

Disaster-Proofing Your Computer Systems

**A 40-Point Checklist for Data Security, Backup,
Power and Virus Protection**

**Sponsored by
SW Computers Limited**

www.swcomputers.co.uk

Copyright © SW Computers Limited. All Worldwide Rights Reserved.

Unauthorized reproduction or distribution is expressly prohibited.

This report is intended to provide accurate and reliable information with regard to the subject matter at hand. This report's purpose is to educate and entertain. It is sold with the understanding that neither the publisher nor the author is engaged in rendering legal, accounting, or management consulting services. This report is also not a substitute for information technology consulting. If information technology consulting, legal guidance or other professional assistance is necessary, the services of a competent expert should be sought. The publisher and author shall not be held liable or responsible for any misuse of this report's content. If you do not wish to be bound by these terms, you may return this report to the publisher for a full refund.



Preparing a Small Business for a Data Disaster

Many small business owners and managers procrastinate unpleasant tasks, in favor of more immediate day-to-day challenges. After all, who really wants to consider the outcome of unlikely catastrophes such as a flood, fire, hurricane or earthquake?

But sooner or later your company could become the victim of one of these natural disasters, or something much more common such as a massive lightning storm, downed power lines, or sabotage by a disgruntled employee or sleazy competitor.

What You'll Learn:

How to Rapidly Survey Your Readiness to Respond to Common Computer Disasters

In this report, we'll start by looking at why small businesses are so vulnerable to potential data disasters. Then we'll move right into over 40 questions that will help pinpoint your exposure to potential problems with data security, workstations, networks, data backup, organizational issues, utility power and computer viruses.

Why Disaster-Proofing a Small Business is So Important

Unless your company has a full-time computer support manager, or a similar outsourced relationship with a local consultant, there's a good chance that no one is paying much attention to various disaster recovery computer planning and data protection issues.

However, data disasters tend to strike when you least expect. Small businesses without a formal in-house computer support function are especially vulnerable to these potentially catastrophic risks.

When looking at disaster recovery computer planning best practices, you'll find only two kinds of small businesses: those that have experienced a data disaster and those that will.

Countless studies have shown that a big percentage of small businesses that ignore disaster recovery computer planning never fully recuperate. Small

businesses without a thorough, regularly tested disaster recovery plan are likely to go out of business within a few months after a data disaster.

Ignoring basic disaster recovery planning can be very dangerous to your company's survival. Just because your company is a small business doesn't mean it's immune to big data disasters.

So with these risks in mind, what can your organization do right now with disaster recovery planning, on a small business-friendly budget, to protect against some common hazards? Use the questions below as a checklist for jump-starting your data disaster recovery planning efforts.

Physical Security

- What procedures are in place to guard your data backups against tampering or theft?
- Are your critical technology assets, such as servers, hubs, routers and phone system controllers, in locked areas of your office?
- Do at least two, but no more than four, people have physical access to your company's critical technology assets? (Or can "anyone" just walk over and reboot your server just for the heck of it?)

Physical Security – all required measures taken to maintain control over access to facilities housing IT assets and prevent unauthorized individuals from inadvertently or deliberately accessing, tampering with or misappropriating PC systems, telecommunications equipment, backup media and data cabling; protecting facilities and IT assets from physical risks such as theft, fire, water, wind damage and earthquakes.

PC/Workstation Security

- Do your company's desktop PCs and notebooks run a locally securable operating system, such as Microsoft Windows 2000 Professional, Microsoft Windows Vista or Windows XP?
- Are there any desktop PCs or notebooks that have confidential data stored locally? Are any of these systems running an inherently insecure operating system, such as Microsoft Windows 9x or Microsoft Windows Me?

- Are power-on passwords used to prevent unauthorized boot-ups or tampering with BIOS configuration settings?
- How does your company go about keeping service packs, critical updates, and service releases current on desktop PCs, notebooks and servers?

Network Security

- How do you protect individual data files on network-shared folders?
- Are you relying on shared application-level file permissions, such as those in Microsoft Word and Microsoft Excel? Or do you use a more sophisticated, integrated security management approach, such as user and group security permissions?
- Are usernames and passwords required to logon to all servers? Does each network user have a unique set of logon credentials, or do users share logons and passwords?
- If users have their own network logons, do you have company policies that reinforce these efforts? For example, are employees forbidden from sharing logons or posting their usernames and passwords on yellow sticky notes near their PCs?
- When an employee resigns or is terminated, do you have a procedure regarding network logons?
- How many logons and passwords do users have to contend with as they run various network applications? What's holding you back from implementing a single sign-on approach?
- How often are network users required to change their passwords? How is this enforced by your network operating system (NOS)?
- Are there any policies in place that mandate sophisticated password selections, such as a mixture of upper and lower case characters, as well as the inclusion of both letters and numbers?
- Do your designated administrators only use the "Administrator" logon when absolutely necessary? In other words, do administrators have stripped-down logons for everyday desktop software usage?
- What kind of hardware redundancy do you have in place on your server(s) to protect your company from a single point of failure?

Data Backup

- Do you know where all of your company's crucial data files are located?
- How are these files being backed up?
- How often are these data backups run, verified and tested?
- What kind of automation and controls are in place to make sure that data backup jobs run correctly and consistently?
- How often do your data backup tapes go off-site?

Organizational Concerns

- Do you keep common, easy-to-replace spare hardware parts, such as a mouse, keyboard or monitor, on hand to minimize downtime? In the event a crucial system was to fail without warning, do you have a spare system on hand?
- If you were unable to get into your office for several days following a disaster, would your company be able to operate in another location? What are the most critical functions that you need to get up and running immediately?
- Do your employees have a list of key personnel home phone numbers? Is a hard copy of this list kept at employees' homes?
- Do you have an up-to-date inventory of all of your hardware and software assets, as well as current, coherent system documentation, stored on- and off-site?
- What's the chain of command for deciding that an event is in fact a data "disaster" for your company?
- How will key personnel and strategic vendors be notified in the event of a data disaster?

Power Protection

- Does every sensitive electronic device in your company, both PC and non-PC equipment, have at least some form of real surge protection?

Note:

Don't be fooled by cheap power strips masquerading as surge protectors.

- Do battery backup or UPS (uninterruptible power supply) units protect your desktop PCs and servers?

UPS (Uninterruptible Power Supply) – broad category of power protection products designed to prevent tremendously expensive damage to data during utility power fluctuations; protects against common utility power problems including sags, brownouts, blackouts, spikes and surges.

- Do these UPS units have the ability to automatically send out network alerts and shutdown the affected PC or server during a prolonged blackout? When was the last time you tested these capabilities?
- Are you protecting your telecommunications lines with appropriate data line surge protection?
- Do notebook PC users have portable surge protectors with data line protection?

Data Line Power Protection – a device that sits between various telecommunications cables and your PC hardware to protect your PC hardware from utility line voltage spikes and surges; although products need first to be grounded properly, data line power protection devices can interface with many connectors including RJ-11 and RJ-14 for telephone circuits, RJ-45 for network cabling and RS-232 for serial lines.

Virus Protection

- Is antivirus software installed on every desktop PC, notebook and server in your organization?
- How current is the antivirus software?
- Are you entitled to updates and upgrades through your existing antivirus software license?
- If the update process is not automated, how often do you update virus definitions? How often do you update the core-scanning engine?
- If the update process is automated, or supposed to be automated, how often do you verify that the antivirus software is in fact being updated as promised by the software vendor?
- Are end users permitted to install their own software applications? If so, what controls are in place to prevent end users from inadvertently introducing viruses into your office's technology backbone?
- How are your e-mail client applications and server(s) protected to keep viruses from spreading through inbound (POP3), outbound (SMTP) and other related messaging mechanisms?
- Have you done anything with hardened security settings on programs, such as Microsoft Outlook, Microsoft Internet Explorer, Microsoft Word or Microsoft Excel, to lessen the risk of virus damage?
- Do you use the Microsoft Windows Update and Microsoft Office Product Updates Web sites to regularly install critical security patches?
- Are end users trained on how to recognize telltale signs of a virus?

Virus – any kind of malicious software code that can be delivered through a variety of mechanisms including conventional software media, Internet downloads, e-mail file attachments, file macros, scripting, ActiveX or Java applets, and instant-messaging software.

The Bottom Line

While it's impossible to plan for every conceivable small business data disaster or contingency, there are a number of relatively painless and inexpensive best practices your company can put into place right away to get proactive.

These 40+ disaster recovery computer planning tips shouldn't be regarded as the be-all, end-all of your data protection efforts. Rather, use the bullet points and examples to jump-start your disaster recovery planning.

Disaster-proofing your computer systems is *not* a one-time project. You need to monitor and guard against ongoing risks and re-evaluate your strategy at regular intervals.

In much the same way that you cannot plan for when you'll need an insurance policy, data disasters tend to strike when you least expect.

Unfortunately, many data disasters can have a crippling effect on your company's immediate prospects, while even threatening your firm's future survival in the days and weeks following the disaster.

However, there are a number of relatively simple, straightforward steps that you can take right now to fortify your defenses.

Remember though, you must take **action** to improve your company's ability to weather common disasters. It's not going to happen by putting this report under your pillow at night.

Which of these ideas do you plan to implement this week? This month? This quarter?

Pick out the ones you want to focus on, build your task list in priority order, and schedule some time on your calendar to get started. Remember, it's the future of your business that we're talking about!

Here's to you getting **your** small business better prepared!



Stephen Parkinson (Director & MCSA)
SW Computers Limited
Tel: (01209) 613645 – stephen@swcomputers.co.uk
www.swcomputers.co.uk