Protecting your Data

CASE STUDY

Power struggle: data backup dilemmas

SITUATION Dean Parnell has handled data backup and systems administration in a variety of small businesses (usually as the only IT resource) for over 13 years. Although he now works for a multi-branch organization, he vividly recalls the data backup challenges small businesses face and offers a real worst-case scenario.

"Most small businesses don't realize what data backup does for them until they have a problem and it's not there," Dean points out. "That's what happened in a DVD replication business I worked for. They had spent a small amount of money on backup tapes, but the business soon outgrew that solution — they were handling a lot more data."

Dean urged the company managers to upgrade their backup strategy and put an emergency plan for data recovery in place, but they didn't want to allocate any budget or time for a policy or new solutions. And then the power went out.

"One day a drunk driver hit a telephone pole and knocked out power to most of the grid. No one took any steps to save our data — I was away and no one knew what to do. The servers ran on battery power for two hours and then failed, losing most of our data. We had to get a lot of new copies from customers and there were major delays to our schedules."

RESULT Although they were growing at the time, the company is no longer in business today — not specifically due to this incident, but it didn't help. The business was viewed as a technology company which should be able to manage an essential technical process like data backup.

Dean adds, "Every business needs a backup routine and an emergency plan. Also, they need to test their plan to make sure they're not storing incorrect or corrupt data. Even a business that has appropriate backup solutions and policies needs to do a full test restoration of their data quarterly."

Photo source: Veer® stock photos.
Photo does not represent Mr. Dean Parnell, or any related associates or products.

CenturyLink™ Business

Plugging the protection gap

Data backup is a priority for businesses of all sizes. Even if you are your venture's sole employee, you'll likely have customer information and other data you'd greatly regret losing or damaging. Appropriate data backup will minimize those risks.

And you don't have to be an expert to put the right plan in place. See the facts and ideas below to get started.

What is data backup?

Broadly speaking, data backup means **ensuring the security and availability of your critical business information**: financial records, customer information, transactions, schedules, documents, etc. You want to make sure your critical data is safe and that you can always access it when you need it. There are two main ways to back up your data:

- **Offline data solutions:** You can save your files to traditional physical media such as digital tapes, virtual tape libraries, CDs, DVDs, flash drives, external hard drives, onsite servers, virtual servers and network attached storage (NAS). These options are generally affordable on a tight budget and may be all you need if your store of data is small and slow-growing.

  It's a good idea to store some copies of your most important data offsite in case of fire or natural disasters. Your plan could include anything from taking disks home and securing them in a safe to using professional storage (such as Iron Mountain's offsite tape vaulting service) for ultimate security.

  Also, it's advisable to encrypt your backup media to help prevent data theft in case your backup media are lost or stolen. Encryption software encodes data into an unreadable series of characters with a secret key or password so you can send or store it securely.

How much can data loss cost a small business? A survey of 1,425 SMBs worldwide showed that SMB data loss incidents were followed by lost sales in 30% of cases, lost customers in 20% and severe business disruption in 25%.

— Symantec, 2009[2]

- **Online data backup solutions:** With this method, your data is transmitted to a remote location and stored on servers. You could set up your own secondary backup location, but a popular low-maintenance option is to use an online data backup service, a.k.a. cloud or remote access services. Online data backup solutions collect, compress and transfer your data to a remote backup service provider's servers.[1] (Providers also typically offer the option to encrypt stored and transmitted data.) It's essentially the "set it and forget it" option — you can automate your online backups and eliminate both the human error and effort that data backup normally requires.

Am I legally obligated to back up my data?

Depending on your industry, regulations may require that **all of your key business and IT assets are protected in the event of a disaster or accident**. Even less privacy-sensitive businesses may be required by state and local laws to make sure employee records and customer information are kept safe and complete — no matter what.

How will it make my business better?

Think of it as information insurance. When you have appropriate data protection in place, you will:

[1] http://en.wikipedia.org/wiki/Remote_backup_service

[2] "SMB Protection Gap." Symantec, 2009. www.symantec.com/business/solutions/article.jsp?aid=20090428_global_study_identifies_smb_security_gap

CenturyLink™ Business

- **Recover from incidents faster and more reliably.** Being able to recover information quickly and easily is especially important if your business relies on customer service.
- **Save time and hassle.** Data backup is like any other process: When everyone in your business understands when and how to do it, efficiency improves and your management burden decreases.
- **Enjoy greater control and stability.** When you have the right solutions and support to reduce data risks, you keep the focus on building your business, not rescuing it.

How do I get started?

Naturally, your data backup strategy will vary based on the size and type of your business, but here are some basics:

☐ Identify the information you need to back up

Mapping out your vital information will help you determine how and when to back it up. List your accounting information, business plans, customer databases, vendor information, marketing documents, etc. Include older records as well as current info.

Next, divide your list into confidential and non-sensitive data. Finally, define and limit who has access to your business' confidential data.

☐ Choose your backup solution

Your optimal backup solution will depend on how much data and IT support you have. If you only have a small amount of confidential data to back up and not much else, an offline solution may be ideal. If you also have lots of non-sensitive data and little in-house tech support, an online backup service can be a lifesaver. For details, please see our *Protecting your data* white paper.

☐ Set a backup schedule

How frequently you back up your data will depend on the type of data it is and how often it changes. You may only need to back up certain files once a month if they are rarely updated, but other items may need backup every day. Also consider if and when you need to keep older versions of your data, and be sure to dispose of outdated information securely.

☐ Test and review your solutions regularly

Once you invest time, energy and money in a backup system, it only makes sense to ensure it passes the ultimate test: full data recovery. Do a test restore shortly after launch, then once every few months. (If you use a hosted solution, ask your vendor how often they test the system.) Review data backup options online — you may find better or more cost-effective solutions as technology advances.

Know the risks

Even if your business isn't data-driven, any critical information on your computer workstations, networks, portable drives, laptops and phones will be vulnerable to:

- Accidental loss
- Hard drive failure
- Theft
- Data corruption
- Employee sabotage
- External attacks
- Natural disasters
- Power outages

And if your business depends heavily on data — if you're in marketing or finance, for instance — damage or loss **can undermine your credibility as well as your day-to-day business.** Fortunately, there are also plenty of accessible data protection solutions for small businesses.

Related guides:

Preventing security threats and stopping unwanted activities

Maintaining compliance

Managing data storage

Maximizing your Internet connection

For more detailed information about protecing your data, please refer to the accompanying white paper on this topic.

CenturyLink™ Business

Need more? We're with you.

Your community representative is always happy to help. You can count on them as a resource for compliance solutions to consider that fit your specific business needs, budget and level of expertise, as well as advice and resources on a range of small business technology issues.

Visit **http://centurylink.com/smb-resources** to contact your community representative, and learn more about how technology can boost your business. You'll find information sheets, videos, case studies and more.

Visa estimates that approximately 85% of data breaches occur at the small business level.

— Better Business Bureau[3]

[3] www.bbb.org/data-security/intro-to-small-businesses/

CenturyLink™ Business