HOUSTON BUSINESS JOURNAL
Strictly Houston. Strictly Business.
Vol. 36 No. 26 Week of October 14 - 20, 2005 houston.bizjournals.com

Put plan into action to protect computer systems from disaster

Hurricanes Katrina and Rita showed how quickly life can change. Every hurricane that unleashes its fury on the U.S. mainland is a devastating reminder of Mother Nature's power to uproot residents and businesses. Immediate property losses can be staggering, especially for businesses whose electronic assets are destroyed by water or airborne debris. Every business needs an emergency preparedness plan.

TONY MICKLE

Data is the heart of any business. Whether it's critical customer information or propriety business data, it is the key differentiating factor between growth in today's competitive marketplace and failure.

With the stakes this high, it is surprising how few resources some of today's entrepreneurs dedicate to protecting the technology that stores and processes this vital business data. Many seek help only after a costly accident like a system crash, data loss, virus infestation, hacker invasion, or disgruntled employee sabotage.

Industry pundits reiterate the value of "availability" of a business computer system. A system is "available" when a company's employees can access all applications and programs. When the system is not available for business, it eats into profits.

Consider a company with fifteen employees with an average burdened per employee cost of $25 per hour and an average gross profit per person hourly cost of $50. If the system is available 98% of the time (94.6% is average for small and medium-size businesses), this translates to 2% downtime. How much will this cost the business? More than most would imagine:

Most businesses work approximately 50 weeks a year, 5 days a week, and 8 hours a day. That's roughly 2,000 hour a year. Two percent of 2000 is 40 hours. This results in loss of $1,040 in payroll alone, and $2,080 additionally in gross profit. Any entrepreneur can take several steps to make the company's information system withstand unexpected events and lead to higher profitability.

BACKUP

Establish proper backup process. The single most important issue in regards to availability is a reliable verified backup of all data. Having good backup ensures that no matter the circumstances - electrical blackouts, environmental threats, etc. - the company can always restore critical data and get operating again.

To ensure that the company has a reliable backup solution, it should have a policy (technical procedure) in place, and be sure to adhere to the plan to verify the consistency of all backups. This could be as comprehensive as doing an actual "mock restore" of the data to verify the viability of your backups. A copy of all backups to a secure offsite location, preferably out of state. (In the event of a disaster in your state, your data will be safe.)

REDUNDANCY

Many executives do not realize the importance of redundancy until a serious problem occurs. Having a sound and verified backup is an excellent safety net but does not prevent network downtime. Having a redundant IT Infrastructure is the only sure way to reduce your downtime.

When implementing a comprehensive redundant IT Infrastructure: invest in "doubles" of everything in your network! It is a simple idea that requires investments in money, time and expertise to implement; however, it will enable a company to reach the coveted five "9s" (99.999%) of data availability. For example, make sure the company implements two routers, switches, firewalls, data carriers, security software (antivirus), servers (such as domain controllers and application servers), data paths, etc.

SECURITY

Properly install and maintain system security software, Not all disasters come in the form of natural disasters - fires, hurricanes or earthquakes. More than likely, the disaster that affects a company will be a hacker - either internally or externally.

Security is a broad and extremely critical concept: however, there are several key areas:

- **Firewalls.** A company should have multiple firewalls in place. Not just on your network's perimeter, but also protecting the server and other important devices from internal employees. Most successful hacks originate internally, not from an external source. Also designate someone to be responsible for maintaining and monitoring the firewalls. Don't fall into the "set-it-and-forget-it" trap!
- **Antivirus.** A company should have, at the minimum, one antivirus software package that is installed on all devices. It is critical that it be updated on a frequent basis (hourly if possible) and that someone is responsible to maintain and monitor it.
- **Antispyware.** Antispyware is as important as an antivirus package. Many viruses and other malicious code are starting to be delivered via spyware. (Follow the same rules as you would for an antivirus package.)

There are several alternatives for implementing these procedures. Company managers can hire a consultant, but bear in mind that these experts likely have many other customers to attend to. If they hire an in-house IT professional, they should make sure the person has (at the very least) the minimum industry certifications and is proficient in more than one area. Or they can enlist the services of outside experts who have both the credentials and the availability to tend to the specific business needs of the company.

When choosing outside help, remember that the alternative must ensure high IT availability, reliability and security to keep the computers humming and your profits coming.

Tony Mickle, Senior Systems Engineer of Houston-based Xvand Technology Corporation (www.xvand.com), provider of utility computing services that allows businesses to take advantage of Fortune-500 class technology via a virtual IT department without the headaches associated with owning and managing an onsite network.

This article appeared on page 13 of the TECH-HOUSTON section of Volume 36, No. 23 of the Houston Business Journal on October 14-20, 2005.