

# 9 Tips to Manage Your I.T. Investment

*A guideline for Small business to get the most from their Technology*

August 2009

[www.jsotechnology.com](http://www.jsotechnology.com)  
PHONE: 414-455-0720  
FAX: 262-436-2111  
10437 Innovation Drive STE 439  
Wauwatosa, WI 53226

## Highlights

- Standardize hardware and software
- Use computers for business purposes only
- Install spyware, spam, and virus protection on all devices
- Select industry leaders for all products
- Maintain warranties and support contracts for all hardware
- Perform regular backups
- Keep software and hardware up to date with the latest patches and service packs
- Filter internet access to keep good employees from doing bad things
- Use managed services to allow experts to manage your system at a fixed cost

## Executive Summary

Small businesses face many challenges when planning and managing their technology investment. From our experience in helping small businesses in a wide variety of industries, JSO Technology has developed a short list of best practices to help small businesses leverage their technology investment in a cost effective manner.

JSO Technology firmly believes that utilizing best practices can help reduce the complexities commonly found in technology solutions, leading to a better and more reliable end-user experience.

A summary of the recommendations is provided to you.

## ***Standardize your hardware, software and policies***

Standardizing your hardware, software, and policies simplifies your environment making troubleshooting issues a simpler and more consistent process.

### **Why standardize?**

With each different piece of hardware and software, the complexity of your network increases. With each increase in complexity, troubleshooting all of the different layers becomes more difficult. Without a standardized environment, each problem takes more time to identify, troubleshoot, and resolve. The result is higher IT costs regardless of whether a consultant or internal staff is solving the problem.

### **How to standardize?**

Replace as many computers as possible at the same time. The fewer computer models in your organization, the lower the maintenance costs. A multiple-year lease is a convenient way to spread out costs while refreshing technology.

If replacing computers all at once is not an option, then standardize on a certain computer manufacturer and model line. Purchase that same computer model when ordering new computers. Place computers on a life cycle and create a phased purchasing plan to replace older computers. The machine components will be easier to inventory, replace, and manage.

Utilize the same version of operating systems and software suites on all computers. Upgrade and patch all computers at the same time.

### *Use computers for business purposes only*

Most small businesses give their employees full control of their computers and do not provide a policy on what is and is not acceptable use.

Spyware, malware, viruses, and trojans often enter your network through personal email and web surfing that is not work related. They also come from software such as Weatherbug, screen savers, and numerous other “helpful” programs. These programs report back to websites stealing valuable resources from your computer and Internet connection and wasting your employees’ time.

Create a written policy which clearly states what acceptable and unacceptable use of company computer resources is. Enforce that policy.

Use tools that will allow tracking and blocking of unacceptable websites. This type of pro-active system helps protect your business assets and prevent good employees from doing bad things.

## ***Install spyware, spam, and virus protection on all devices***

According to Dell, over 20% of all support calls are related to spam, viruses, and spyware.

The toolsets required to prevent spyware, spam and virus infection are typically inexpensive; often paying for themselves in a matter of months. However, even the best software will not prevent all attacks. Providing your employees with guidelines and rules for email and Internet use will help combat viruses and spyware. A list of best practices and tips should be made readily available for your users to help them identify suspicious emails and websites. Also, many companies implement a policy to not allow employee or customer laptops to connect to the network until it has been verified that virus protection is installed and up to date.

### **Best Practices and Tips for Employees:**

- Update virus protection daily
- Don't open email/attachments from unknown senders
- Don't open email attachments with file extensions such as .exe, .bat, and .vbs.
- Use a popup blocker to help prevent automatic spyware downloads.
- Don't forward joke or chain emails.
- Don't use your business email address to sign up for mailing lists and newsletters.
- Don't click on links in emails that contain banking site information; instead, go to the site directly.

### ***Select industry leaders for all products***

Hardware and software play a critical role in the overall success of any company. Your business is not a place to experiment with unproven products. Purchasing inexpensive but untested products could lead to lost revenues and may be costly to your business. Select proven products from recognized market leaders in their respective industry.

Many businesses are tempted to save money on software licensing fees by dumping Microsoft for Linux or “free” open source office products. This is almost always an unwise investment. Lost productivity and additional training costs will easily outweigh the small savings that may be found by implementing inexpensive, 3<sup>rd</sup> party software.

Provide your employees with a strong, industry-standard tool set and your company will benefit with increased productivity.

### ***Maintain warranties and service contracts for all hardware***

Warranty and service contracts will provide you with replacement parts for your equipment and critical updates for your software packages. These services can be a large annual expense, but they are necessary for the proper operation and support of your computer network and applications.

Dealing with hardware failures is difficult enough when a product is under warranty. Without a service contract, your business is gambling on extended downtime or rushing into a purchase you aren't necessarily ready to make. Buy the warranty and save yourself the risk and headache.

## *Perform regular backups*

Every business should have a sound, well-documented disaster recovery plan in place. Your data is one of the most valuable assets you possess so every step should be taken to ensure it is protected.

The first part of a good DR plan is properly organizing your data on the network. A company-wide policy is needed to address where data is to be stored. Without it, data is scattered across the network and there is no way to know whether or not it is being backed up.

All businesses should have some type of backup device which allows for media to be taken off site and allows for restore quickly.

A regular backup schedule needs to be defined as well. This schedule should at a minimum include full backups weekly and differential (backups where only the changed files are backed up) backups daily. A full set of backup media should be taken off site at least weekly.

That being said, tape backup solutions are not the end-all of backups. Tape backups are often temperamental with tapes going bad, media rotations not properly maintained, tapes wearing out or succumbing to environmental conditions, etc...

A comprehensive disaster recovery plan includes an additional backup using Internet based storage resources. The cost of backup over the Internet has decreased greatly recently to the point where it is affordable for many small businesses. An Internet based backup is highly compressed to limit the bandwidth needed to copy your data. The entire backup session is encrypted to ensure your privacy while it is being sent off-site to a secure location. When you need to restore a file or recover data, it easily retrieved with a simple point and click on a secure website.

No backup strategy is 100% bulletproof, but taking these steps will protect you from the vast majority of data loss scenarios.

***Keep software and hardware up to date with the latest patches and service packs***

Every business should keep updated with the latest operating system and office patches. These patches fix security vulnerabilities which helps protect your business from malicious hackers and provide new functionality which helps make your software run more efficiently.

Consider purchasing a patch management system or use the free patch management system provided by Microsoft. Patch computers at least quarterly although monthly is recommended. If you are not utilizing a patch management system, consider placing individual computers on Microsoft automatic updates. This will ensure that you get the latest security patches as they are released.

### ***Filter internet access and keep good employees from doing bad things***

While the Internet is a great tool for businesses; it is also a great tool for criminals. Employees can be tricked into accessing dangerous websites by an email scam know as phishing. The criminal attempts to obtain information such as social security numbers and financial information by imitating a valid web site and asking users to enter that data.

Employees can also access websites that download programs to computers without the employee realizing it. These programs can be used to steal passwords or to capture users' web surfing habits for marketing purposes. It can also display pop-ups that are often offensive in nature.

Putting Internet filtering in place will help prevent employees from accessing these malicious websites. Most employees don't realize that they have done anything wrong until it is too late. An Internet filter is cheap insurance and helps keep good employees from doing bad things.

***Use managed services to allow experts manage your system at a fixed cost***

Managed services allow businesses to outsource monitoring and maintenance of critical IT systems at a fixed cost. Depending on the level of managed service, the managed service provider (MSP) monitors and maintains your systems remotely. This allows for proactive management.

With managed services monitoring most IT systems, problems are corrected before they are allowed to cause a failure or an outage. Using managed services changes most businesses' approach to IT from reactive to proactive. Instead of calling in someone when a system fails, many issues are fixed remotely, before you even realize a problem existed.

Managed services can also ensure that systems are kept up to date with the latest security patches. This preventive maintenance ensures that the latest worm or vulnerability is patched before it becomes an issue on your network.

Using managed services provides all these benefits at a fixed price of a few hundred dollars per server while allowing you to focus on what you do best: running your business.