

# TechTidbit.com

brought to you by Tech Experts

## Raise IT Security Measures And Lower Your Stress

### Updating Your Network Security Protects Your Valuable Data

Simplify. Prevent problems. Do it right, not over. These are just a few of the phrases among the most popular published in "Stress Reducing Tips" articles. But, how do you achieve these goals?



Take a look at your IT security measures first. Protecting your information systems

from unauthorized use, disruption or destruction can help you reduce the number of stressful incidents that may arise as a result of a vulnerability. How can you decide what level of security is right for your organization?

### Dive into a threat and risk analysis.

We can work with you to review the current security mechanisms and determine what needs to be protected. The level of security necessary for your business is largely reliant on the possible threats. If you have many employees, you may have a greater interest in user account changes versus a small dental practice whose chief concern is confidentiality.

Take advantage of our Free Network Audit and learn about the current options available for firewalls, controlled accessibility, anti-virus, spam filtering and much more.

Take time to develop a plan. Listen to employee feedback, analyze your current operations and review key points for development within your company in order to simplify business processes and protect your company data.

### Think of the future.

Is your organization in growth mode or are you looking to stabilize your current position? Many clients come to us with only a few changes and end up with many things they would like completed to help increase security, increase efficiency, decrease operating costs or prepare for the future.

### Prevent problems.

Security is everyone's responsibility. According to Datapro Research, the most common causes of damage are: Terrorism, 3%; water, 10%; technical sabotage, 10%; dishonest people, 10%; fire, 15%; and, finally, human error, 52%. Unfortunately, 81% of this damage is caused by current employees.

You could install the most elaborate security and computer protection systems available, but if passwords are written on sticky notes and stuck to computer monitors in the office, or saved in Word documents, we cannot guarantee security.

New threats and vulnerabilities emerge everyday that can endanger your company. Take a preventive approach to managing your information systems with reliable security measures and proper staff training.

Firewalls and virus protection must be current. If you don't know if these measures are in place, we can help you identify current software installed and enable or update them if necessary. A good anti-virus or firewall solution will automatically update itself as new updates are available.

Spam filtering is essential and can solve many e-mail problems that plague your inbox. Everyday spammers find new ways to get into e-mail inboxes. A lot of spam is simply unwanted advertising that is just annoying and takes up space. Some, though, are used to transmit viruses, adware or spyware that can eventually infect your entire network.



If you're concerned about network security and threats to your critical systems, our 67 point "Free Network Audit" can put your mind at ease.

To schedule your free, no obligation Network Audit, just give our office a call at (734) 457-5000.

We're proud to partner with the computer industry's leading companies:

**Microsoft**  
GOLD CERTIFIED  
Partner

Microsoft  
Small Business  
Specialist

IBM  
Business  
Partner

ca CHANNEL  
PARTNER

Need help? Call the Tech Experts 24 hour computer emergency hotline at (734) 240-0200.



## Eight Steps To Prepare For Business Disruptions

### Summer Storms, Crazy Weather Highlight Need To Be Prepared

With the crazy weather we've been experiencing the past few weeks, now is the perfect time for your business to put together a basic disaster planning and recovery plan.

Here are some key points to consider:

#### **1. Prevention costs less than recovery, and it's faster.**

When a disaster occurs, one of the first questions asked after the smoke clears (or the debris is cleared) is how it could have been avoided. That's the prevention component - and the issue for most businesses is when they want to answer that question, and how much they are willing to spend to avoid a major disruption to their business.

#### **2. Don't put all your eggs in one basket.**

Our professional recommendation is to spread "vital" operations across more than one location if at all possible. Full backups should be performed every business day, and stored off site. The key thing here is, backups must be tested - this means you need to frequently pick random backup sets and attempt to restore from them. In far too many cases, data that was thought to be securely backed up couldn't be accessed when the chips were down.

#### **3. When disaster strikes, the first thing to go haywire is the plan.**

Your business should review the disaster plan for adequacy (are you covering all the bases) and currency (has the plan been updated to match your new technology?). Special attention should be paid to new systems and processes that weren't in place in the business when the

initial plan was developed.

#### **4. When disaster strikes, your competitors will notice.**

If your company doesn't maintain market presence and reputation after a disaster, the absence can create a vacuum in the market place. This being the case, competitors will step up to fill that void.

#### **5. Remember the four "P's of disaster planning - People, property, priorities and planning!**

Your company's security plans should be up to date, including how to contact local fire, police and rescue departments. Some examples of questions to answer in your disaster management plan? Has it been tested recently? Do you know when to call in authorities, and who has the authority to make the decision? How are visitors and vendors controlled in your building? Do your security procedures reflect what you really expect employees will do?

#### **6. Tailor your business continuity spending to real threats and key priorities.**

Recent events have made us think of terrorism as a major threat, but for small businesses like ours, there are more pressing and diverse threats. Things such as employee or non-employee workplace violence, cyber threats (including computer viruses and denial of service attacks), electrical disruptions, torna-



does or other storm related damages are, for most businesses, much more appropriate threats to invest in remediation efforts against.

#### **7. Successful recovery is like a recipe - everything has to come together at the right time.**

Your business should also consider asking critical vendors about their plans and capabilities to deal with emergencies. Relying on one or more critical vendors to keep your business going could be dangerous because a crisis that affects them could spill over to your company if they're unable to provide goods or services.

#### **8. Regional disasters have a way of mandating priorities you weren't even aware of.**

It is a good idea for your business to look at the immediate area surrounding your facility and perform a risk assessment. Are you near a river, stream, dam or lake? Focusing on employee safety will pay off during a disaster, since knowledgeable employees are an important key to your company's recovery plans.



## Tips For Handling, Storing, & Disposing Of Confidential Documents

In the past 10 years, over 10,000 new regulations have been placed on the books by local, state and federal agencies pertaining to the handling, storage, and disposal of confidential client, patient, and employee documents.

A few examples are:

- SEC Rule 17a-4 Electronic Storage of Broker Dealer Records Graham-Leach-Bliley Act
- Financial Services Modernization Act
- Sarbanes-Oxley Act
- DOD 5015.2 Department of Defense
- Health Insurance Portability and Accountability Act (HIPAA)
- Fair Labor Standards Act
- Occupational Safety and Health Administration (OSHA) Act
- Payment Card Industry Data Security (PCI DSS)

No matter how small your business is, you are surely going to be affected by one or more of these new government regulations. Naturally some industries are more regulated,



such as financial or medical, but all companies that hold information such as employee social security numbers, credit cards, financial statements (credit applications, bank statements, order forms) fall under these new regulations.

While we cannot cover every single aspect of protecting your company, here are a few tips that will go a long way in making sure you don't end up fined, sued, or with a bad reputation for not securing your clients information:

**Seek professional help.** If you think you are holding confidential information that should be secured, ask a qualified attorney who specializes in data confidentiality

in your industry about what you must do to meet new government regulations.

**Shred all documents that contain confidential information.** A good shredder should do a cross cut or diamond cut versus a simple strip shredder to make it more difficult for someone to piece together a shredded document.

If you have to keep a copy of contracts or other documents that contain confidential information, contact a high-security document storage facility like Iron Mountain ([ironmountain.com](http://ironmountain.com)) and they will store your documents in a high-security location.

**Keep a fire-proof safe with a lock and key for employee documents you need to keep onsite.**

**Make sure your offsite backups have 32-bit encryption (ask your provider).**

Also make sure the facility where the information is stored is under lock and key with security camera and access-controlled security.

*Shred all documents that contain confidential information. A good shredder should do a cross cut or diamond cut versus a simple strip shredder to make it more difficult for someone to piece together a shredded document.*

## Play Your Vinyl Records On Your iPod or MP3 Player

So procrastination paid off and you can finally justify why you saved dozens if not hundreds of those old bulky vinyl LPs from the 70's or 80's. Now you can use one of several easy ways to transfer those hard to get favorites to an electronic format.

The simplest way to do it is to send your old LPs to an internet company such as Reclaim Media or Ferris Mastering. The charge for a single LP ranges from \$10 to \$15 (about what you paid for the album in the first place) and gets cheaper in bulk, but the upside is they may be able to improve the sound quality by removing the crackles and pops associated with scratches or dust.

However, the cheapest way to convert albums is via a USB turntable with prices ranging from \$49 - \$250.

Turntables come in a wide variety of quality levels from well known and off brand names. Be sure the turntable comes with feature packed user friendly software to avoid hours of record "babysitting" and headaches trying to break up the tracks.

**Check it out on the web:**

<http://www.reclaimmedia.com>

<http://www.ferrismastering.com/>

<http://www.thinkgeek.com/electronics/mp3/90a0/>

**Need help? Call the Tech Experts 24 hour computer emergency hotline at (734) 240-0200.**



### Contact Information

24 Hour Computer  
Emergency Hotline  
(734) 240-0200

General Support  
(734) 457-5000  
(866) 993-9737

support@MyTechExperts.com

Sales Inquiries  
(734) 457-5000  
(888) 457-5001

sales@MyTechExperts.com

Take advantage of our  
client portal! Log on at:  
[https://connect.  
expertsmi.com/support](https://connect.expertsmi.com/support)



**T E C H  
EXPERTS**

980 S. Telegraph Road  
Monroe, MI 48161  
Tel (734) 457-5000  
Fax (734) 457-4332  
info@MyTechExperts.com

## Tired of Dumping Money Into Your Network?

Read On To Discover How You Can Make Those Darn Things Finally Pay Off!

If you ask most business owners why they invest in computers and technology, you will hear things like “to increase employee productivity,” or “to improve customer service” or even to lower operating costs, make information more accessible, and give them a competitive advantage.

But the question is, are the computers in your office actually contributing to your productivity, or do they act as a money-sucking stumbling block to your businesses success?

In this dog-eat-dog world, you cannot afford to have anything slowing you down or interfering with your day to day operations. Especially the tools you rely on in your computer network. If you want to learn how we can help you experience fewer interruptions, problems, and downtime, AND lower the overall costs associated with your computer network, then you’ll want to know about our “Experts Total Support” plan.

This program was designed specifically for small business owners that do not have a full time IT staff taking care of their computer network.

For a small, fixed monthly fee, we will monitor and maintain your computer network 24 hours a day, 7 days a week to make sure all systems are running at peak performance. We’ll also make sure critical network maintenance such as security and virus updates, back ups, and system optimization happens when it should to avoid bigger, more expensive problems from happening.

### Our Free 60 Minute “Technology Tune Up” May (Finally) Make Your Computers Pay Off

To introduce this new program to all of our clients and prospects, we are offering a free, 60-minute “Technology Tune Up” to the first five businesses that contact us this month.

In less than 1 hour, we can come in and examine your computer network, talk to your employees, and provide a very revealing analysis of all the under utilized or overlooked capabilities being wasted in your current computer system. We’ll also look for security loop holes, check your system back ups and virus protection, and look for other hidden problems lurking in the background, waiting to turn into bigger, more expensive disasters.

After doing this analysis, we can not only advise you on how to improve the speed, reliability, and security of your computer network, but also on ways you can improve your overall office productivity.

Normally we charge \$297 for this type of service but we are giving it away FREE as a special promotion

this month to demonstrate our “Experts Total Support” plan. To secure your spot, simply call our offices at (734) 457-5000 or e-mail us at info@MyTechExperts.com and we’ll schedule a convenient time for us to come out and conduct this tune up.

### No Risk, No Obligation, No Hassles

You will be under zero obligations to do or buy anything if you sign up for a FREE Technology Tune Up. This is just our way of introducing our new network maintenance program to you and we certainly don’t expect everyone to sign up.

So what are you waiting for? Call us right now while you’re thinking about it. Remember, we are only giving away five tune ups on a first come, first serve basis so call now while there are spots left!

This offer will expire as soon as we have five companies signed up, or on August 29th. Call today!

