The 7 Disaster Planning Essentials For Any Small Business

Little-Known Facts, Mistakes And Blunders About Data Backup And IT Disaster Recovery Every Business Owner Must Know To Avoid Losing Everything *In An Instant*

InnoTek
computer consulting, inc.

Don't lose everything you've worked so hard to achieve in an instant! This report will reveal important planning strategies you should have in place now to protect yourself from common data-erasing disasters including natural hazards, human error, cyber criminals, hardware failure, software corruption and other IT failures.

24 West Main Street, 2nd Floor
Bloomsburg, PA 17815
Phone: 570-245-0033

The 7 Disaster Planning Essentials For Any Small Business

Little-Known Facts, Mistakes And Blunders About Data Backup And IT Disaster Recovery Every Business Owner Must Know To Avoid Losing Everything *In An Instant*

Written By:
Fred Reck, President
InnoTek Computer Consulting, Inc.
24 West Main St.
Bloomsburg, PA 17815

570-245-0033
fredr@consultinnotek.com
www.consultinnotek.com

About The Author:

Fred Reck, a technology consultant in Central Pennsylvania, has successfully built multiple businesses and advised well over 500 on technology and systems integration issues. Fred is known for advising clients on improving business efficiency. By putting a solid technology infrastructure and processes in place, Fred helps businesses improve their business processes while reducing the risk of business downtime and gaining the ability to quickly recover when disaster does strike.

InnoTek
computer consulting, inc.

24 West Main Street, 2nd Floor
Bloomsburg, PA 17815
Phone: 570-245-0033

Why You Desperately Need A Disaster Recovery Plan For Your Business

In a study* of companies that experience a major data loss without having a solid disaster recovery plan in place, ONLY 6% survive; 43% close their doors immediately and 51% limp along and eventually close within 2 years. And the situation is getting worse as more and more companies store – and rely on – digital information and systems to serve customers and keep the doors open.

Fact is, every business connected to the Internet with human beings accessing digital information is highly vulnerable to hackers, viruses, data corruption, data loss, system failures and downtime. A disaster can happen at any time on any day; and thinking, "That could never happen to me," is an open invitation for Murphy to visit you and wreak havoc on your business. (Murphy's Law: Anything that can go wrong, *will*.)

The cost of the aforementioned disasters is enormous and spread far beyond simple downtime. Client data stolen can cost you big in reputational capital and easily turn into lawsuits and government fines. Extended downtime can cause you to lose customers and miss important deadlines, not to mention put a damper on productivity. And with more and more private data being captured and stored by companies, the long-term losses and legal challenges can have significant short AND long term impact.

That's why it's no longer "nice" to have a disaster recovery and business continuity plan for your business – it's an outright necessity to protect what you've worked so hard to create and achieve. This report will outline 7 simple things you can do right now to minimize the impact or even prevent such disasters.

1. **Have a written plan.** As simple as it may sound, just thinking through in ADVANCE what needs to happen if your server has a meltdown or a natural disaster wipes out your office, will go a long way in getting your business back online fast. At a minimum, the plan should contain details on what data and systems are most important, and a step-by-step process of how those systems will be secured, backed up and brought back online. Any good, professional IT person or firm can help you with this part of your disaster recovery and business continuity plan. If they can't (or won't) find someone who will. Here's a ***short list*** of what your Disaster Recovery Plan should include:
    - An IT Asset Inventory of all hardware, software licenses and assets. Your IT person or vendor should have this anyway in your basic Network Documentation. If you don't have this, make sure you get one!

- A list of all the cloud applications you use, what data is stored there, how it's accessed (UN/PW)
- A process for how the data in these 3rd party cloud applications will be backed up to YOUR location to avoid losing it from the company closing, being hacked or having them simply deny you access to your data for any reason. This would include web sites, member portals, CRM systems, accounting systems, etc.
- A "Break The Glass" document of critical web sites, passwords and other information held only by key executives that are critical for running the business. If something should happen to that executive, you want to be able to keep the business running.
- A detailed process of how all your PCs, laptops, servers and other devices are being backed up AND who is responsible for backing them up and validating the backups through periodic test restores.
- A telecommunications recovery plan that would deal with a situation where all phone lines are down or your building is inaccessible.
- A "high impact" disaster plan for how your business would continue to operate if your building was inaccessible temporarily or permanently.
- A list of key vendors and their contact information. You should also have emergency contact information for each employee in case of a major disaster where you are unable to access your office and you must contact them at their home.
- Information about your insurance policies, coverage, contact information for the insurance provider, a copy of the policy, etc. You should also have documentation (receipts) and pictures of the assets in your office in case you need to submit a claim. Having this is proof that you actually owned the assets you are claiming.

2. **When writing your plan, think business continuity, not just backup.** A HUGE mistake made by almost all business owners is thinking that having a backup copy of your data will enable you to be back in business quickly. Not so. Business continuity is the process of planning and systems to make sure your business continues operating after a disaster. We often see business owners shocked to learn that it may take 5-7 days, sometimes more, to get their operations back online and functioning because they only have a copy of their data. Don't make this mistake! With some simple planning (and help from your IT pro) you can make sure critical operations, e-mail and other functions don't go down for

extended periods of time.

3. **Automate your backups OFFSITE (to the cloud).** If backing up your data depends on a human being doing something, it's flawed. The #1 cause of data loss is human error (people not swapping out tapes properly, someone not setting up the backup to run properly, etc.). Plus, local backups and tape drives are NOT secure and can easily fall into the wrong hands, be misplaced, lost, etc. That's why it's just smart to backup your data to a reputable, highly secure, highly available data center. Second, automate that backup so it runs automatically. We further recommend hiring a professional to set this process up and monitor it daily to make sure all of your data is being protected as expected.

4. **"Image" your server or consider cloud computing.** Having a copy of your data offsite is good, but keep in mind that all that information has to be RESTORED someplace to be of any use. If you don't have all the software disks and licenses, it could take days to reinstate your applications (like Microsoft Office, your database, accounting software, etc.) even though your data may be readily available. "Imagining" is simply a process of making an exact copy of your server and everything on it; that copy can then be directly copied to another server saving an enormous amount of time and money in getting your network back. Best of all, you don't have to worry about losing your preferences, configurations or favorites. To find out more about this type of backup, ask your IT professional.

   Another option may be to simply move your network to the cloud and eliminate the onsite server altogether. Cloud technologies are advancing fast, offering more secure and less complex and expensive options to purchasing and maintaining a server onsite. Plus, Internet connectivity is getting faster and more reliable, which is making it easier for companies to utilize cloud technologies to run their business. Best of all, cloud offers built in business continuity and backup.

5. **Network documentation.** Network documentation is simply a blueprint of the software, data, systems and hardware you have in your company's network. Your IT manager or IT consultant should put this together for you. This will make the job of restoring your network faster, easier AND cheaper. It also speeds up the process of everyday repairs on your network since the technicians don't have to spend time figuring out where things are located and how they are configured. And finally, should disaster strike, you have documentation for insurance claims of exactly what you lost. Again, have your IT professional document this and keep a printed copy with your disaster recovery plan.

InnoTek computer consulting, inc.
24 West Main Street, 2nd Floor
Bloomsburg, PA 17815
Phone: 570-245-0033

6. **Maintain Your System.** One of the most important ways to avoid disaster is by maintaining the security of your network. While fires, floods, theft and natural disasters are certainly a threat, you are much more likely to experience downtime and data loss due to a virus, hacker attack or human error (be it intentional or accidental). That's why it's critical to keep your network patched, secure and up-to-date. Additionally, monitor hardware for deterioration and software for corruption. This is another overlooked threat that can wipe you out. Make sure you replace or repair aging software or hardware to avoid this problem.

7. **Test, test, test!** A study conducted in October 2007 by Forrester Research and the Disaster Recovery Journal found that 50 percent of companies test their disaster recovery plan just once a year, while 14 percent never test – and that's the companies who actually HAVE one! If you are going to go through the trouble of setting up a plan, then at least hire an IT pro to run a test once a month to make sure your backups are working and your system is secure, and revisit the plan quarterly or every six months. After all, the worst time to test your parachute is AFTER you've jumped out of the plane.

Want Help In Implementing These 7 Essentials?

If your e-mail, database, accounting data, client work products and other IT systems and digital information is extremely important to you and could not be easily (or cheaply) replaced, then call us about developing a simple IT-specific disaster recovery and business continuity plan for your business.

Our process involves documenting all the hardware, software, data and critical systems you need to keep your business running, and then putting together a solid plan to make sure you can be back up and running again fast.

We'll also audit your current security systems and virus and hacker protection to check for loopholes, oversights and gaps in your systems that would be access points for cyber criminals, hackers and disgruntled employees.

To request a FREE, no-obligation Disaster Readiness Assessment to learn more and to see if you are at risk, **call us at 570-245-0033**
or go online to http://www.consultinnotek.com/free-stuff/

*Cummings, Haag & McCubbrey, 2005