Office Network Report
COMPUTASSIST

Six Things

Your Network Should Be Doing for Your Small Business, Church or Non-profit Office

Almost every small business, church, and non-profit organization has a few computers in the office, tied together on a network and connected to the Internet. Many owners and C-level executives know it's there but don't know how to get the most out of it.

Today's desktop computers and laptops are as powerful as yesterday's mainframes. They are also connected to a world of information and resources. How can you put that power to work to do more for your organization?

Read on to discover six things your computer infrastructure should be doing for you. If you're not getting all these benefits, contact COMPUTASSIST to start turbocharging your network today!

Your office network should be:
Protecting your network and computers

The first thing your office network must do in order to benefit your business is survive! There are thousands of criminals scanning the Internet every moment for vulnerable systems. So step one is to install a true business-grade firewall or Unified Threat Management (UTM) device at the edge of your network.

While the $50 four-port router at the local electronics store is tempting, a business-grade firewall will have higher performance, more features and manageability, and give you more control over your incoming and outgoing network traffic. Some are not much more expensive than the cheap consumer-grade products.

A **router** directs network traffic. It knows where all the devices are on your network, and the pathway out to the Internet. When a computer on your network asks for a web page or a file from a server, the router handles that request and sends it on to the correct machine. When a server returns a page, the router sends that data to the machine that requested it. Think of a railroad switch yard, putting incoming trains on the right rail to get to their destinations. That's what a router does.

A **firewall** is a router with added capability. It directs traffic just like a router, but it can also apply rules to the traffic. These rules can govern where the data goes, redirect it to a different machine based on the type of traffic, block traffic from passing through, or give a higher priority to certain types of traffic.

A firewall will help protect your computers from some Internet-based attacks, and allow you to improve the performance of your network based on your business's needs.

A **UTM appliance** directs and controls traffic like a firewall, and *also* defends your network against a variety of malicious threats, from viruses and trojans to spam, phishing and hacked web sites, even internal users emailing confidential data. The capabilities vary by vendor, but can include web site filtering, anti-virus and anti-spam, time-of-day access control, and monitoring and reporting.

The hardware required for a UTM is higher than for a firewall, so they generally cost more. In addition, some have subscription costs for updates to the filters and anti-x services so there can be ongoing costs. But for the best network and computer protection, you may decide that a UTM is worth it.

Action Step 1: Install A Business-grade Firewall or UTM

Your office network should be:
Protecting your business information

One of your business's most unique assets (besides yourself, of course!) is your business data -- your documents, spreadsheets, accounting files, pictures and other media, and so on. Think of the thousands of hours it has taken to create. Your business data is irreplaceable.

Now consider that the average life span of a computer hard drive is around five years. Some last longer and some die when only a year old. They die with little warning, and when they go, they take all the data with them. If the only copy of your business information was on a hard drive that is now dead, it's gone. (It's true there are forensic techniques that can recover some of your data, but they cost thousands per drive.)

Beyond hardware failure, other things can rob you of your data. If your computers are stolen, the chance of recovery is less than 5% according to the FBI. A natural disaster such as a fire, flood, or storm can destroy your property and take your data with it.

Any backup is better than none at all, so if you are currently copying *all* your business files to an external drive, that's a start. But there are at least two problems with this approach: geography, and human nature.

Let's look at the geography problem first. Any backup that stays on site is vulnerable to the same hazards as the main data storage. You need a backup that is geographically separated, off-site. An off-site backup is much more likely NOT to be burned up or stolen along with the primary copy. Today's Internet speeds allow this backup to be done dynamically online with no need to transport discs or tapes.

The other problem with manual backup to an external drive is human nature. No matter how serious you are about backup, you will overlook doing it sometimes. You may forget to do the backup, forget to add new folders as they are created, or forget to take the discs with you when you leave. The last thing you want to discover after a disaster is that your backup is too old to contain your most recent and relevant data, or incomplete due to changing directory structures.

The best solution to protecting your business data from loss is an automated, off-site backup. It should support all your computer system types (Linux, Mac, Windows) and run on an automatic schedule. The backup specification must include every folder that contains any type of business information. Operating system files are less important, as they take much space, and need to be reinstalled using system discs anyway.

Once the automated off-site backup system is in place, do not assume your backups are good! You must periodically test the restore process to make certain you can recover every file and that the files are readable in their respective applications.

Also test the restore speed. In the event of a disaster, how long will it take to get your business back online? Try restoring a few Gigabytes of data from your backup system back to your computer to find the restore rate in minutes per GB. Multiply by the number of GB of backup storage you use. That's how long it will take to recover all your files and be back in business. With large data sets and slow backup services, it can take days to recover all your data after a disaster, unless your provider has means to get a drive to your location for direct connection to your network.

Action Step 2: Set up and test an off-site backup system

Your office network should be:
Protecting your users

While we most often think of protecting computer networks from outside penetration, one should also consider potential threats from inside. Passwords that are shared, written on sticky notes or easily guessed are as good as no passwords at all.

Passwords are a part of user authentication, which validates that the user of the computer is who they claim to be. User authentication serves many purposes, just one of which is to control access. Authentication also provides an audit trail to inform as to who created or changed files, who was active on the system at what times, and what actions they performed. Passwords that are shared or compromised are similar to identity theft. One person then masquerades as another, rendering the audit trail invalid.

You must implement effective computer security policies, including passwords, user access levels, and system patches for security vulnerabilities. Your PC or server operating system will usually provide means to configure required password change intervals and complexity requirements.

But there is a balance between security and convenience. People will work to find ways around policies that are too arduous, whether it's sharing passwords or writing them down on sticky notes. A secure password has often been characterized as complex, with a mix of upper and lower-case, numbers and symbols. But users find “gx8#jYtL” difficult to remember because it is meaningless. Requiring passwords to be changed every 30 days, while seemingly good for security, almost guarantees that users will be using sticky notes.

Here is how to get good policy compliance *and* keep your users protected. Drop the complexity requirements and instead require a longer password, or pass*phrase,* of fifteen characters or more. While a short password needs complexity to be secure, a longer passphrase is exponentially harder to crack even if it is comprised of simple characters. Systems today can accept passphrases many words long. Using passphrases ("my old car has new shoes") helps users to remember, and that means you are less likely to find passwords taped to monitors. A passphrase with a little nonsense, misspellings, untruths, even puns thrown in is even better, e.g., "knock for tech-knuckle support."

With long passphrases in place, you can relax the other requirements, for example, changing passphrases every six months instead of every 90 days.

Action Step 3: Enforce passphrase security

Your office network should be:
Keeping pace with your growth

Small office networks often grow from one PC to several or a dozen over time. The computers will be of varying ages and operating system versions. Often one user shares a folder from his or her drive to the network so that others can access certain files. If that PC is turned off, the files are inaccessible. The whole system is haphazard, difficult to use and difficult to maintain.

To get the most from your network, I strongly recommend a centralized file server. Not only will it make it easier for your staff to work together on projects, it will simplify network maintenance and the implementation of the other Action Steps. A server can enforce password policies and other network controls. It will make possible a systematic off-site backup plan. You can run an intranet, wiki, or collaboration software, and support shared databases.

It doesn't have to be expensive. An old PC can be converted to a file server for a small office that is simply sharing files. But if you do use old hardware, keep in mind that the need for an off-site backup plan is more urgent.

If your office network is currently just a cable between PCs, a server is the next step for your network. It will form the basis for the future growth of your organization.

Action Step 4: Install a network server

Your office network should be:
Gaining the benefits of Free software

To further enhance your staff's capabilities, seriously consider Free software for your small office. Capital-“F” Free software is any software that is released under a license that protects your freedom to run, modify, copy and distribute the software. Free software helps in one simple way: it removes barriers, both legal and technological, enabling you to do things that you couldn't do before. It does this while preserving your freedom to access your own data. Free has much to do with *freedom***,** and little to do with *cost*. It is not the same as “freeware” or “shareware.”

However, most Free software *is* available for free or just the cost of packaging and distribution. More importantly, the software can legally be installed on *all* your computers. A typical Free software license allows you to install it on as many computers as you like. You never have to worry about a software audit. Your staff can do their jobs instead of tracking software licenses. And they can have access to hundreds of business applications, including word processors, spreadsheets, e-mail clients, web browsers, imaging tools, and the best networking and development utilities.

With fewer expenditures for software licensing, you can focus on growing your business. And Free software often has lower hardware requirements, so your computers can last longer and cost less.

Free software gives you guaranteed access to your data. Proprietary software often changes, forcing you to upgrade or lose access to your own files. Because the source code for Free software is available (and there is no profit motive to “force” you into upgrades), you will always be able to access the documents and databases you create with it. Free software most often uses globally-accepted standards as opposed to obfuscated file formats, so your data is more accessible to begin with. Proprietary vendors hide their program's technical attributes by building complex, binary-only structures. With Free software, there is nothing to hide (configuration via plain text file is the norm), so your data remains free.

That said, these programs are also compatible with your vendors and customers, so you can share data without difficulty.

Action Step 5: Implement Free software in your organization

Your office network should be:
Helping your staff work together

At this point your office network is humming along nicely, and your staff is more productive and excited about what technology can help them do. Now help them share their new-found knowledge by setting up a corporate wiki on your server, where they can create and edit documentation about your organization's procedures, vendors and customers, equipment specifications, and anything else.

A wiki is an intranet web site with read-write privileges, where users can create their own content and update others' (think “Wikipedia.”) As people contribute their knowledge, you are increasing the knowledge retention of your organization, so that if and when individuals depart, they don't leave a big information gap behind. A wiki can provide information to staff about corporate policy, a calendar of events, supplier and customer notes, shared resources, etc.

There are many Free wiki programs, so you can set up a wiki quickly at little cost, knowing that your group's knowledge will not only be collected to help other staff and for future reference, but stored in file formats that will remain accessible and portable.

Action Step 6: Set up a wiki for your staff to use

Your office network should be:
Powering your staff's productivity

Your office network should be:

- Protecting your network and computers
- Protecting your business information
- Protecting your users
- Keeping pace with your organization's growth
- Gaining the benefits of Free software
- Helping your staff work together

Is your office network doing all these things? Do you see your network and computers as a powerful and useful tool helping you achieve your goals, or dead weight on your fixed asset list?

ComputAssist can help you implement these ideas and more, to transform your office computing infrastructure into a valuable resource. Contact Bill Bardon at ComputAssist today!

COMPUTASSIST
The RIGHT Technology!

Omaha, Nebraska
Web: www.computassist.com
Email: info@computassist.com
Phone: 402 321-5244