

2012

The 10 Most Frequent Computer Disasters That Wipe Out Non- Profits and Small Businesses ...

And What To Do About Them

This eBook is filled with actionable information that every executive can use to protect their organization, its security, its data, and its budget from those unnecessary and expensive technology surprises.



The Top 10 Most *Expensive & Deadly* Computer Disasters That Wipe Out Small Businesses... *And What To Do About Them!*

This Report Explains In Simple, Plain English What Every Business Owner Must Know About Protecting Their Business From:

- Data Loss and Corruption
- Extensive Downtime
- Expensive Computer Repair Bills
- Viruses, Spyware and Worms
- Hacker Attacks
- Spam
- And Other Disasters

You'll Discover:

- **Critical security measures** every small business should have in place.
- **The single costliest mistake** most small business owners make when it comes to protecting their irreplaceable company data.
- **How to avoid costly network repair bills.**

**From the Desk of: Ed Becker
President, BeckITSystems, Inc.**

Dear Colleague,

Have you ever lost an hour of work on your computer?

Now imagine if you lost days or weeks of work – or imagine losing your client database, financial records, trade secrets, and all of the work files your company has ever produced or compiled.

Imagine what would happen if your network went down for days where you couldn't access e-mail or the information on your PC. How frustrating would that be?

What if a major storm, flood, or fire destroyed your office and all of your files? Or if a virus wiped out your server...do you have an emergency recovery plan in place that you feel confident in? How quickly do you think you could recover, if at all?

Many small business owners tend to ignore or forget about taking steps to secure their company's network from these types of catastrophes until disaster strikes. By then it's too late and the damage is done.

6 Out Of 10 Businesses Will Experience A Major IT Disaster

After working with over 500 small and mid-size businesses in the Washington, DC Metropolitan area, we found that 6 out of 10 businesses will experience some type of major network or technology disaster that will end up costing them between \$9,000 to \$60,000 in repairs and restoration costs *on average*. That doesn't even include lost productivity, sales, and client goodwill that can be damaged when a company can't operate or fulfill on its promises due to a down network.

What's most exasperating about this situation is that 100% of these disasters and restoration costs could have been completely avoided easily and inexpensively. That's why I decided to write this report.

I have found that most business owners have no idea of the importance of regular preventative maintenance and disaster recovery planning because they are already swamped with more immediate day-to-day fires demanding their attention. If their network is working fine today, it goes to the bottom of the pile of things to worry about. In most cases, no one is watching to make sure the back-ups are working, the virus protection is up-to-date, or that the network is "healthy."

99% Of Businesses Get "Too Busy" To Think About Network Security And Maintenance...I Strongly Caution Against This

Being 'too busy' to think about network security is like saying you're too busy driving your car on the highway to put your seatbelt on. Taking that simple preventative step doesn't really show its true value until you get into a head-on collision; at that point you are either extremely relieved that you had it on or incredibly sorry that you didn't.

The same holds true with your computer network. Obviously the information on the disk is far more valuable than the disk itself. If your company depends on having access to the information stored on your server or PC, then it's time to get serious about protecting it from damage or loss.

Why Small Business Are Especially Vulnerable To These Disasters

With the constant changes to technology and daily development of new threats, it takes a highly-trained technician to maintain even a simple 3 to 5 person network. The costs of hiring a full-time IT person are just not feasible for many business owners.

In an attempt to save money, most try to do their own in-house IT support and designate the person with the most technical expertise as the part-time IT manager. This never works out because this make-shift IT person has another full-time job to do and is usually not skilled enough to properly support an entire computer network anyway.

This inevitably results in a network that is ill-maintained and unstable. It also means that the back-ups, virus updates, and security patches are not getting timely updates, or may even be set up improperly, giving a false sense of security.

It's only a matter of time before the network crashes. If you're lucky, it will only cost you a little downtime; but there's always a chance you could end up like one of these companies:

Auto Body Shop Shells Out \$20,000 To Clean Up A Virus

A local auto body shop with multiple locations discovered the importance of preventative maintenance the hard way. Without warning, a virus was downloaded to their server and started replicating and attaching itself to files. This virus corrupted their data, impaired their customer management system, and immediately brought down their Exchange server (no e-mail could come in or go out).

Preventing this disaster would have only cost them 1/25th of the cost (\$800 per month) AND they would have experienced better performance and fewer problems with their network. Instead, they were forced to spend a whopping \$20,000 to remove the virus and restore their network, and that only got them back up and running. Their systems were still not optimized, secured, and updated as they should be.

Two Destroyed Hard Drives Cost Local Company \$40,000 and

9 Days of Downtime

A local company had an employee at the same time causing them to lose a large number of critical customer files.

When they contacted us to recover the data from the system back-ups, we found they were sabotaged and not functioning properly. Even though they appeared to be backing up all of the company's data, they were in fact worthless. In the end, recovering the data off of these failed drives took a team of disaster recovery specialists 9 days and \$15,000. In addition to the recovery costs, they also incurred \$25,000 in other services to get their network stable.

Had they been properly monitoring their network, they would have been able to see that these hard drives were failing and that the back-ups were not performing properly. This would have prevented the crash, the downtime, and the \$40,000 in costs to get them back up and running, not to mention the 9 days of lost productivity while their network was down.

Property Management Company Spends \$9,000 And Weeks Of Downtime For A Simple Inexpensive Repair

A 10-user property management company was not monitoring or maintaining their server. Due to the overuse and lack of maintenance, it started to degenerate and eventually shut down under the load. This caused their entire network to be down for two full days and cost them \$3,000 in support fees to get them back up and running. Naturally the costs were much higher when you factor in the lost productivity of their 10 employees during that time.

This client did not want to implement a preventive maintenance program, and the same problem happened again two months later, costing them another \$3,000 and two days of downtime.

Six months later it happened yet another time bringing their total to \$9,000 in hard costs and tens of thousands in productivity costs for a problem that could have been quickly detected and prevented from happening from the start.

The Top 10 Biggest Threats To Your Network's Security...And Simple, Easy Ways To PREVENT Them From Happening

While it's impossible to plan for every potential computer disaster or emergency, below are the top 10 biggest threats and disasters that wipe out businesses and simple, easy steps you can take to dramatically lower the chances of them happening to you.

Threat #1: Viruses and Worms

Today, viruses are still by far the most common type of network security threat. Viruses can do a wide range of damage from displaying a steady stream of annoying popup ads to freezing your entire network and corrupting your data. Not only can a virus corrupt your files and bring down your network, but it can hurt your reputation. If you or one of your employees unknowingly spreads a virus to a customer, or if the virus hijacks your e-mail address book, you're going to make a lot of people very angry.

Worms are even more dangerous because they don't need a host file to infect your network; they can simply be embedded into an e-mail. Once a computer is infected with a worm, it can make quick copies of itself and infect an entire network within a few hours. Because of this, worms are responsible for a good number of companies' widespread network failures.

Prevention:

Obviously you need to make sure every PC and laptop in your office has anti-virus software installed. We recommend AVG Professional Edition Anti-Virus Software. But you can't just install it and forget about it; someone needs to monitor your network to make sure every machine has the most up-to-date version installed AND to make sure the software isn't accidentally disabled.

Threat #2: Not Backing Up Your Data, AND Failing To Keep An Offsite Copy Of Your Data

It just amazes me how many businesses never back up their computer network, OR only keep an on-site copy of their data. Imagine this: you write the most important piece of information you could ever write on a chalkboard and I come along and erase it. How are you going to get it back? You're not.

Unless YOU MADE A COPY OF IT, you can't recover the data. It's gone. That is why it is so important to back up your network. There are a number of things that could cause you to lose data files. If the information on the disk is important to you, make sure you have more than one copy of it.

Prevention:

The first step is to make sure you have a good on-site copy of your data. We recommend BeckITSystems' Hassle-Free IT Continuous Data Protection Program. This program creates a backup copy of your critical data and then captures all changes every 15 minutes.

Second, it's absolutely critical that you keep an off-site copy as well. No one expects a flood, fire, hurricane, tornado, or other natural disaster. But did you ever consider theft? What if someone breaks into your office and takes every single piece of computer equipment you have? It has happened. BeckITSystems' Hassle-Free IT Continuous Data Protection Program transmits an encrypted and compressed copy of the new data to our data centers in Phoenix, AZ, and Baltimore, MD; making it possible to recover any lost data rapidly.

What if a neighboring office catches fire or if a faulty sprinkler system waters your server room? Here's another on-site disaster most people never consider...

What if your data becomes corrupt or a tape drive hardware failure erases your data? Again, your data is nothing but a memory. That's why you want to not only keep an on-site copy of your data, but also an off-site copy. Your data is just too important to not do everything possible to protect it.

We recommend BeckITSystems, Inc's Hassle-Free IT Continuous Data Protection Program. With continuous data protection, off-site storage of the data in an encrypted form, and a backup appliance that can become a failed server to restore functioning within hours rather than days, **YOUR BUSINESS IS PROTECTED BECAUSE YOUR DATA IS PROTECTED!**

Threat #3: Not Testing Your Back-ups To Make Sure They Are Working

This is another big mistake I see. Many business owners set up some type of back-up system, but then never check to make sure it's working properly. It's not uncommon for a system to APPEAR to be backing up when in reality, it's not.

Prevention:

At least once a month, have someone perform a restore of your data to see if it CAN be restored and to see if your data is intact. Tape drives have a failure rate of 100%—that means ALL tape drives will fail at some point.

Problem is, it often happens without any warning or sign, so you THINK you are backing up a good copy of your data when you aren't. Remember the Health Products Company that shelled out \$40,000 to recover data they THOUGHT they backed up? Don't let this happen to you. Frequently test your data back-ups. BeckITSystems' Hassle-Free IT Continuous Data Protection Program performs these tests on a regular basis.

Threat #4: Trojan Horses

A Trojan horse is a malware attack that hides in something innocent such as a screen saver, computer game, or even a YouTube video.

Not too long ago the Saddam Trojan horse infected a number of PCs by using a link in an e-mail that promised to connect to a web page that showed the Saddam Hussein hanging, but instead infected the user with malware. Once installed it was designed to record screen shots and key strokes to steal financial information, accounts, and passwords.

Prevention:

Trojan horses are very difficult to remove so an ounce of prevention is worth 5 pounds of cure. Educating employees is not enough to protect against these attacks because hackers are constantly coming up with new and innovative strategies to access your network.

We recommend that you block users from downloading freeware and computer games, as well as imbedded links in e-mails. You may even want to block all web sites that are not on an approved list of web sites that employees may visit. BeckITSystems, Inc. provides Internet content management that will provide this type of essential protection.

Threat #5: Spam

Spam is an irritating and potentially malicious menace that every business has to deal with. Not only does it kill office productivity, introduce viruses, worms, and Trojan attacks, but it can also take up so much bandwidth that it causes your network to crash.

Prevention:

When it comes to fighting spam, fortunately, a great deal of spam can be filtered out by a good email filter. BeckITSystems, Inc. provides email management to clients or commercial services like POSTINI can be very effective.

Threat #6: Not Maintaining A Secure Firewall

Small business owners tend to think that because they are “just a small business,” no one would waste time trying to hack in to their network, when nothing could be further from the truth. Experiments have been conducted where a single computer was connected to the Internet with no firewall. Within hours, over 13 gigabytes of space were taken over with malicious code and files that could not be deleted. The simple fact is there are thousands of unscrupulous individuals out there who think it’s fun to disable your computer just because they can.

Prevention:

BeckITSystems, Inc. recommends SonicWall Firewalls or Cisco PIX Firewalls.

Threat #7: Not Installing The Most Up-To-Date Security Patches and Updates

Software companies (like Microsoft) are always discovering security loopholes in their programs that allow hackers to access your network. That is why they offer patches and updates to their users for free.

However, most hackers do NOT discover these security loopholes on their own. Instead, they learn about them when Microsoft (or any other software vendor for that matter) announces the vulnerability and issues an update or a patch. That is the hacker’s cue to spring into action; they immediately analyze the update and craft an exploit (like a virus) that allows them access to any computer or network that has not yet installed the security patch. The time between the release of the patch and the release of the exploit that targets the underlying vulnerability is getting shorter every day; that is why it’s important to keep an eye out for security updates and patches.

Prevention:

We recommend that you engage BeckITSystems, Inc. to manage and monitor this critical function for your network. BeckITSystems, Inc. reviews and tests all updates and service packs before deploying them to ensure they work and that all your systems are consistently updated.

Threat #8: Phishing Attacks

Phishing refers to spam e-mails designed to trick recipients into clicking on a link to an insecure web site with the intention of stealing account information and passwords for e-commerce sites, as well as credit card and bank account numbers.

Chances are you’ve received the infamous PayPal e-mails alerting you that your account is going to be deactivated or closed if you don’t log in to verify your account information. This is a classic phishing attack.

Prevention:

The best line of defense is educating employees on how hackers try to phish your account information. Even though simplistic phishing attempts like the PayPal scam now seem obvious to regular Internet users, a single phishing attack can compromise your entire network's security if the employee is tricked into giving his network account information. That is why you need to frequently remind your employees to never enter personal information in a web site solicited through an email. BeckITSystems' email manager and Internet Content Manager protects users and systems from this very common attack.

Threat #9: Hardware Loss and Residual Data Fragments

Not long ago a number of government laptops were stolen, making national news. This story brought to light another security problem for businesses: stolen laptops and computers. While this may not seem like a big issue, it is a major contributor to the 10 million cases of identity theft suffered by Americans each year.

Prevention:

Thankfully, this threat can be minimized in a few easy steps:

1. Encrypt sensitive company data, especially the laptops used by employees who frequently travel. If your laptop gets stolen, this will prevent the thief from doing further damage by accessing financial records, patient files, sensitive client data, and other confidential information.
2. Wipe and/or shred files on old hard drives before they leave your organization.
3. Develop a policy for keeping track of employees' use of smartphones and USB memory cards around sensitive data.

Threat #10: You and Your Staff!

No, we are not kidding. End user mistakes are often the biggest threat to a network's security. Whether it's downloading a virus, accidentally deleting an important folder or file, visiting shady web sites, or sharing confidential information, end users are usually at the root of every computer problem.

That's not to say you and your employees are intentionally doing things to harm your network; in most cases, the damage is done innocently enough. But a virus's effects are the same whether the download was intentional or purely by accident.

Prevention:

All of the above measures will go a long way in preventing problems; but we also recommend continually educating you and your staff on proper e-mail, Internet, and PC usage. We also recommend regular maintenance and monitoring of your critical data and systems so that IF a problem arises, it can be dealt with immediately and the damage minimized.

How Disaster-Proof Is YOUR Network? FREE Security Audit Reveals the Truth

Hopefully this report acted as an eye-opener to all small business owners who are not adequately protecting their data and computer network. If you are not doing the 5 steps outlined in this report, your network is an accident waiting to happen, and the most important thing for you to do now is take immediate action towards protecting yourself.

One of the biggest, costliest mistakes you can make is to ignore this advice with the false hope that such a disaster could never happen to you.

Because you have taken time to request and read this report, I would like to help you make sure your company is safe from harm by offering you a FREE Network Security Audit. Normally we offer this service for \$350 for this type of audit, but during the next 60 days, I'll make room in my schedule to give away 5 of these to business owners in the Washington, DC region that are concerned about keeping their network and data safe. The only thing I ask in return is 20 minutes to review the audit results and to learn more about how you use technology for business results.

During this audit our engineer and I will come on-site and...

- ✓ **Pinpoint any exposure or risk** to potential lapses in security, data back-up, power outages, and system downtime.
- ✓ **Review your system back-ups** to make sure the data CAN be recovered in case of a disaster. You don't want to discover that your back-ups were corrupt AFTER a major disaster wiped out your network.
- ✓ **Scan your network for hidden spyware and viruses** that hackers "plant" in your network to steal information, deliver spam, and track your online activities.
- ✓ **Outline a powerful and comprehensive line of defense** against even the most evasive and deadly computer viruses, hackers, and spam for your specific network.
- ✓ **Answer any questions you have** about your network or keeping it running problem free. I can also give you a second opinion on any projects you are considering.

Upon completion of this audit, we'll give you a detailed report in plain English that outlines where you are at high risk for viruses, downtime, or other problems, and discuss what options you have for protecting yourself.

Good Networking for Good Business!

For BeckITSystems, Inc.

Ed Becker, President

703-433-0730

877-649-9829

P.S. Please note that this offer for a **FREE Security Audit won't be around forever**. While we would love to be able to give these away to everyone, staff and time limitations simply won't allow it.

That's why we can only give away 5 of these audits within the next 60 days on a first come, first served basis (sorry, no exceptions). There are zero obligations for you to do or buy anything when you sign up—so do it now while you're thinking about it!

Fast Response Form

Fax This Completed Form to: (571) 287-2530

YES! Please sign me up for a FREE Security Audit so I can know for sure if my data and network are protected from viruses, worms, hackers, spam, spyware, and a host of other expensive disasters!

Sign me up for **THE PORTAL**, your monthly newsletter packed with useful information on the latest technology, problem-solving strategies, and stories on how other local business owners are increasing sales, profits, and productivity with IT.

Contact me about your Hassle-Free IT program and bullet-proofing my data to discover how I can get the benefits of a full-time IT staff without the costs or overhead.

Your Name: _____
Title: _____
Company: _____
Address: _____
City, State, Zip: _____
Phone: _____
E-mail Address: _____
Number of PCs: _____

BeckITSystems, Inc.
22570 Markey Court Suite 200 Dulles, VA 200166
(703) 433-0730 FAX: (703) 740-9248

Need To Speak To A Technician Immediately?
Call our computer crisis hotline at: (703) 433-0730