

The Bottom Line



TECHNOLOGY SOLUTIONS FOR SMALL AND MID-SIZED COMPANIES

Volume 4, Issue 4

April 2007

Data Protection for Small to Mid-sized businesses

Information on protecting your company's vital data and options on how to do so.

One definition for data protection is "to protect against loss of data access." The need for protecting business data is universal, whether you own a small or medium size business or you are a large enterprise. Being able to backup and access data in times of need is crucial for any business today.

There are many different data protection options out there for small to mid-sized businesses. However, it is important to find a solution that works best for your business needs and is cost effective. Some examples include:

1. **Internal Storage** - This solution copies data to another disk and allows for fast backup and recovery. There is also no removable media. However, this solution tends to be the most

expensive.

2. **Tape Storage Systems** - The traditional method for backing up data to a removable media.

3. **Remote Service Providers** - This solution replicates data offsite to a storage system provider. However, a small business may not have the appropriate bandwidth needed to restore data.

4. **External USB Drives** - This solution copies data to another disk attached to a USB port. However, this option does not allow for cyclical backups and is not a rugged, portable media.

5. **Removable Disk System** - This solution is the newest solution. Backups are created to removable media with rugged cartridges.

A backup and recovery solution strategy should be specific to the circumstances of an individual company. Individual companies employ many different strategies for data protection. A few general guidelines for providing assurance that the information of a company is being protected includes:

• **Archive Backup**



data. Data that is unlikely to be used on a every day basis should be moved to another type of device where it is protected and can be recalled when needed.

- **Backup data on a regular basis.** Backups may be done as complete backups or some form of incremental backup where only changed data is backed up. Backups should be done on a periodic basis and done cyclically.
- **Remember to test backups regularly.** Backups need to be restored to provide some measure of assurance that the data protection being done will work when needed.
- **Notify your IT support.** If you notice a potential problem with your backups let your IT staff know as soon as possible.

It is important to remember that a small to mid-sized business has many of the same requirements for data protection as a large enterprise. Attention must be paid to providing data protection that meets the business's needs.

Things to Consider: Are you Concerned about Uptime?

An IT inventory and criticality review can help to determine how uptime can effect your business.

Okay, admit it. You are concerned about uptime! In fact, as a business owner it is one of your major concerns. If your computer systems are not up and running, you experience lost productivity, increased costs, lower levels of customer service, reduced employee morale and many other problems. So what can you do?

Many organizations start by completing an **inventory of their IT equipment**. The goal is to identify your Single Points of Failure (SPOFs). Once you identify your SPOFs, you can do something about them. Look at each component to determine if the failure of the device could cause an impact to your operations. For example, if you only have one hard drive, you have a single point of failure.

Next the **criticality review** examines time and its impact to your organization. At what point does having your printer down move from low priority to medium and then to high? Maybe you can last a couple of days without a printer or perhaps even weeks if you have other printers in your office. If Internet connectivity is important to you, and you only have one line, it may be a high priority from the first hour of downtime.

Now that you have a criticality review and inventory of your IT equipment, the last step is a plan to build in redundancy and/or replacement. In the printer down example, you may be able to shift printing from the down device to another printer in your office. If Internet connectivity is critical, you may need to install a second line. A RAID system may help protect you from a hard drive failure.

If reliability and uptime is important to you, identifying your business's SPOFs is your first step to increasing confidence in your IT systems. Contact Black | Line Consulting if you would like a Network Assessment done to help you identify and fix your business's SPOFs and increase your uptime. Black Line can be reached at (630)388-1700 or by email at support@blacklineconsulting.com.

Things to Remember:

- Perform backups regularly for all irreplaceable data.
- Regularly monitor backups to verify the integrity of the backups.
- Notify your IT support as soon as you notice a potential problem with your backups.

The Bottom Line

TECHNOLOGY SOLUTIONS FOR SMALL AND MID-SIZED COMPANIES

Black | Line Consulting
1560 Wall Street
Suite 105
Naperville, IL 60563

Phone: 630-388-1700
Fax: 630-388-1697
E-mail: sales@blacklineconsulting.com

Data Protection for Small to Mid-sized businesses

Things to Consider: Are you Concerned about Uptime?

10 Tips for Using Instant Messaging in Your Business

Tips for Instant Messaging in your business. Protect your business and your employees with these dos and don'ts.

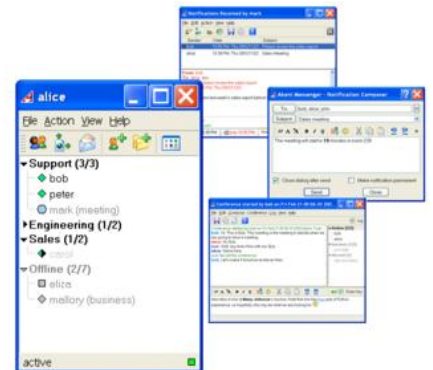
"Instant messaging [IM] could well be the dial tone of the future-albeit a silent one," says The Wall Street Journal, noting that more than 200 million people are now sending IMs. The above number also includes employees who use IM at their business. Whether it's for a meeting or receiving real-time information from vendors or suppliers, employees from businesses large and small are using it as a communication tool.

However, aside from the opportunities for time and cost savings, there are risks and downsides to IM use as well. Here are 10 IM do's and don'ts many business owners should consider.

1. **DO:** Create a user policy for IMs. Employees need to understand what is okay and what is not okay

from company standards.

2. **DON'T:** Use IM to communicate confidential or sensitive information. IM is better suited for quick information to avoid a phone call or email.
3. **DO:** Organize your contact lists to separate business contacts from family and friends.
4. **DON'T:** Allow excessive personal messaging at work. Urge that personal chats be done during breaks or on their lunch hour.
5. **DO:** Be aware that instant messages can be saved.
6. **DON'T:** Compromise your company's liability or your own reputation. Be careful about what you say regarding other companies or employees.
7. **DO:** Be aware of virus infections and other security risks. Learn about the quality of your own firewall protection before allowing file transfers via Instant Messaging.



8. **DON'T:** Share personal data or information through IM.
9. **DO:** Keep your instant messages simple, to the point, and know when to say goodbye.
10. **DON'T:** Confuse your contacts with misleading user names or status. User names should be consistent throughout the company and users should update their status regularly.