basis, at least four times per year or more. In addition, consider changing the wireless network names (SSIDs) at least once per year. Finally, be sure to keep the business wireless network hidden.

How many people have keys to your buildings? How often do you find doors at your church left unlocked? If individuals have physical access to computers, they may obtain access to sensitive information that on them. If your computers are stolen the culprits will have unfettered access to all of the data stored on them.

How can you help to protect your computers and the data that resides on them? Be sure to use usernames and passwords on all computers. Remember to change the passwords frequently. Beside the concern for sensitive information to be accessible to the wrong people, there are often those with malicious intent who don’t care about your member list. Instead, they seek pleasure by erasing all recorded sermons or other important church business files. Think about the time it would take to rebuild all of that data, if it was even possible.

What about theft? To protect all information on computers, you may want to consider encryption of all computer hard
drive(s). There are many affordable or even free hard drive encryption applications that can protect your data in the event that the computer is stolen.

**Backups, Backups, Backups.**
Remember in all cases, you should maintain backups of your data that, if possible, can be stored offsite in a secure location. In the event that any of the disaster mentioned above or others occur, you do not want to have to rebuild from scratch.

There are many other pieces and depth to a robust security plan. The basics outlined above are a good place to start. Once these are in place the security plan can grow from there.

by: TONY VARGAS
**MANAGER, INFORMATION TECHNOLOGY**
Adventist Risk Management, Inc.