Protecting your data

Considerations for creating and implementing a data back-up and protection strategy **Interviewed by Rona Gilbert**

With so many opportunities for things to go wrong, businesses are playing Russian roulette if they haven't implemented a plan for protecting essential business data. Even something as innocent as an unplugged server can wreak havoc on a business's ability to respond to customers. Add computer viruses, human error, and natural and other disasters to the mix, and the opportunity for lost data becomes very real.

Businesses of all sizes should take proactive steps to ensure their data is secure and able to be recovered in case of a disaster, says Ryan Stephens, president and CEO of Perpetual Technologies Inc.

Smart Business spoke with Stephens about the many ways businesses can lose data, the importance of protecting business data and how to go about it.

Ryan Stephens
President and CEO
Perpetual Technologies Inc.

Why should companies be worried about protecting their data?

Business thrives on data. Most businesses cannot survive without it. Companies store intellectual property, financial information, customer information and other critical information in a database. All of this critical data facilitates effective daily operations.

If data is lost or simply temporarily unavailable, consequences such as financial penalties, loss of productivity, loss of customers and ultimately, loss of the business can occur. All equate to a decreased ROI, which is clearly unacceptable for any technology investment.

How can data be compromised or lost?

Data protection means much more than protecting data from unauthorized access. Consider user error, hardware failure, power failure, inadequate backups and natural disaster. These are only a few serious threats that exist. Consider the number of businesses affected by Hurricane Katrina that failed to have a disaster recovery plan in place. How will they rebuild their data?

What measures can companies take to protect their data?

First, identify both authorized and unauthorized users of data. Then identify all possible avenues to access your data. Enforce strict security policies and monitor database activity routinely. Stay up-to-date with security threats; make sure you are proactive and have a remedy in place for violations.

Next, educate your users on security policies and how they can play their role in data protection. Finally, create a backup and recovery strategy. At a minimum, your strategy should include a standard backup and recovery plan, along with a disaster recovery plan.

Today, hardware technology and software solutions exist to provide data redundancy and quick recovery time. Service solutions exist that provide off-site data storage, off-site hosting and remote monitoring services.

Most important, test your backup and recovery strategy. Many business have never tested a recovery and don't know if it works, nor how to execute in the event of data loss.

How much do these measures cost?

Many factors determine the cost of these measures. Size of the database, criticality of the data and maximum acceptable database downtime are the main factors associated with the cost. The investment to protect your data can literally range across the board from a minimal investment to a small fortune.

Obviously, environments that must guarantee 24/7/365 uptime and near-immediate recovery will require more detailed solutions. For these organizations, the investment is worth it and a small fraction of the cost of the potential consequences.

What results will companies see from these measures?

Data protection is business protection. Technology is being used to maintain business stature and support growth. Data becomes business intelligence with customers and database end users as content.

In the long run, businesses should experience a much greater return on their technology investments. Home insurance is an investment most people are happy to make. A business owner is no more in the position to rebuild the business from scratch than the homeowner is financially able to rebuild a house that has burnt to the ground.

What qualities should a company look for in its technology partner?

Technology partners should be selected based on factors such as reputation, trust, past performance, known reliability, ability to respond and depth of technical staff.

Of course, cost is a significant decision-making concern. However, when comparing cost, make sure you are comparing apples to apples. Lower cost may equate to lower quality or less experience. Neither can we assume that greater cost equals better quality. Value is balance of opportunity cost and actual cost; so you will have to do your homework.

Finally, request past performance information, case studies and client referrals. The prospective technology partner should be able and happy to provide them without hesitation.

RYAN STEPHENS is president and CEO of Perpetual Technologies Inc. Reach him at rstephens@perptech.com or (317) 824-0393.

Insights Technology is brought to you by Perpetual Technologies Inc.