

Five Top Dos and Don'ts of Network Management

By Bruce W. Roeckel

<http://www.immaculatetechnology.com>

Keeping your business running smoothly means having a network that's stable and secure. But even minor oversights and errors can cause big problems; cybercriminals are becoming more sophisticated, and they're increasingly targeting smaller businesses that aren't as likely to have the security that a large enterprise would have.

Luckily, good security doesn't have to be complicated or expensive. There are a few relatively simple dos and don'ts you can follow to help ensure your security bases are covered. Here are our top five:

1. Don't forget backups and recovery

You know you need to back up your business data, but in the long list of IT priorities, it sometimes ends up lower down the list than it should be. And beyond the physical act of performing backups, your business should have a comprehensive disaster recovery plan. It should include strategies for detecting and diagnosing problems, and the actions needed to repair the problem and get your system up and running as soon as possible, with little or no data loss.

2. Do install security updates and patches

According to a June 2008 survey by IT security firm Sophos, 81% of the corporate network endpoints they tested failed one or more basic security checks, including missing Microsoft® security patches, disabled client firewalls, or missing endpoint security software updates. And the results can be devastating. "Ultimately, machines that fail such a test represent 'low-hanging fruit' for cybercriminals and a real danger to their corporate networks," said Bill Emerick, vice president of product management for Network Access Control at Sophos. So don't delay or skip those updates and patches — they're an integral part of keeping your network secure.

3. Do manage passwords properly

There are a lot of ways in which password management can go awry. Two of the most common are not changing the default passwords on all network servers and other devices, and sharing a password among multiple devices. Do we really even need to explain why these aren't good practices? Probably not, but a surprising number of IT departments don't bother to address these two simple issues, instead of leaving their networks vulnerable to attack and misuse.

4. Do educate your users

While large enterprises almost always have relatively comprehensive IT policies and user education initiatives, this is an area where smaller businesses often don't pay enough attention. Usually, responsibility for maintaining and securing the network falls to just a few people (or maybe even one person) — but network safety should be everybody's responsibility. Anyone who uses the network should be aware of the risks posed by security threats like viruses, spyware, and phishing attacks — and educated on the proper use and management of e-mail and attachments, passwords and downloads.

5. Don't overlook access control

A December 2008 survey by Napera Networks revealed that over 50 percent of the 200 small and medium-sized businesses surveyed had guests accessing their networks every day, with 20 percent allowing non-employees to plug directly into the network without security check or controls. And nearly two-thirds of respondents do not check mobile users or computers for compliance before they connect to the corporate network, potentially bringing unknown threats with them. Network access control is one of the most vital parts of your security strategy; without it, you are exposing your business to threats that could severely jeopardize it.

About the Author

With more than 30 years as an information technology professional, Bruce has significant experience in IT management and operations. Working for a variety of Fortune 500 companies, he has established consulting practice areas, managed a variety of IT departments -- including application developers, quality assurance professionals, systems and network engineers, R&D analysts, and project managers -- and led efforts in establishing standards and methodologies in varying capacities.

For the past ten years, Bruce has been instrumental in building up an IT Outsourcing firm serving the small-to-medium business market in San Diego, CA. Known as Immaculate Technology, Bruce's firm has built a customer base consisting of businesses in the publishing, home building, real estate, and medical industries. He established a level of service based on a simple concept -- bring his experience and know-how of more than 20 years working in the Fortune 500 business world to the small business owners of Southern California.