

Security: What Every Business Needs to Know

Five Steps To Secure Your Business

For small and medium-sized businesses (SMBs), the impacts of a disaster can result in loss of or lack of access to data, applications, and work facilities. Those with disaster recovery plans in place fared much better than those without such contingency plans.

More SMBs Beginning to Plan for Disasters

While the business impacts of disasters—such as the loss of data and communications infrastructure, are widely understood, SMBs have been slower to develop disaster recovery plans as compared to larger organizations. But that appears to be changing.

According to the Yankee Group's 2006 U.S. Small and Medium Business IT Survey, *after security, the other major concerns of SMBs are now backup and restore and then application and data availability.* Globally, spending on data protection and recovery management among all businesses will surge from \$58 million in 2006 to more than \$200 million by 2011, according to research from IDC.

Yankee Group analyst Gary Chen found that among SMBs, *"Most are on the edge, where a couple of bad events could shut down business. They need regular backup, either traditional scheduled file-based or continuous. And they need to have it off-site and tested, to ensure they can bring up critical applications and data if headquarters is wiped out."*

People, processes, training, and planning are also part of effective disaster preparedness. Here are five key steps to consider when implementing a program for your company:

- 1. Understand what data and systems are critical to business continuity:**
Many governments have mandated the remote replication and storage of financial, medical, and certain other kinds of data. Businesses have realized that their data and applications are their life blood. Make sure you know where all of your company's critical data and applications are located and that they can be integrated into a remote backup solution.
- 2. Identify and fix single points of failure in your network, business processes, and people:**
In network design, redundancy eliminates single points of failure. Make sure that network elements — including switches, routers, and other components — are redundant and enabled with software failover features. Review business processes and job responsibilities to ensure that there are similar "failover," should a process or employee become adversely affected in a disaster.

3. **Create a workforce continuity plan:**

If employees can't get to their offices for days, weeks, or longer, it is important to understand what kinds of remote access solutions they need to continue being productive, based on their individual job requirements. For example:

- Back office workers need access to applications and data and can probably use e-mail or instant messaging to communicate.
- Other categories of employees whose jobs require a lot of collaboration may need high-availability voice-over-IP (VoIP) services along with access to corporate data and applications. The benefit of IP and Ethernet in a disaster is that they are so pervasive compared to other technologies that devices are truly plug and play.

Executives and employees who must interact with customers, partners, or the press may need remote communications solutions with guaranteed quality of service (QoS), a VoIP phone with guaranteed toll-quality service, and collaborative software applications like Cisco MeetingPlace, which allows audio- and videoconferencing.

4. **Create a disaster recovery plan:**

A formal plan should be initiated and endorsed by senior management and should involve all levels of personnel in your company. An inclusive process of gathering information and drafting the plan will create the necessary sense of everyone's ownership in and responsibility for disaster recovery. Every company's plan is unique, but common elements include:

- Risk and threat analysis
- Leadership and succession plan
- Emergency response plan
- Internal and external communications requirements
- Human resources responsibilities
- Facilities management
- Availability of information and communications technology
- Cooperation with first responders, public officials, vendors, partners, and customers

5. **Train your staff on disaster response:**

Training and practicing facilities evacuation and other emergency responsibilities for certain types of disasters relevant to your business could have dramatic consequences related to personnel safety, business continuity, data confidentiality, and asset security in the event of a real disaster.