

# Where Were You When the Lights Went Out

By June Campbell

August 2003 will be remembered as the month when North America's East Coast suffered massive power failure, rendering cities, communities and businesses without power.

The repercussions of that localized event affected Internet users on a global level.

Web sites went down. Email servers were rendered inoperable. Online businesses were unable to provide customer support, process credit card transactions, fulfill orders or process refunds.

My friend in Vancouver was without email for almost a week. Her ISP's email server is situated in the East. It's a small world, after all.

It was business as usual on my web site, since it is not hosted on the East Coast. However, there could have been problems. InternetSecure, the company that processes my online credit card transactions is situated in Toronto -- a city that experienced the blackouts. Thanks to InternetSecure's backup power supply, there was no break in their ability to provide service. Obviously, they had done their homework and implemented an excellent disaster recovery plan.

I wonder how many of us have done the same?

It's equally important for small and medium sized businesses to implement a disaster recovery plan as it is for big businesses. As we see only too clearly, the unexpected can and will happen. What can we do to be ready for it?

Consider the following:

1. When purchasing services from a web host, credit card processing company or ISP, ask about THEIR disaster recovery plans. Your **online business depends on your suppliers' ability** to survive natural and man-made disasters including power failures, floods, fires, hackers, vandals and more.
2. **Back up your computer data** regularly. How many days' worth of data can you afford to lose? The answer to that question tells you how often you need to back up. And, equally importantly, store your backed-up data off site. If fire or flood damages your computer, it will also damage the stack of backup tapes sitting beside it.
3. **Protect your computer with anti-virus software and firewalls.** Please note that you must update your anti-virus software regularly or it will be close to useless.

Typically, when you purchase anti-virus software, the package will include a year of updates. It's a good idea to update twice weekly and daily when a major virus outbreak is occurring.

4. **Install security updates** to your system and other software as these patches become available.
5. **Appoint someone to look after your business in the event that you are unavailable for any reason** -- death, illness, accident, crime victim, extended vacation, etc. Draw up a Power of Attorney giving that person the legal right to manage your affairs should it ever be necessary.
6. If you have employees, **develop a written plan to be followed in case of disaster or emergency**. Stipulate who should be notified, who is responsible for doing the notifying, who is responsible for contacting emergency services, etc. Without this information, your employees are likely to delay acting, believing it is someone else's responsibility. Ensure the disaster plan includes phone numbers and full contact information. Lastly, be sure your employees know where the disaster plan is stored.
7. **Ensure your insurance needs are covered**. Do you have business insurance? Disability insurance? Do your policies cover loss or damage to expensive technology equipment?
8. **Ensure that your physical setting is protected** adequately against fire, vandalism, theft, etc. Are your fire alarms functional? Do your employees know how to locate and operate fire extinguishers? Do you know exactly who has keys to your business location? Do you change the locks from time to time?
9. Before disaster occurs, **locate a business or service that provides disaster planning and disaster recovery services**. Consult with them to ensure that your disaster recovery plan is comprehensive and suited to your individual requirements. Google for "disaster recovery service" and you will find an assortment of businesses. As always, apply due diligence and research the company before signing a contract.

No disaster recovery plan is foolproof, but it can go along way towards protecting you. Ask Air Canada personnel. They're struggling as I write this to recover from a computer hack attack that demolished their online booking system, leaving travelers grounded for days. One can be sure the national airline will be revising their disaster recovery plan in the weeks ahead.

Do yours now.

---

How to Write Business Plans, Business Proposals, JV Contracts, More!  
No-cost ebook "Beginners Guide to Ecommerce".  
Business Writing by Nightcats Multimedia Productions  
[www.nightcats.com](http://www.nightcats.com)

---