

Reasonable Network Security

© 2008 by Nick B. Nicholaou, all rights reserved

President, Ministry Business Services, Inc.

Reprinted from *Christian Computing Magazine*

Church and ministry networks have unique security needs. Many mistakenly approach network security in our niche like they would a club or hobby, and thus don't go far enough to protect our data and our team. Others mistakenly go so far they impede the team and increase their support call volume unnecessarily. We have worked or consulted on hundreds of networks in churches and ministries, and we have developed an approach that protects and empowers while minimizing support needs. I'll share it with you so you can enjoy the same results.

We Are Vulnerable!

There are those who want to hurt us! Whether they're hackers, disgruntled former employees, or internet programs (bots and other malware), our systems are vulnerable. Our systems have full-time internet connections that offer an opportunity to those on the outside to cause damage.

We also have system users who accidentally delete files, introduce malware, or lower our security protection by sharing their passwords. Some question why we need to be so protective.

The first step in reasonable network security is the regular reminder to staff that we have sensitive data on our systems—contributions information, payroll information, social security numbers of staff, counseling notes, and more—that we are required to protect on behalf of those who could get hurt if that information were made public. System users need to keep their passwords confidential, not sharing them with anyone on the team other than the network administrator.

Biometrics Anyone?

Many are beginning to use fingerprint readers instead of passwords to improve network security. The cost is minimal; in fact, Dell is now shipping systems with these devices at no extra cost when asked to! The benefits include no one being able to use another's network username, including team members' kids!

Off-Site Access

Most churches and ministries have staff that need to access the network from off-site. There are a number of ways to accomplish this; the best is via Microsoft's Terminal Services. Any network running Windows Server 2000 or newer has this feature available. It allows approved users to access the network from off-site as though they were sitting at a desk on the campus and connected to the network.

The benefits are:

- It's very fast! The only data that gets transmitted is monitor images, keystrokes, and mouse movement.
- It's very secure! All the data stays on your network servers! Security can even be improved more by adding a security certificate, which we strongly recommend.
- It's very inexpensive! You already own the technology, all you have to do is configure it and show your team how to use it. And since it's all server-based, there's no need to keep workstations running and using electricity like some other solutions.

Firewalls

A firewall on a network is a protective barrier that blocks harmful things. We recommend three solutions that address different needs:

- *SPAM Firewall.* If your system is in any way typical, more than ninety percent of the email that hits your email server is SPAM. It is essential that network users be protected from SPAM

because a lot of it contains malware and other schemes intended to harm them and/or you. Our favorite SPAM firewall is from Barracuda Networks (www.barracudanetworks.com). Their devices are very capable and reasonable in price.

- *Access Firewall.* Who—or perhaps better stated—what should have access to your system? In addition to controlling which team members can access your system from off-site, it is necessary to protect your system from internet programs (referred to as 'bots') that are constantly looking for server and system vulnerabilities. Our preferred access firewalls are from SonicWALL (www.sonicwall.com). They have the ability to completely secure your system from intruders, and are well worth the expense.
- *Internet Accountability.* For most, internet filtering is not necessary. But for all, internet accountability is! The difference is helping those on our team to *want to* avoid any inappropriate internet content even when no one is watching. The best solution we've found to accomplish this is from Covenant Eyes (www.covenanteyes.com). Their software does not filter content (though they also offer that option). Instead, it sends easy-to-read accountability reports to those holding system users accountable (we recommend at least two: their supervisor and their spouse or parent, etc) with scores that highlight inappropriate sites. They have special pricing for church and ministry teams so that it's very affordable, and we consider it essential on all ministry-owned systems.
- *Internet Content Filtering.* For those with schools or who offer public internet access through wireless cafes, etc, internet content filtering is a must. Again, we recommend SonicWALL's solution for this. The good news is that it's all done through the same device as access filtering!

Local Workstation Rights

An area where many go beyond what's necessary is local workstation security. We have found that an easy way to empower users is to give each user local administrative authority. This does not mean they have administrative authority on the network; only on their local computer. This eliminates a large percentage of support calls and keeps users from feeling like they're fenced in.

The potential dangers are that users might install something they shouldn't or that they would do something that requires rebuilding their system. Training can help the first (though that risk never completely goes away), and using a strategy employing software such as Symantec's Ghost (www.ghost.com) to build local workstations reduces the cost of the second threat.

Backup, Backup, Backup!

Enough can never be said for the responsibility to ensure the most critical data is backed up daily and a copy stored off-site at least weekly. This may be the network administrator's most important responsibility because it ensures the ministry's data will not be lost in a catastrophe.

That's our strategy! And anyone can do it! I hope it helps you and your team to do more for less, and to do it more reliably and without distraction.

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 website (www.mbsinc.com) and his unofficial blog at <http://ministry-it.blogspot.com>.