

WRITING SAMPLE

IS YOUR COMPANY MEETING THE DATA-BACKUP CHALLENGE?

DATA LOSSES, SYSTEM CRASHES, NATURAL DISASTERS – THEY DON'T JUST HAPPEN TO THE "OTHER GUY." MAKE SURE YOUR BUSINESS CAN RECOVER YOUR MOST PRECIOUS ASSET: YOUR INFORMATION

By Rick Chernick
Chief Executive Officer
Camera Corner/Connecting Point

Whether it's a small manufacturer, an independent insurance broker, a foodservice distributor, or travel agency – virtually every small and mid- sized business (SMB) in almost any industry segment increasingly relies on computing infrastructures to help automate, manage, and analyze its operations. But what happens when those computing services are interrupted?

The risks aren't just limited to hurricanes, tornadoes, and floods. They can arise from *any* event that prevents you from accessing the data you need to operate – a regional power outage, a virus outbreak, employee sabotage, external data fraud/hacking, or devastating terrorist attacks.

We all like to believe that there's only a very low probability of these events striking us. But that simply isn't the case. Every company faces the risk of IT interruptions that can grind business to a halt – and the implications of these disasters are ominous. Computing interruptions and data losses can cripple your business by hindering customer service, lowering productivity, reducing sales performance, or creating embarrassing episodes that lower customer and investor confidence.

According to Gartner, 50 percent of all small and mid-sized businesses facing a computing interruption will go out of business within three years, if they can't get their data back within 24 hours. Amazingly, however, nearly 40 percent of small and mid-sized businesses don't backup their data at all.

Depending on the industry and other factors, every hour of computer downtime costs businesses hundreds of thousands – even millions – of dollars. Given the stakes, *every* SMB needs a complete backup plan.

FACTORS AND DECISION CRITERIA TO CONSIDER

Many of the SMBs we work with have increasingly expressed a strong preference for new, streamlined processes and technologies that can simplify the backup process – and make it more likely to be effective. When you're ready to evaluate a backup strategy for your business, you may find it helpful to consider the various factors that other SMBs have used to make their decisions.

- **Offsite Storage** – It's not enough to make a data backup (disk OR tape). You have to get it far away from your main computing site. After all, if a natural disaster hits your building where your primary and backup data are co-located, you're still out of luck. It's essential that your backup data is stored far away from your computing systems.
- **Disk-Based Technology** – Businesses today have spoken loudly – *no more tape-jockeying* for data backups. Virtually every computer uses hard disk for storage today – so why would you still rely on outdated tape for backups? Without question, tape can play a valuable role for longer-term

archiving, where the odds of needing a retrieval are extremely low. But for routine near-term daily backups, tape can be too labor-intensive, time-consuming, and inefficient way to store data. And the failure rate for restorations from tape is alarmingly high. Today, as the prices of disk storage and network bandwidth continue to decrease, online disk-based backup solutions are more than cost-competitive. And the greater reliability is what you want in a backup solution as well.

- **Automation** – Too often, over-taxed IT managers and staff can overlook the crucial nightly tape backup process. That can leave you unnecessarily exposed if disaster strikes on one of those occasions. Look for an unattended solution that can automatically backup your data – without requiring human intervention.
- **Online Movement** – Perhaps the best way to move data offsite efficiently is to use a remote backup facility. By transmitting only the changes to your data – the so-called “deltas” – you can move your data to a remote location to reduce the risk of data corruption, loss, or failure. For example, Hewlett-Packard’s Smart Desktop Management Service can move data offsite through a simple network connection to provide *remote* backup and retrieval of critical data.
- **Continuous Coverage** – Typically, tape-backup processes take place nightly. For example, at the end of each day, your tape drive captures a snapshot of your data at that point in time. But, if you have a data failure at, say, 3 p.m., your only recourse is to restore data from a tape made almost a day earlier. You’ve lost all of your data that’s changed since that backup was made. For many businesses today, that’s an unacceptably long gap. They’re increasingly adopting “continuous data protection” that transmits changes over the network to the remote facility as frequently as every 15 minutes. When it comes time to restore your data, you can load data from as recently as 15 minutes prior to the outage or failure.
- **Long-Term Histories For Compliance** – In many regulated industries, you’re required to store customer data for extended periods of time. As a result, many businesses work with partners to store their data for up to two years – and then move the information to long-term archives on CD-ROMs or other permanent media.
- **Better Virus Protection** – If a virus strikes your server, it can infect the very tape backup systems you’re counting on for backup protection. With remote online backups, you’re protected from viruses by simply rolling back to the last uninfected backup.

- **Faster Recoveries** – When your systems are down, every minute costs you money. With online, disk-based backups, there are no tapes to sort through and load. In most instances, it's as simple as pointing and clicking to choose and restore files from disk backups.

Given the potentially enormous long-term costs and implications of a business-systems interruption, it's important to carefully evaluate and implement plans to mitigate the damages and costs. It's critical to remember that, while you can't control many disaster events or data corruptions – you *can* implement sound plans to ensure your business doesn't miss a beat.

Rick Chernick is the chief executive officer for Camera Corner/Connecting Point, a 52 year old technology firm, based in Green Bay, Wis., that specializes in technologies focusing on business improvement tools from computers, software solutions, security, photo, and video. He holds a bachelor's degree in business from the University of Wisconsin – Green Bay and serves on Hewlett-Packard and Lenovo councils.