December 2014

TechTidbit.com

brought to you by Tech Experts

Most Employees Use Work Computers For Outside Activities

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

GFI Software, a leading software tool provider for companies like Tech Experts, recently released a report that found the personal use of company computers and other devices is leading to major downtime and loss of confidential data in many businesses.

The study of about 1,000 small business employees who used a company-provided desktop or laptop computer found that 39 percent of them said their businesses have suffered a major IT disruption caused by staff members visiting non-work related websites with work-issued hardware, resulting in malware infections and other related issues.

Even more alarming, the study showed nearly 36 percent of staff members said they would not hesitate to take company property, including email archives, confidential documents and other valuable intellectual materials, from their work-owned computer before they returned the device if they were to leave their company.

Since laptops are usually brought home, the study found, they frequently get used outside of work hours for both work and non-work activities.

The study also found that over 90 percent of employees said they have at least some understanding of their company's policy on company-provided desktop or laptop computer usage, and 94 percent said they follow it to at least some degree.

Nearly 70 percent said they believe their employer can monitor iOS, Android or Windows-based tablet use as easily as their employer can monitor conventional PC use.

Almost half of those surveyed said they use a personal cloud-based file storage solution (e.g. Box, Dropbox, OneDrive) for storing and sharing company data and documents.

More than a quarter of those surveyed said they have had to get their IT department (or outside IT vendor) to fix or reload their computer after an issue occurred as a result of non-work use, usually a virus.

How can businesses control data security challenges?

Content controls are critical to ensure data does not leak outside of a company or expose a business to legal and regulatory compliance penalties. Businesses can also better control data security challenges if they adopt clear policies and guidelines for employees, and then follow through with them.

It is also important to lock down machines to prevent the installation of unauthorized software, and rigorously update anti-virus and anti-malware programs.

Employee Internet use should also be strictly limited and monitored to prevent data loss and system infections.

The Real Risks Of Running Outdated Software

Michael Menor is Vice President of Support Services for Tech Experts.

Are you still holding onto your trusty old server that's aging towards uselessness?

Or perhaps you are still running important applications on older servers with old operating systems because they're "good enough" or "doing the job just fine."

In many ways, your old server is like a trusty old car. You know where the kinks are and it gets you where you need to go.

But lurking below the surface of that trusty old car, and your old server, can be hidden risks that can result in very big problems, even dangers. Uusually, when least expected.

Security risks are the number one danger of older technology. The older your operating system or application, the longer the bad guys have to find and exploit vulnerabilities.

This is especially true when the manufacturer is no longer actively maintaining support. Dangers can lurk across the entire aging application platform.

Your older versions of SQL Server are at risk. Perhaps you are still using an old FTP server that's innocently sitting in the corner. Or you have some older network equipment and appliances.

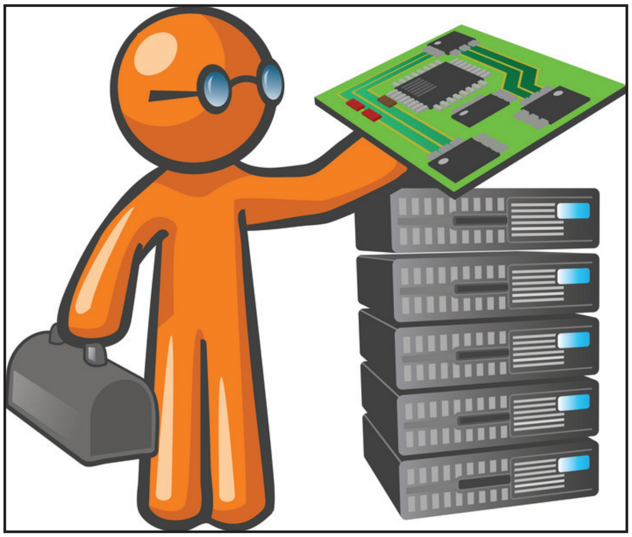
The bottom line is anything that listens on the network is a potential threat to the server, and therefore your business.

If that software or firmware isn't up to date, you're doubly at risk of a major security incident.

Here are the top 5 risks you're taking with running outdated software:

Crashes and system downtime

Aging systems are more vulnerable to failure, crashes and corruption causing significant downtime.



Targeted technology upgrades can reduce total annual outage risk and reduce downtime.

Increased costs

Outdated software is more expensive to maintain than newer versions. Failing software increases costs by overloading IT personnel. The process of applying patches is also costly and time consuming.

Updated software portfolios not only decrease maintenance costs but also free up IT budgets for more strategic and innovative programs.

Decreased productivity

Aging software applications that crash or require maintenance result in reduced employee productivity.

Modernizing software increases productivity by improving the efficiency and quality of work.

Security holes

Mission critical software is more vulnerable to security breaches as it ages. A security breach can compromise sensitive customer and employee information, and proprietary company data.

Legal and regulatory compliance risks

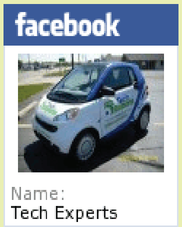
Updated software ensures compliance to governance, regulation and policy as regulatory bodies continue to mandate new global requirements.

This is especially important for healthcare professionals that need to comply with new HIPAA regulations.

With older technology, any of the above risks can strike you at any time. The consequences can be loss of productivity, or worse, loss of critical data that negatively impacts your business.

Perhaps "good enough" isn't really good enough after all.

Visit The Tech Experts Twitter & Facebook



Our Facebook page is a great place to keep up with everything we're doing at Tech Experts! You can check out staff photos, press releases, blog postings, and enter our occasional contests! You can visit our page and become a fan at www.fb.com/TechnologyExperts

Twitter is another great place to keep up with everything going on at Tech Experts! You can follow us at www.Twitter.com/TechExperts

The Human Factor In Network Security

Scott Blake is a Senior Network Engineer with Tech Experts.

As you're aware, disaster can manifest in many forms. In the past, we have included articles about weather-related events and how to best prepare your business against disasters.

However, there is another type of disaster that's unlike flooding or fires that can also have devastating effects on your business.

The Human Factor

When it comes to safeguarding your business both physically and virtually, you have the power and controls available to give the edge against company espionage, cyber-attacks, or absent-minded employees.

It comes down to three basic areas: Software, Hardware and People. Once you have a firm grasp and control over these areas, you will have reduced your risk level considerably.

Software

Make sure all of your company's electronic devices - from company-owned smart phones, tablets, laptops, workstations and servers - are running anti-virus and have a firewall in place.

While some devices are easier to secure and manage than others, this is a critical area, so be sure to make the best attempt to cover all your devices.

Be certain that your data storage devices are running backups and the backups are indeed good. As an added form of protection, encrypt your data being stored, making sure you save the key offsite as well.

That way, if your data is comprised either through internal access or external, it will become very difficult to use the data that was stolen.

The size of your company and the amount of sensitive data you have will dictate the frequency of your backup schedule. Remember, it never hurts to be overprotective when it comes to your data.

Hardware

Have security/firewall devices in place. Make sure they are fully configured for your business and that the firmware is up to date.

A lot of security devices add increased measures through the firmware updates.

They often have the ability to fully lock down your internal network as well. Restrict Internet access to only websites necessary for your business operations.

If your business offers Wi-Fi access for either internal use or guest use, make sure that controls are in place to limit access to your company's internal network. The best precaution is to place the guest Wi-Fi on a completely separate network.

While Exchange mail servers can increase overhead, they will also add a level of increased security to combat against viral infections being delivered via email and attachments.

I'm sure everyone is well aware of Crypto-Locker and its variants. The majority of Crypto-Locker infections were delivered through infected PDF files sent as attachments.

People

By nature, humans are (and will always be) the most random aspect to safeguard your business from. It is vital that you run full background checks on any employee that will be given access to sensitive data or hardware.

Restrict the use of portable media such as flash drives and external hard drives while employees are working on or in the server room. Some companies may go as far as banning all portable media devices entirely.

Be proactive in actively monitoring your employees and watch for any changes in behavior, appearance, attitude and tone of speech. These can all be signs something is wrong.

If you have questions or you're looking for suggestions, call Tech Experts at 734-457-5000, or email us at info@mytechexperts.com.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5001
(888) 457-5001
sales@MyTechExperts.com

Take advantage of
our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Don't Forget Your End-of-Year Data Backup

In a ritual akin to spring cleaning, computer users far and wide are backing up their data en masse. Although backing up your vital data is a wise idea to prevent the loss of important documents during crashes or even computer theft, it often goes undone.

By the end of the year, however, an amazing amount of data would have been stored which may slow computers' performance. This is a silent reminder to clean out the cobwebs and back up the files you want to keep.

There are various ways to back up your data, and one is readily available right on your PC. Windows users can access backup tools by pressing the Start button, typing "backup" in the search area, then clicking "Backup and Restore."

This allows users to back up files instantly. Similarly, Mac users can open the System Preferences menu and select Time Machine. It will promptly perform backup tasks with the selection of the appropriate disk to store the files.

However, the aforementioned tools on your PC or Mac, don't address more complex situations where your computer may be completely damaged or lost.

Therefore, it is also advisable to back up important documents, such as financial records or critical documents or emails, on a separate device.

If you depend solely on your computer's backup system, your backed up data is vulnerable to the same threats that can damage the whole computer.

There are various data storage solutions on the market. The more expensive ones offer extra features, but the main factor to consider is the data storage size that you will need to have on the device.

Alternatively, simply upload your most important data to cloud storage, which can also be automated for future backups.

Other computer users prefer to back up data on an external USB device and keep it in a safe place.

It would also be best to automate your backups based on a recurring schedule that takes into consideration the particular files/folders that change often and/or are the most critical and include them in the backup set.

If you require assistance in figuring out the most appropriate automated backup solution for your home or business, give us a call at (734) 457-5000 and one of our technicians will be glad to help.

My Laptop's Ethernet Port Isn't Working. What Can I Do?

If the Ethernet port is damaged, purchase a USB to Ethernet converter.

The laptop Ethernet port is integrated into the motherboard, which makes it hard to replace only that part without swapping out the entire motherboard.

Since it just doesn't make sense to throw the proverbial baby out with the bath water, just make it possible to plug into another port that is undamaged with a USB to Ethernet converter.

Fortunately, these converters are relatively inexpensive, so there's no need to despair. Converters are available at virtually any store with an electronics section and there isn't much difference between converters.

One thing you may wish to consider is to purchase the latest model of adapter, even if your current laptop is not new.

These converters are backward compatible, so the latest USB 3.0 to Gigabit Ethernet adapter works with even the oldest computers with older USB ports.

With the latest version as part of your arsenal, you can still use it in the future with a newer laptop.

These adapters have another great feature which is that they don't require any technical knowledge, saving you time and money for installation and troubleshooting in case of problems.

Simply plug it in the USB port, and it's ready to deploy your Ethernet connection, getting you back online without any hassle.

Windows automatically detects the adapter and the operating system installs the appropriate drivers for you.

Remember to use an in-line surge protector on your Ethernet cable, particularly if you travel frequently.