

# Managing Security vs Controlling Users

© 2007 by Nick B. Nicholaou, all rights reserved

President, Ministry Business Services, Inc.

Reprinted from *Christian Computing Magazine*

Computers and data networks are vulnerable, and wise IT Directors establish policies to protect them. They are guided by their research and experience in protecting these systems that contain valuable and sensitive data. But many go further than necessary, and without ever intending to, frustrate their staff. So let's talk about some 'best practices' ministry security strategies.

## The Challenge

Developers of malware (malicious software) love to exploit computer operating system weaknesses and control computers around the world for their benefit. In the form of viruses, trojan horses, spyware, root kits, and more, these programs get into computers via the Internet and email and wreak havoc.

To serve their teams well, IT Directors must do all they can to protect computers from these attacks.

## The Problem

While at a Church IT Roundtable recently, a colleague who supports ministries nationwide told the IT Directors in the room that for years he has felt they go further than necessary in locking down local operating systems. I chimed in because I have felt that way too, and have proven through the many clients we serve that locking local operating systems down is unnecessary in most cases.

Local computers are those where users do their work, and are in contrast to servers which users never work at and to which their local computers connect.

Their thinking is that if users don't have administrative authority on their local systems, they can't install any software, malicious or otherwise. So they keep users from logging into their local computers with administrative credentials. That protects them from malware and keeps them from installing software for which they don't have a license.

The result, however, is that many users get frustrated when they visit a website and are told that they need to update a browser utility to view the site, or a friend tries to share a file with them on a USB drive that needs to install a driver to be accessible. In both cases, the user won't be able to install the necessary software without the intervention of IT staff. Thus this policy contributes to the perception of IT staff as people who keep ministry teams from doing what they need to. Users feel controlled.

## Strategies Worth Considering

The concept of protecting local systems is important, but locking their operating systems down misses the IT purpose of serving and supporting teams well. So our firm set out to provide the same protection without frustrating users. Here's what we came up with, and by the way, it really works:

- To allow users to install software updates, etc, as needed, we automatically log each user into their local computer with administrative authority. It only affects their local computer. That local authority is very different than their network authority where they are restricted as to which files and folders they can see, modify, and/or delete.
- Because logging them in locally as administrators increases their malware vulnerability, we established a three-part strategy to protect them and keep them productive.
  1. Install a high-quality virus protection program locally on every computer. We chose McAfee ([www.mcafee.com](http://www.mcafee.com)) because it leaves the local operating system alone and only does virus checking, leaving as much RAM and processing capability as possible for other functions. We also run all email through Barracuda Networks' SPAM Firewall ([www.barracudanetworks.com](http://www.barracudanetworks.com)) to eliminate viruses and SPAM.
  2. We modify the registry (the registry is the operating systems' database that tells it how to run) to have all software save files to the network rather than to the local hard drive or desktop. For those using notebooks, we install a utility, SmartSync Pro ([www.regsoft.net](http://www.regsoft.net)), that very reliably copies new or changed files to the network every time they connect and login. In addition to improving the disaster recovery and business continuity strategy, this also means that local hard drives have very little on them that is unique and/or necessary.

3. This is the part that is our failsafe protection. We use a configuration distribution tool, Ghost ([www.ghost.com](http://www.ghost.com)), to create hard drive images and distribute them as needed. In addition to dramatically reducing the time necessary to deploy new desktop and notebook computers, this also allows us to bring an infected system back online in 10-15 minutes. So, if someone's computer gets infected with malware we can't quickly resolve, we can just rewrite the hard drive.

This three-part strategy allows us to give users the local rights they need to get their work done while also giving us a quick path to fix a system if it has problems. It also has the benefit of reducing the IT staff workload.

## Yea, But...

In that Roundtable there were churches represented with dozens— and even hundreds!— of computers on their networks. And they were skeptical. But I told them our firm manages dozens of networks that include thousands of computers. Almost every one of our desktop and notebook computers are set up this way, and it works very well. I encourage you to consider this strategy which will reduce your IT staff workload, improve your disaster recovery and business continuity strategy, protect your computers, and help your team feel they are not being controlled.

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](mailto:nick@mbsinc.com)) and may want to check out his firm's web site ([www.mbsinc.com](http://www.mbsinc.com)) and his unofficial blog at <http://ministry-it.blogspot.com>.