

# Ten Common Management Mistakes: And How to Avoid Them

By Dirk A.D. Smith

Network World, 06/09/2003

Source: <http://www.nwfusion.com/research/2003/0609mistakes.html>

Your job is to keep the network up and running, so employees can work without interruption and so that you can get home at a reasonable hour. The problem is that things don't always go the way you want them to go. Some days just plain stink. There are many reasons, but we'll just stick to the 10 most commonly encountered network management potholes.

## 1. Using interruptible UPSs.

One shop was squeezing the last life out of its system. The elderly server could barely keep up with the demands of the shop, and management refused to even update the battery in their UPS, something that should be done every couple of years.

One day there was a power outage. The UPS was so old that it could not control the server in a safe power down. The battery had lost so much of its power that it too went quickly. As a result, the RAID controller failed, bringing down the server.

The shop was 100% dependent on this server for daily operations and transactions. It took three days to recover the server, and it took the company much longer to recover the lost revenue. A \$75 battery would have prevented the failure.

## 2. Not packing a kitbag.

The call came in to corporate headquarters saying the server was down in a branch office. The network administrator flew out of his office to help. After driving for an hour, he rushed into the server lab and dove into the problem. He found a section of corrupted operating system files. All he had to do was reinstall the operating system. The onsite network administrator had no idea where the CDs were. No problem, the visiting administrator had a set he could use - back at his office an hour away, two hours round-trip.

Pack a kitbag and leave it by the door (or in your car). Everything you might need, from copies of every operating system in use by your users to a roll of duct tape, should be in that bag. This is simple to do, costs little and can mean the difference between updating the operating system and updating your résumé.

## 3. Failing to patch.

A toy manufacturer had file connection problems on its server. The situation degraded to the point where staff members lost all access to their files, and manufacturing stopped for two days. Revenue losses were skyrocketing. The newly hired network administrator stepped up to solve the crisis. He quickly found that the previous administrator had not installed patches since the server was installed three years earlier. The problem the manufacturer had was a known issue that had been resolved two years earlier by one of the patches.

Patch kits are free. While they might be a bit unwieldy, they are generally pretty simple to deploy. Any system administrator could have done it. Apparently, the departed administrator had said that because the system was running fine, there was no need to patch.

## **4. Making bad "good" backups.**

A medical office's server that held medical documents and patient history crashed. Office operations ceased because no information could be accessed. The network administrator immediately grabbed a copy of the last good backup and prepared to rebuild. Her heart sank when she found that the tape was empty. She checked the others: blank.

She checked the office logs and found that her staff had been changing tapes every day for two years, but they were put into a server that had no back-up software because no one had ever loaded the software. The tape drive wasn't even connected internally. No one knew that the backups were no good because they never checked. They had never even done a test restore. They just changed blank tapes for two years.

After two days of work, she salvaged the database, but the office lost a huge amount of money. Any onsite database administrator easily could have prevented the problem with a simple back-up check. They are doing this now. Daily.

## **5. Not using a licensed cabling guy.**

A bank's network was failing constantly. An inspection of the phone closet revealed a bird's nest of wires of different sizes, shapes and lengths. Additionally, the cabling guy had jammed RJ-11 and RJ-12 voice plugs into the many RJ-45 sockets in the patch panels. Not only were the connections poor, but they were falling out constantly. To remedy the situation, the cabling guy had jammed toothpicks in each socket to hold the connectors in place.

Many network problems can be traced to improper cabling. Be sure to have cable installed by a licensed, bonded and insured cabling contractor.

## **6. Failing to check under the hood.**

A professional sports team bought a high-end, brand-name server, but it started having problems. The network administrator called for help from the operating system vendor and the hardware vendor. It turned out the reseller that provided the "brand" server had filled it with nonbrand memory and nonbrand disk controllers, and linked it to a set of nonbrand external disk drives, all because the components were less expensive.

The hardware vendor and the operating system vendor refused support because the server was polluted with nonbrand components, and the configuration was not certified. Your network operating system vendor only promises to provide support for certified, tested servers that were certified and tested as a unit, not as a collection of parts.

## **7. Skimping on warranty contracts.**

An office spent a pile of cash on its first fault-tolerant server last year. The system had a RAID Array 5, dual power supplies and 24-7 support. After a year, a drive choked.

The 24-7 guy arrived. He called the hardware vendor, who asked for a warranty contract number. The office had not bought a warranty contract. "No problem," the vendor said. "They still have two years left on the out-of-box warranty, and that includes 'next business day or best effort.' I can get a replacement drive to you in five or six days."

Fault tolerance is not enough. Make sure you have full, onsite 24-7 support. Then go to an office-supply store and buy labels. On each one write the warranty contract number and support phone numbers, and then stick them on each machine.

## 8. Not using a test environment.

A few years ago, a software development company installed a new workstation. It was loaded with RAM, hard-drive space and the fastest processor around. It was the president's new workstation. Shortly after installation he accepted a request from his largest partner company to test a new satellite communications board. The result was blue screen. After he picked up his jaw from the office floor, he restarted the box. Nothing. After rebuilding the system, it took four days to get most of the kinks out.

Another company, run by a more knowledgeable president, had a test network built. Before upgrading to a new patch kit, they would try it on the test network. They would find mistakes, reset the network and do it again and again, until it was flawless. With all of this documented, they would move to the production network and deploy the upgrade.

The president of the first company doesn't run tests on his own box anymore.

## 9. Planning for incapacity.

When the theater arts company bought a new server five years ago, it could hold six 8G-byte RAID Array 5 drives. To save money, the company insisted on getting four 4G-byte drives. The network administrator pleaded, saying they would need more space before long. The bean counters compromised and added two more drives, thus filling the chassis.

After three years they ran out of space, so badly that they were deleting files as small as 50K bytes. They looked at getting new drives. The 8G-byte drives were no longer made, and the server would not support larger drives. A new external subsystem would cost more than the original server. They replaced the server two years earlier than they had planned.

Capacity planning is deliberately buying more hardware than you need. This includes more disk space, memory and processor power. Doing this, you won't have to fund a serious upgrade when your server reaches its half life. This forethought adds about 10% to the cost of the server. Compared with a new system or serious upgrade, the 10% upfront is chump change.

## 10. The X-factor: users.

The office power went out late in the afternoon. The nervous office manager was certain it would damage their two servers, so he took fast action. He walked over and turned off the servers. He went home with the sure knowledge that his quick action averted a crippled office network.

The next morning, he returned to work and turned on both servers. Nothing.

The servers were in the middle of a series of complex updates to critical files when he hit the power buttons. He had zapped the boot drive on one and corrupted the disk volume holding the most critical database on the other. It took two days to repair the network.

Of all the problems that plague a network administrator, none can be more daunting than users from hell. Of all the problems to protect your network from, these are the most unpredictable.

## We want your tales!

Of course, these are just a few of the tales of network woe. We'd like to hear from readers about administration horror stories, savvy system advice or request for specific topics. Send tales to [dirk@alexander.com](mailto:dirk@alexander.com).

## **RELATED LINKS**

Smith is president of Alexander LAN, in Nashua, N.H. Industry veteran Allan Hurst also contributed to this report.

All contents copyright 1995-2003 Network World, Inc. <http://www.nwfusion.com>

Management research center

Latest management news, analysis and resource links.

<http://www.nwfusion.com/topics/management.html>