ITSUPPORTLA

7 IT DISASTERS THAT COULD RUIN YOUR BUSINESS

Dear Fellow Business Owner,

Businesses today are more dependent than ever on Information Technology. Here are some statistics you may not be aware of:

- 30% of all businesses that have a major disaster go out of business within a year. 70% fail within five years. (Home Office Computing Magazine)
- 31% of PC users have lost all of their files due to events beyond their control.
- 60% of companies that lose their data will shut down within 6 months.
- North American businesses lost more than $60 billion as a result of viruses during 2010. (Research by TechNews World)
- Every week 150,000 hard drives crash in North America. (Mozy Online Backup)

In short, **a serious IT failure could put you out of business!**

And the reality is that most IT failures are the result of benign neglect or just plain incompetence. **Don't** let that happen to your business!

In this free report, we've identified **seven** key areas where a **simple, low-cost fix** can make a **dramatic** improvement in the **reliability** of your network, and the **safety** of your data.

But whatever path you choose, you should take steps to make sure that your critical business infrastructure is protected. Business comes with many risks, but losing your data doesn't have to be one of them!

Dedicated to your success.

#1 - Insufficient or NO Backup

You'd think that - by now - everyone would know how important it is to back up your data.

Unfortunately, you'd be **wrong**. It still amazes us how many times we walk into a new customer only to discover that either:

a) Their backups haven't been running for months
b) They backup onto the **same device every night**
c) They only backup **some** of their data
d) Their backups **never** leave the building
e) There are only two backup sets and no history
f) Some combination of the above

Every one of the above scenarios is a **recipe for disaster**. Every one of them has the potential for **significant data loss**. Remember the statistics we quoted at the beginning of this document?

Unless you are backing up **all your data**, **at least once a day** and saving it **offsite** (ideally, using **cloud backup**), your business is **genuinely at risk.**

That's **no exaggeration**. Think about it: if your Accounts Receivable information goes missing, how are you going to keep your business afloat? If your Payroll database is corrupted, how can you make sure your employees are paid correctly and on time?

The simplest solution is **cloud backup**. For a few dollars a day, **all** of your data is automatically backed up to a **secure, offsite location**. You can even keep **unlimited** backup history. If you need a copy of a specific file, from a specific date, it'll be there, waiting for you.

No other form of backup offers this level of safety. Tapes are slow and unreliable and hard drive backups are not very portable. Today's standard **is** cloud backup. Don't be left in the dust.

#2 - Insufficient or NO Power Protection

If your company is like most businesses, then your servers are *probably* plugged into a **UPS** (Uninterruptable Power Supply). But did you know that:

a) The battery on a UPS doesn't last forever

b) You need to have a UPS that's big enough to provide time for all your equipment to recognize a power outage and perform an **orderly shutdown**

c) ALL your servers have to be **UPS-aware** and have shutdown software installed and configured. Otherwise the UPS won't provide any real protection

d) If you don't provide power protection for other critical infrastructure components (like printers, Ethernet switches, wireless equipment, etc) then your network **could still be destroyed** by a power "event"

If you've ever experienced an accidental "jolt" from touching live electrical wires, you know just how dangerous electricity can be. And when the power goes out or turns on suddenly, it can wreak havoc with sensitive electronic equipment.

A few years ago, we had an experience at one of our clients where a printer was damaged by an electrical surge. You see, they had plugged it directly into a wall outlet, against our advice.

The damage caused the printer to flood their network with bad data with the result that everything on the network **slowed down to a crawl**. But because the printer was located in an obscure corner of their warehouse and the damage wasn't visible to the naked eye, it took us nearly 2 days to trace the problems to the printer and disconnect it.

And all of those problems - and the enormous cost to the business - could have been avoided by the installation of a $45 **surge suppressor**.

When you buy an expensive television, the salesman will probably tell you that it's always a good idea to plug your TV into a surge suppressor or power bar.

The same logic applies to your IT infrastructure. If **a single component failure** can take down an entire network, isn't it worth a small expenditure to make sure that never happens?

As the old saying goes: **An ounce of prevention is worth a pound of cure!**

#3 - Insufficient or NO AntiVirus / Anti-Malware

Do any of these risks apply to **any** of the computers in your office?

a) No AntiVirus software
b) Subscription lapsed on AntiVirus software
c) Still running a 3-year-old version of AntiVirus software
d) Haven't run a virus scan in 2 years
e) No Anti-Malware software

It amazes us how often we find users relying on an **out-of-date** AntiVirus program to protect their critical business data and infrastructure.

According to a report published by **Microsoft** and **IDC Corporation**, viruses and other malware cost businesses **$114 billion** worldwide in 2013. And that number grows every year.

A serious virus infection can put your company out of business for **days**. It can get your company's emails **blacklisted**, effectively **crippling business communications**. And it can generate tens of thousands of dollars in repair costs and lost productivity.

Even if **only one** of your computers is infected, it could still impact your entire network.

And that's absurd, because effective AntiVirus software is **inexpensive**. For a network of 30 computers, the cost is **less than $900 a year**. Isn't your business worth that investment?

Well, that addresses the software. But if you don't actually use it properly, you've only fixed half the problem.

In order for AntiVirus and Anti-Malware software to be truly effective, you have to **run periodic scans**; we recommend once a week. Most software will even let you configured automated scans at times that won't impact your work schedule.

An effective AntiVirus / Anti-Malware solution can keep your network safe and sound. But to **keep** that solution effective, regular monitoring and maintenance goes a long way.

#4 - Missing Security Patches

It's so annoying. Those continual reminders from Windows that patches are waiting to be installed on your computer. And it's so easy to ignore them. After all, installing the patches usually means rebooting your computer, and who has the time for that in the middle of a busy work day?

It's even easier to ignore those warnings on your server. How often do you even look at the server console? It could be months since the last time you actually paid attention.

But here's the problem: those Windows patches, particularly the **security patches**, were created for a really good reason. They plug "holes" in Windows security that would otherwise allow hackers, viruses, trojans, spyware and all kinds of other **bad stuff into your network.**

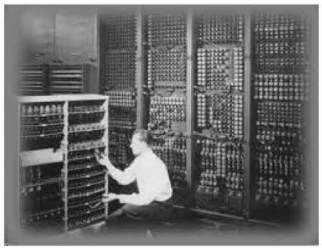
In fact, hackers are **constantly** looking for these holes, searching for an opportunity to penetrate your networks. What's worse is that as soon as Microsoft releases a patch, it's like sending up a red flag, letting hackers know **exactly** where to attack.

But - you ask - isn't my AntiVirus software going to protect me?

Unfortunately, the hard truth is that the bad guys are always one little step ahead of the good guys. That's why it's so essential to make sure that **all** of your computers have the latest patches. Just like with AntiVirus software, if even **one** of your computers is not up-to-date, it could become the point-of-entry for an attack that could cripple your IT infrastructure.

And there's no good reason for that. **A few minutes** spent on each computer and server, every week can ensure that all of your computers - Windows, **Mac** or **Linux** - are totally up-to-date.

#5 - Dependence on Obsolete Hardware / Software



Here's an example of a nightmare scenario that we've run into more than once:

> Several years ago, you purchased a line-of-business software program. Maybe it's a property management package, or perhaps it's a retail system. But regardless, the software that you purchased is now an older version that's no longer supported.
>
> Here's where it gets worse: that software is running on a 5-year old computer, that's still running Windows Server 2003, an operating system that's scheduled to be decommissioned by Microsoft in July, 2015. And to make matters **even worse**, your software doesn't support more recent Microsoft operating systems like **Windows Server 2008**.
>
> Then, one day, the hardware fails and the cost of repairing it would run to thousands of dollars. You'd prefer to purchase a new server, but you can't run Windows 2003 on a new server and you can't run your software without Windows 2003.
>
> **Now what?**

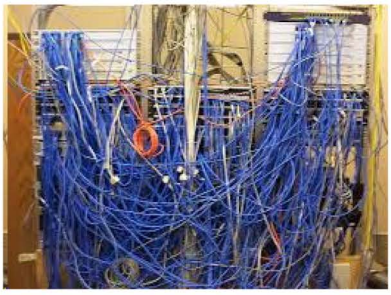
Unfortunately, there is **no simple answer**. For most users it would a choice between an expensive and difficult repair to an obsolete piece of equipment, or a painful (and likely expensive) migration to an up-to-date version of your software.

And that's assuming that the software is still available. We've actually seen cases where the software vendor was no longer in business and the customer was left, effectively, **stranded**.

Think of it this way: there are people out there who collect vintage automobiles. But they would never make one of those vehicles their "daily driver." After all, an older vehicle is much more prone to failure and it can take weeks to locate parts if something breaks.

So if that's logical for your car, isn't it equally logical for your business? Surely you don't want to bet your business on obsolete technology.

#6 - Bad Network Cabling



If you were buying a brand-new house and you found out that the wiring was not installed by a licensed electrician, would you still buy it? Or what if you found out that the electrician installed wiring or fixtures that didn't meet the building codes? Would you still be willing to part with your money?

Chances are that your answer to both questions is a resounding **NO**. And that makes perfect sense. Why would you choose to put yourself or your family in jeopardy?

But many people do just that when it comes to installing cabling for their office computer network. Instead of hiring an experienced contractor to install their wiring, they'll have it done by their building superintendent, or perhaps by the electrician who happens to be doing work in the office.

Now, we're not saying that those people will necessarily do a bad job. In the example above, the fact that the wiring in the house wasn't installed by a licensed electrician doesn't mean they are incompetent.

But it's not particularly reassuring.

And what can happen if your computer cabling is installed badly, or if the wrong kind of wiring is used? Here's just a partial list:

a) Slow network performance

b) Intermittent connectivity failures

c) Data loss or corruption

d) Potential damage to your workstations or servers

e) **Serious injury or death**

And no, (e) is not a joke. The wrong kind of network cable can emit toxic gases in the event of a fire. Is that really something you're willing to risk, to save a few bucks?

That's why it's so important to make sure that you hire only skilled professionals to build and maintain your infrastructure.

#7 - Hiring the Wrong Technician(s)

Think it's okay to turn the management of your computer network over to your 16-year old nephew?

Think again. No matter how smart that young kid may be, there's a world of difference between knowing how a computer works and a proper understanding of the IT requirements of a running **business**.

In a recent teleconference, one of the "gurus" of the IT consulting industry told us a story about how her company had gone through 3 sets of IT providers until they found one which **actually** did what it promised to do.

It sounds shocking: they were paying a company to make sure that all of their systems were up-to-date with all the latest patches and fixes, only to discover that they had actually done **nothing** of the sort.

Unfortunately, stories like this are all too common. In many cases, when we take on a new customer, we find ourselves stunned by the level of neglect and sometimes - outright incompetence - that we discover when we start examining their IT environment. The fact is that the IT industry has **no** certification requirements and **no** professional standards. Anyone can call themselves an IT consultant and many of those who do lack the skills and the discipline to do a professional job.

So how do you protect yourself from being put into this position? Well, here are a few simple hints:

1. Hire a company with a **team** - not a "one-man band." No matter how clever your "computer guy" may be, how can he look after you when he's away on vacation, or sick, or busy with another client?
2. Look for a company with a track record. We're not implying anything negative about startups, but the only way to really judge the kind of service you will get is by working with a company that's been around for a while.
3. Make sure that your IT provider offers **guarantees**. If they're not willing to stand behind their work, how can you rely on them to look after your best interests?
4. Ask for References and check them out. The most honest opinions that you'll get about any vendor will come from their other customers.

In short, do your homework. A good IT provider can help your business stay sharp and competitive. A bad provider can put your whole business at risk.

Our Mission Statement:

IT Support LA's mission is to provide high quality IT services and support to small and medium sized businesses through proactively monitoring and managing their IT infrastructure.

Although they don't like to admit it, most IT consultants are one-trick ponies; they have only one specialty. They're very good at Microsoft Windows, but they don't know much about Linux. Or they know all about Cloud services, but have no experience with Voice-over-IP (VoIP).

At IT Support LA, we think differently. Your business has more than one need, so we have more than one skill.

Due to our expertise in Hardware and Managed Services, IT Support LA is the only true Hardware as a Service (HaaS) provider in the country. We have millions of dollars worth of hardware stock at our immediate disposal which we implement and install for our clients at no additional cost. This allows our clients to use the latest and greatest in technology without the huge capital expense that is normally accompanied by it. In addition to all of this, IT Support LA is the only HaaS provider in the country that does not utilize any contracts on the equipment we provide which allows our customers to be in total control of their infrastructure.

IT Support LA was founded in 2002, located in Los Angeles, we specialize in delivering effective outsourced and Managed IT services which includes hardware, software and service solutions. Our clients depend on us to provide a complete IT solution that encompasses desk-side support, help desk services, network management, security and technology consulting which we strive continuously to exceed our clients' expectations. This is shown by the fact that we don't require our clients to enter into a long term contract as we will prove the value we bring every day.

In our nearly 20 years of business, we have established solid alliances with the top suppliers in the IT industry. We have strong partnerships with Microsoft, VMware, Cisco, Dell, HP, Ubiquity, QNAP and other partner relationships as well. In addition to this, we have partnerships with many of the industry's best-known niche providers of advanced computer, network hardware and software.

By combining all of these facets together we have the industry contacts and expertise required to help our customers achieve the results they need to power their businesses in the twenty-first century. Our years of experience in working with business customers means that we are uniquely qualified to understand the needs of our clients and to respond to them in a timely, professional and responsible fashion.

ITSUPPORTLA

www.itsupportla.com

818-805-0909