Cyber Risks and Information Technology in Churches

By Mike Mwemba

During visits to most churches today it is easy to witness the extensive use of technology in worship services, as well as the daily operation of the church. Laptops, iPods, music, and communication audio equipment, high cost video recording cameras are readily visible in the sanctuary. For operations, accounting, and word processing software and the use of various databases make the daily work much easier. An area in which churches are advancing is the storage of member information on databases, which may or may not be kept onsite.

Today many laws require organizations/institutions to ensure that data stored in databases and that which is in transit via the Internet, email, faxes, etc. is properly protected. The need for data protection in churches becomes paramount, with an unstable legal environment where class action litigation exists and regulatory impositions from the Federal Trade Commission and states’ Attorney Generals’ offices are a common feature.

What has caused this increased advent to security and privacy exposure risks? Some commentators point to the information age. It first began with the industrial age, which
involved mass production and a need for physical protection of assets such as tangible property, plant, and equipment.

As time progressed, mass customization began to evolve. This led to the use of information assets, such as computer systems, data, and intellectual property. This was the birth and growth of the information age.

Today we live in an information age where the use of technology has become a way of life. Cell phones, television, Internet, and computers/laptops are common everyday tools. It has led to growth and increase in the use and reliance on technology by both individuals and businesses. At a minimum level, this is an indicator that institutions do depend on and use technology. It implies that non-profits such as churches are just as likely to use technology.

The question must then be asked, “What precautions should the church take when dealing with technology?” One feasible option is to ensure internal controls are robust enough to prevent any data or security breaches. Types of data security risks and privacy exposures to consider include missing backup tapes, stolen laptops, hacked computers, viruses, dumpster diving, accidental exposures due to errors or omissions, and employee misuse including sabotage of data systems.

For the church, primary information exposures include personally identifiable information, such as names, residential addresses, and telephone numbers of church members. The church may sometimes have databases that include dates of birth, and in some instances may collect information via online payments through the use of credit cards or PayPal.

Each of these risks creates potential exposures under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) laws and regulations, Federal Trade Commission regulations, Securities and Exchange Commission regulations or through requirements for the maintenance of internal procedures or good internal controls as mandated under the Sarbanes Oxley Act of 2002, Section 302.

These laws and others impose heavy responsibilities and penalties on data management and control. For example, HIPAA requires national establishment of standards for electronic health transactions and national identifiers for providers, health insurance plans, and employers. The church as an employer is affected by provisions of this Act. Since churches depend on the goodwill of their members for financial, social, and spiritual support, any loss that could seriously impact the church’s mission requires proactive action to prevent its occurrence.

Unauthorized or accidental release of protected information requires both best practice and legal compliance to redress the problem. In the event of a data breach, there are notification laws that apply in approximately 46 states, Puerto Rico, and the District of Columbia. These include credit monitoring for at least a year, as well as restoration laws. These requirements are based on the location of the consumer, not that of the organization where the data breach occurred.

Several and serious high profile data breaches have been reported in the press over the last six years. For example, in 2007, TJ Maxx had the largest cost of computer data breach in corporate history, estimated at the time to be $256 million. Thieves are believed to have stolen more than 45 million customer credit and debit card numbers. In April 2011, Sony experienced a data breach within their PlayStation network. It is estimated that information of 77 million users was compromised. In January 2008, GE Money, a division of General Electric, disclosed that a magnetic tape containing 150,000 social security numbers and in-store credit card information from 650,000

continued on page 4
Facebook is making changes to your newsfeed once again.

Newsfeed images have taken over, and they are more prominent than ever. Cover images will now appear like stories. For example, if a friend likes a page, you will now see the page’s thumbnail and cover image in your feed. Also, there will be a dedicated image feed that will showcase images from your friends and the pages you like.

Here are a few suggestions:

1. Redo your cover image monthly
2. Start getting creative with ministry photos and link them to specific content on your site and your blog.
3. Make sure your images are high quality

Additionally, if you are a ministry blogger, make sure you include a quality images with your content that Facebook is able to pick up. Linked images will appear larger in news feeds now and will serve as a good hook to attract new visitors to your content, when shared.

Facebook is also streamlining design on all mobile devices so all users have a similar experience.

The images your ministry shares are like the sign outside of your church. Make them look good and engaging and more people will connect with your content.

So what does all this mean for ministries? Simply put, focus on uploading great images. Images are going to define your ministry on Facebook.

---

 Damian “Chip” Dizard operates an online video tutorial website, WebVideoChefs.com, where he shows people how to make better videos.
Frenita Buddy is the production director for Hope Channel. She formerly was a producer for Hope Chanel.

Justin Kim is the communication director for the Michigan Conference. Prior to accepting this position, Justin was director of public campus ministries for the Michigan Conference.

Diane Thurber is the associate director of communication for the Lake Union Conference. She formerly was the assistant communication director.

Two of the top four awards of the National Communication Association convention, including the Lambda Pi Eta division, were awarded to Pacific Union College students this year at the NCA annual event. Three of the students and PUC communication professor Tammy McGuire traveled to present their research at the convention. Pictured are Tammy McGuire, Janna Vassantachart ('12) and Jordan Thornbourgh ('12).

Cyber Risk, continued from page 2

retail customers was missing from an Iron Mountain Incorporated storage facility. This list of data breach cases is not exhaustive, but it does highlight the extent of the problem and the need to secure data from all types of losses.

To mitigate the potential for cyber risk liability, the church through ARM is embarking on an education campaign that will draw attention to the need to better protect data kept on information technology systems. Discussions with insurance carriers are ongoing to secure insurance protection for cyber liability risks. The subject of cyber liability risks is too complex to cover in a general article. Future articles will explain the difference between Cyber Risk Liability insurance coverage and the standard insurance protections offered under the more traditional property policies.

Mike Muemba, CFE, MBA, MS, FCII, is manager of placement services for Adventist Risk Management, Inc., and is a qualified chartered insurance practitioner and certified fraud examiner. Reprinted with permission from Solutions, Adventist Risk Management’s free risk management newsletter.