Your Data Security Report

“7 Essential Questions Every Business Owner Must Ask About Their Data Backup, Security and Disaster Recovery”

Too busy to read it all?
jump to page 6

HardSoft Systems Ltd www.hsl.ca or info@hardsoft.ca 905 631 3075

Why Did We Create This Report

From The Desk of: Dan Struthers
CEO - HardSoft Systems Ltd

Dear fellow Business Owner,

Have you ever lost an hour of work on your computer?

We wanted to give Business Owners and CEOs an informative, easy to read guide that would explain what they need to know about backups, security and business continuity (a 50 cent word for keeping your business up and running).

By investing a few minutes in reviewing this report, you are putting yourself far ahead most business owners who never get around to thinking about this issue until it's too late.

I hope that you find in this report the information and the encouragement that you need to put the proper systems in place now so you can sleep easier at night knowing you're prepared for the worst;

Dan Struthers
CEO– HardSoft Systems Ltd.

Hope is not a Strategy!

After working with hundreds of small and mid-size businesses in the Greater Toronto Area (GTA) we found that over 80% of business owners we talk to do NOT have a reliable backup of their data and do NOT know how or what they would do in the event of a data-erasing disaster. They simply "hope" their backup is/was working and that it will save them when disaster strikes.

- **96% of all business workstations are not being backed up** *(Contingency Planning and Strategic Research Corporation)*
- **58% of downtime incidents are caused by human error alone**.*(Enterprise and the Cost of Downtime, Independent Oracle User Group, 2012)*
- **93% of companies that lost their data center for 10 days or more during a disaster, filed for bankruptcy within one year of the disaster** *(National Archives & Records Administration in Washington)*

Get Personal - What is the Cost of a Data Loss?

I can quote the above statistics but in reality the only statistic that is important to you involves your business. If you could not access our computer data for 6 hours, what would the total cost to your business?

- Direct revenue lost that day, opportunity costs, cannot quote or schedule work – lost business
- Cost to catch up once the data is available – overtime, etc

Below is a quick way to estimate the cost of a data loss or the inability to connect to your server. For this example we show 5 employees with a chargeable time of $ 80 per hour. If you were not able to access data for 6 hours, the cost would be $2400 dollars.

		Cost of Downtime Calculator		
Line	**Employee Productivity**			
1		Number of Employees:	5	
2		Average Chargeable time per hour per Employee:	$ 80.00	
3		Loaded Cost of employees per hour (line 1 x line 2)	$ 400.00	per hour
	Lost Employee Productivity Cost			
4		Total Hours the system is down:	6	hours
5		Loaded cost of employees from line 3	$ 400.00	
6		**Total Cost of System Downtime (line 4 x line 5)**	$ 2,400.00	

HardSoft Systems Ltd www.hsl.ca or info@hardsoft.ca 905 631 3075

Data backups are performed for 3 main purposes:

- Rapid recovery from data corruption, hardware failure, or human error
- Long term storage of data. Archive / Compliance / Audit
- Disaster recovery

Each has different time and location constraints.

- ✓ **Recovery from data corruption** needs most rapid recovery speed, and location of backup does not matter (however, you do not want your Rapid Recovery Server located in a different city, campus, or if possible, building)

- ✓ **Long term storage of data**. Speed is not as much an issue, location dependant in as much as it must be access controlled otherwise, when used for compliance / audit, it may not be accepted if too many people have access to it as the archives may have been tampered with.

- ✓ **Disaster recovery**. For this scenario, speed is not as much an issue as location, the backup data CAN NOT be in the same facility, otherwise the backup data will not be accessible (just like the live data) if the facility itself is not accessible or if it has been compromised.

So, what does this mean? Data backup is only ONE aspect of what's REALLY important: disaster recovery, or your ability to RESTORE the data in a usable format quickly and painlessly

Too often we see clients with the raw data backed up but not the server operating system, nor the configuration of the server. As a result, the rebuild is longer and costlier than it has to be.

Data Sovereignty

Is your data stored in Canada? If you are using many of the standard cloud providers your data may be at risk. Why? The **USA Patriot Act** signed into law in October 2001. Under the Patriot Act any US government official can, under suspicion only, seize servers. If your data happens to be on that server, your data is lost and most likely being read by a US Government Agency. This sounds like science fiction, but there have been numerous seizures of servers in the U.S. Why risk having your data looked at by the US Government when there are many Canadian cloud suppliers that can provide you with a safe and secure data backup solution. **All HSL servers are located in Canada and all HSL Backup servers are themselves backed up. We believe this strategy provides our customers with the best security possible.**

Backing Up to the "Cloud": What it Means and the Secret Cloud Strategy

One of the BEST ways to protect your data is to maintain an up-to-date copy in a high-security data center somewhere other than your office. The generic term people use to describe this type of backup is "backing up to the cloud" or "cloud backups," which simply means that your data is hosted in a remote data center and accessed via the Internet.

This type of backup is set to run automatically either after hours, when most people are not using their computer systems (1:00 a.m. for example), or continuously throughout the day whenever a file is changed or added. The data on a particular machine is copied and sent over the Internet to a high-security facility where it is stored. Because these backups are automated, you don't have to worry about someone forgetting to run the backup.

Is a single day cloud backup enough?

Most companies, if they have a backup, will have one overnight backup plan in place. In the past this would be acceptable. Nowadays, with the intelligence of Ransomware, virus and malware, a single overnight backup is not enough. In addition, the price of storage is very low so why not add that extra protection?

The secret cloud strategy that many of our clients have adapted is to expand their data backups to a model that **includes the last 5 days plus the last two months**. Why so many backups? If someone accidentally deletes a file on a Thursday afternoon but does not discover the deletion until Monday, under normal overnight backups, the file would be lost. With a 5 day backup solution you can quickly restore a deleted file.

What About Email?

One of our clients was using a very large US company for his email. As part of his 5 day plus 2 month data backups we included his outlook .ost/.pst files each month. One day he accidentally deleted a very important contact. When he called his email provider he was told they do not backup contacts. They only backup email for the last 14 days. By backing up his outlook files we were able to restore the contact for him in a matter of minutes.

Don't Assume – Get the Facts About Your Backups

7 Essential Questions You Need to Ask About Your Data Backup, Security and Disaster Recovery

- ❑ **Have we calculated our true cost of downtime** if we could not access our data? (see chart on page 3 for help) How many hours can we tolerate without our data?

- ❑ **How do I recover my data?** "If my server crashes beyond repair, how exactly do we recover and how fast can we retrieve our data?" Is this time acceptable?

- ❑ **If our building was not accessible tomorrow morning** due to poor weather, or an emergency activity, can we easily access our server? If the power to the building is off, how can we access our data offsite?

- ❑ **Do I get a report each day that the backup actually happened and without errors?** Have we ever tested the backup to see if it is truly working?

- ❑ **Is our server being monitored in real time?** If our server is offline – can we talk to a technician right away or do we fill out a form or submit a ticket and have to wait for an email or phone call.

- ❑ **Does our server have backup power and has the UPS been tested?** Many times the UPS is plugged in but the software to the server has never been installed.

- ❑ **Do we have a data backup of the last 5 days and last 2 months?**

Bonus Question(s)

- ❑ **Do I have a written IT disaster recovery plan**? As the saying goes, "by failing to plan you're planning to fail;" has your IT person sat with you to create the plan and has it been tested?

- ❑ **I am using a big brand name for email and data backup.** Do they backup everything? I need to call and check what specific data they backup and what is the exact procedure to recover data? Will they assist me?

- ❑ **What about archiving email?** Do we archive our email and contacts locally on a regular basis?

Our Free Data Backup and Security Audit Will Give You Peace of Mind

If you are worried about whether or not your current backup and security processes are up to par, I'd like to give you a **Free Data Security Audit ($397 value)** as a means for introducing our services to you. Why do we do this? Simply because I know how confusing and difficult it can be to find a good IT support company that is responsive, easy to work with and actually knows what they're doing. We find that offering this free service is a great, no-risk way of demonstrating how we can help you. At the very least, you'll get a free third party evaluation of your current backup, which is extremely valuable.

What do you get?

- ✓ Audit of your current data security and protection, including backup and restore procedures, tape drives or other onsite backup devices to validate if all of your data is actually being backed up in a format that could quickly be restored. (We often discover data on drives, laptops or PCs that is overlooked.)

- ✓ A simple and easy to understand report that will detail the makeup of your data, including the age and type of files you are backing up. Why should you care? Because many companies inadvertently use valuable computer storage to back up their employees' personal MP3 files and movies.

- ✓ Answer any questions you have about backing up and securing your data. We know everyone has a different level of risk tolerance, and we want to make sure all the risks you're taking with your data are by choice not because of miscommunication or accident.

Depending on what we discover, we'll either give you a clean bill of health or reveal gaps in your data backup that could prove disastrous. If it's appropriate, we'll provide you with an action plan for further securing your data with various options.

But I Don't Need a Backup and Security Audit Because My IT Guy Has It Covered

Maybe you think your data is perfectly safe. Many of our current clients came to us after they discovered how hard it actually was for them to RESTORE THEIR DATA when it became necessary. Unfortunately, that is when most companies "test" their data backup and restore solution.

HardSoft Systems Ltd www.hsl.ca or info@hardsoft.ca 905 631 3075

How to Request Your Data Backup and Security Audit

1 Call our office at 1-800-263-8433 and ask to speak to Joe

2 Send us an e-mail: info@hardsoft.ca

3 Go online: http://www.hsl.ca/free-analysis/

As soon as we receive your request, we'll call to schedule a convenient time for us to meet with you and to conduct the audit of your backup system. Again, you are under no obligation to do or buy anything.

We hope you have found this report helpful. Please check out our website www.hsl.ca for more information and free resources.

Thank you