

Layers of Protection

© 2007 by Nick B. Nicholaou, all rights reserved

President, Ministry Business Services, Inc.

Reprinted from *The Clergy Journal*

We are all masters of risk management! You may not have thought of yourself that way, but it's true! You began learning how to manage risk when your parents taught you that you shouldn't touch something hot because it would burn you. In elementary school you learned to avoid the school bully because any encounter with him or her could hurt. So all through our lives we've learned how to manage risk. And, as risk managers, we need various layers of protection from those things that could hurt our ministry's computer systems.

Power

Power problems come in two flavors—power irregularities (spikes, brownouts, and blackouts) and “dirty power”. The solution for both lies in relatively inexpensive UPSs (Uninterruptible Power Supplies).

UPSs are essential for servers, switches, and routers, and they're optional for desktop workstations (notebook computers already have them built in!). The key is that UPSs connected to our servers must communicate with them to shut them down when their batteries get low. Their configuration should also turn the servers back on when power is restored. Our firm's favorite UPSs are APC *Smart*-UPSs (see www.apc.com) which come with the software and cables necessary to protect and communicate with servers.

Smart-UPSs have batteries that keep systems running for a time, but they are limited if your organization experiences prolonged outages. However, they can bridge the gap between when your power goes out and your generator kicks in, allowing you to buy a generator that takes a little longer to come online, which will save you money on that purchase.

Desktop computers don't usually get UPS protection, but should always have surge protectors to help protect them from spikes that could overheat some of their components. Surge protectors should be UL listed and replaced periodically since every surge they absorb weakens them. Our firm recommends replacing them when new computers are purchased.

Web Content

One of the most dangerous risks our teams face is temptation when they're connected to the Internet. Affecting both males and females, giving in to that temptation has ruined many lives—even those in ministry. In fact, if someone is in ministry they are under greater spiritual pressure, so eliminating this issue is an important part of risk management.

There are generally two strategies to help protect our team members when they're connected to the Internet—content filtering and accountability software.

Web filtering works fairly well, and if there are students who access the Internet through your organization's system it should definitely be used. One of our favorite solutions for this is SonicWALL's (see www.sonicwall.com) content security management device. These work great for browsing the Internet. For email content, we like Barracuda's SPAM Firewalls (see www.barracuda.com), which keep most spam from getting to users' email accounts.

These solutions also protect from viruses, but virus protection should also be in place on desktop and notebook computers. Our favorite solution for this is McAfee's anti-virus software (see www.mcafee.com). It is capable and leaves the computer's operating system alone.

The problem with these filtering devices is that the challenge is constantly changing, and those who are driven to get around them can. So we believe a wise decision is to also add accountability software to each computer. Our favorite is Covenant Eyes (see www.covenanteyes.com). It records every place a user goes on the Internet and sends a report to their accountability partners with scores that are extremely helpful in changing the way users think about Internet content.

Manufacturer Error

The best protection from manufacturer errors (like failed hard drives) is to make sure you have a good backup. We recommend backing up your entire server five nights/week, having enough tapes to save at least 2-3 weeks of backups (that means at least 10-15 tapes), and taking one tape off-site each week in case of a larger disaster. These backups should also be tested periodically to make certain they're working correctly.

User Error

Recent studies show that, for the first time, users are a bigger threat to our systems and data than are malicious software attacks like viruses. All of the above help in this area, but consider also adding a desktop / notebook cloning solution like Symantec's Ghost (see www.ghost.com) to re-establish desktop and notebook configurations that have been “broken” by their users. By configuring a local computer and then using this product, you will have the ability to re-write local hard drives in minutes, quickly making them usable again. The key to this strategy is to make certain all data is being saved to the server hard drive since anything saved to the local drive after the Ghost image was made will be lost.

Those Who Intend Us Harm

- *System Security.* A good password policy and strategy is essential in today's ministry workplace. Our systems contain sensitive data and must be protected from those who try to harm us. The policy needs to address:
 - Password strength,
 - Prohibition of group logins, and
 - Prohibition of sharing passwords.
- *Server security.* Servers should be in rooms or cabinets / racks with limited key access. Their security will keep someone from being able to easily steal or tamper with them. Also, they should
 - Be on a dedicated electrical circuit,
 - Be air conditioned, and
 - Be located in a convenient location for the person responsible for changing the daily backup tapes.

Making certain these layers of protection are in place make your systems more reliable and available for your ministry team members, and that will mean more ministry and, thus, more reached for Christ.

Nick Nicholaou is president of MBS, a consulting firm specializing in ministry computer networks, operational policies, and CPA services. You can reach Nick via email (nick@mbsinc.com) and may want to check out his firm's web site (www.mbsinc.com) and his unofficial blog at <http://ministry-it.blogspot.com>.