Crash Protection

Mind Your Data Like You Mind Your Business

By Matthew Price

It's 7:00 a.m. on Saturday, and after what was supposed to be a routine storage upgrade to our file server, I hear these dreaded words "Your data has been lost, do you have a good tape backup?"

Fortunately, in my case I did have good tape backups and was able to recover all but a limited amount of data. Our project files, operating system, accounting database, and administrative functionality were recovered in time for the next business day.

"...intellectual data... is our product."

For a consulting engineering company, intellectual data, which *is* stored on our computer network, is our product. Protecting that product is vital to the solvency of the company. Owners and IT Professionals should know the importance of protecting this vital asset. So what could have happened if I didn't have "good tape backups"?

Here are a few facts associated with data loss.

- Most companies value 100 megabytes of data at more than $1 million. *(Ontrack Data International, Inc.)*
- 43 percent of companies experiencing serious data loss disasters close and never reopen. *(McGladrey and Pullen)*
- A company that experiences a computer outage lasting more than 10 days will never fully recover financially. 50 percent will be out of business within five years. *("Disaster Recovery Planning: Managing Risk & Catastrophe in Information Systems" by Jon Toigo)*

Hardware malfunctions, system malfunctions and human errors are the reasons for the majority of system failures. Software corruption, computer viruses and physical disasters like fire and water damage account for the remainder of lost data and downtime.

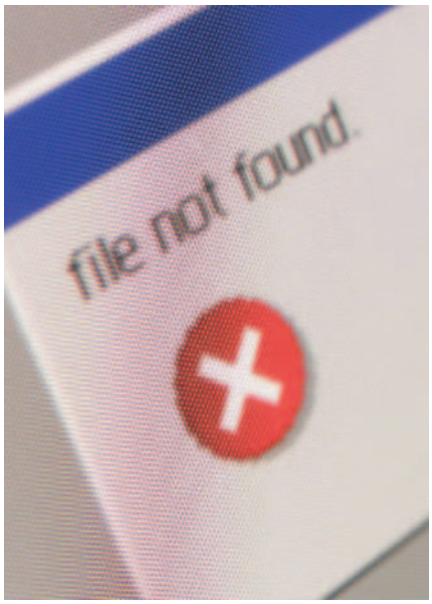
So, what can we do to prevent data loss?

Developing a disaster recovery plan is the first and most important step

The amount of time it takes a company to become fully operational again after a disaster depends largely on the safety measures taken ahead of time. How long can your business remain afloat without your critical data? When deciding on a recovery plan, consider how much money you are willing to spend given the value of your company's intellectual data and your tolerance for downtime. For example, a real time fault tolerant system is costly, but ensures continued operation in the event of a disaster.

A real time fault tolerant system might include a second set of servers located off site that will automatically take over in case of a server failure at your primary location. There is the less expensive, typical alternative of a short time fault tolerant strategy, but be prepared to survive a few hours of downtime. The next step is to determine which data is most critical, and ensure that you will be able to restore this information in the event of a disaster, so your organization can resume business. Document all the software and hardware settings on each server so you can quickly recreate configuration settings.

"...be prepared to survive a few hours of downtime."



Good hardware is essential for good reliability

Always purchase your hardware from highly regarded companies with a good reliability, service and technical support. In my case, the hardware manufacturer's technical support was able to walk me through the reconfiguration of the server hardware after the data loss, my first step in the recovery process.

Purchase servers with a pair of power supplies, multiple RAID controllers and multiple network interface cards, which connect your computers to each other. If one of these components fails, you have a backup and can continue to operate while repairing the other.

"...increases performance and greatly improves system reliability..."

Redundant Array of Inexpensive Disks (RAID) can offer protection from disk failure. A RAID system consists of multiple connected disks, managed by a RAID controller, which writes small amounts of data to each disk. It essentially spreads the data more thinly, or "stripes" the data. This increases performance and greatly improves system reliability because if one disk fails, the data is still protected. RAID systems vary greatly in complexity and price. You can purchase a simple RAID system, such as the one used in our branch offices, starting at a few thousand dollars.

Shield your system from environmental factors

Keep servers and IT systems in a safe, dry, cool and dust free environment. Restrict access to your server room. Install a dedicated cooling system if necessary.

Power failures and surges account for up to 40% of all system failures resulting in data lost. By installing an Uninterruptible Power Supply (UPS) you will be protected from any sudden or unpredictable power surges and outages. A good UPS should keep the system running long enough for the systems administrator to do an orderly system shutdown.

With our growing dependence of the Internet, the threat of losing data from computer viruses and worms increases everyday. Regularly updated antivirus software and a properly configured Internet firewall can greatly reduce your chances of viral infections. Consistently warn your employees of the dangers of virus infection and notify them of new viruses in the wild.

A backup strategy is at the heart of any recovery plan

For low cost and convenience; tape backups are hard to beat. However, to perform full tape backup can be extremely time consuming. To reduce backup time and the amount of data backed up daily, you need to develop a backup strategy. The most popular backup strategy is a three-generation system known as grandfather, father, son (GFS). Typically, a full backup is taken at the beginning or end of each month (grandfather), another full back at the beginning or end of each week (father), with differential or incremental backups in between (son).

A GFS backup creates day-to-day backups of the current week, week-to-week backups of the current month, and month-to-month backups of the current year. Test your backup tapes on a regular basis to confirm that all your data is being backed up correctly. Backups should be stored onsite in a fireproof safe and a duplicate set of backups should be stored offsite in a secure location. During my recent disaster recovery, I first recovered from our full weekly backup (father) then recovered the remaining data from our daily incremental backups (son). The system worked flawlessly, as designed.

Last but not least, invest in a knowledgeable, properly trained IT staff

A professional staff should be capable of keeping your company prepared for disaster. A qualified IT department can quickly recover your data and repair systems when there is a problem. Don't expect an Information Technology Systems Engineer to be a "jack of all trades". Seek different IT specialists for specific areas such as storage or security, etc. to assure that your IT systems are designed and managed properly.

Each one of the above steps will independently improve reliability and reduce the risk of data loss. By combining these strategies, you can protect your business data exponentially and build a practically fail-safe system.Last but not least, invest in a knowledgeable, properly trained IT staff.

A professional staff should be capable of keeping your company prepared for disaster. A qualified IT department can quickly recover your data and repair systems when there is a problem. Don't expect an Information Technology Systems Engineer to be a "jack of all trades". Seek different IT specialists for specific areas such as storage or security, etc. to assure that your IT systems are designed and managed properly.

Each one of the above steps will independently improve reliability and reduce the risk of data loss. By combining these strategies, you can protect your business data exponentially and build a practically fail-safe system.

Matthew Price is the Information Systems Manager for Stewart Engineering, Inc., a consulting engineering company based in Morrisville, NC.