

You're Not As Backed Up As You Think

By Salvatore Salamone,
Executive Editor, Ziff Davis Enterprise

Introduction

IT departments typically configure user PCs so all work files are stored on network drives. But most users circumvent this approach, storing many files on their hard drives. Additionally, laptops users often work outside the office and offline, synchronizing only sporadically and keeping their current work on the local drive.

As a result, data is frequently residing on local drives, where it is not backed up. If a computer experiences a hardware problem or is lost or stolen, the consequences to the organization can include exposure to regulatory and legal risks, lost user productivity, and financial loss.

Data at Risk: Challenges of Data Backup

Many companies are under the assumption that, because their users connect to the corporate network, the data on those computers is safely backed up. The general impression is that user spreadsheets, documents, presentations, and other files are routinely stored on a designated network drive, which is automatically backed up by IT.

Gartner study found that annual failure rates (AFRs) for desktop computers are about 5 percent in a computer's first year, and 12 percent in its fourth year.

If a failure does occur, data recovery efforts can be implemented. If this is done internally, it can be a serious time sink, as it usually requires that the hard disk be removed from the crippled machine and installed in another system. Alternatively, the process might require complicated data recovery tools that operate at the byte level to extract data from a corrupted or damaged drive. Either approach essentially diverts an IT staff's efforts from other, more critical chores.

Alternatively, a damaged system can be sent to a company that specializes in data recovery. But the cost of using such a service is often hundreds or thousands of dollars or more per incident, and as a result, this method is usually undertaken only in special situations, such as when an executive loses critical financial information or strategic plans.

Another potential data loss with desktops involves computer theft where the entire system (hardware and data) is removed from the office.

There are additional problems when laptops are involved. By virtue of their mobility, off-network usage increases the chance of data not being backed up. That can be trouble, as laptops are more susceptible to problems.

Notebooks have higher (relative to desktop systems) AFR of 15 percent in the first year and 22 percent by the fourth year.

Additionally, laptops are more prone to theft and loss. The FBI, Gartner, and others peg laptop theft rates at between three to seven percent.

The laptop theft problem is pervasive. Fifty percent of the 403 senior managers surveyed in the Computer Security Institute's 2007 Computer Crime and Security Survey said their organization experienced laptop or mobile device theft within the last 12 months.

EXECUTIVE SUMMARY

- Growing volumes of valuable corporate data is routinely maintained on desktops, laptops, and mobile devices outside the office
- Organizations are under increased pressure to meet new data retention and protection laws and regulations
- Data backup and restoration tasks are often time-consuming and complex
- Data recovery from off-site tapes often exceeds practical (and acceptable) restoration time limits
- MozyPro™, a SaaS offering, provides an easy-to-use, secure, and robust way for an individual, small company, or large enterprise to backup and restore data

But this is hardly the case. Users often prefer to save files to local drives, and with the increased availability of broadband and wireless connectivity, many users do some or all of their work off-network outside the office.

The question is what happens to that data if a computer crashes or is lost or stolen. IT departments must be prepared for such circumstances, as these events are fairly common.

For example, when it comes to computer crashes, a 2006

And very few of those laptops are ever recovered. In fact, some studies suggest that only about two percent of stolen computers are returned to their owners. Laptop theft and loss extend to all types of organizations. For example, a 2007 Associated Press news story reported that, on average, between three and four FBI laptops are lost or stolen each month.

Consequences of Data Loss

Organizations expose themselves to a variety of risks and penalties when data is not backed up properly and ends up lost.

For example, companies can be face regulatory violations. All U.S. public corporations are subject to reporting laws and regulations such as Sarbanes-Oxley. Companies that do business internationally are often subject to similar laws, such as Japan's J-SOX, France's LSF, Canada's Bill 198, and Australia's CLERP 9. In many cases, loss of data that must be retained in support of these reporting laws can carry significant fines and penalties.

Organizations expose themselves to a variety of risks and penalties when data is not backed up properly and ends up lost.

There are also legal risks. Changes to the Federal Rules of Civil Procedure have produced what are commonly referred to as new eDiscovery laws, which mandate that companies involved in litigation produce e-mail, documents, instant messages, and other electronic information. They must also show how electronic records are stored, retrieved, and deleted. A company in litigation that cannot produce subpoenaed information would risk losing the case or could face fines imposed by the court.

User e-mail brings added complications. Even though Exchange servers are routinely backed up, mail in a user's desktop or laptop PST file may not be. If the user does not back this file up, and the system crashes or is lost or stolen, this could raise problems in litigation if e-mail records are subpoenaed.

Lost e-mail could also mean that valuable corporate information is gone forever. At a minimum, the user is without his or her past e-mail messages, which can result in the loss of many hours of work as the user tries to re-establish message threads with colleagues and recreate the important information.

There are also financial considerations if data is lost. In particular, business can suffer if customer data goes missing. Here, the damage can be two-fold. First, there can be

a direct loss of business by virtue of not filling orders and losing the ability to contact customers with promotions or marketing materials. Second, there can be a loss of customer confidence, particularly considering today's concerns over identity theft.

Challenges with Traditional Backup Approaches

All of these factors simply reinforce the need for all data to be backed up securely and routinely. But there's the rub: Backup is often a complicated process for both IT departments and users.

Many backup solutions are complex, requiring many adjustments. And retrieval of a particular file, e-mail message, or data is frequently labor-intensive. In most cases, a great deal of user intervention is required to back up particular information, such as a newly created document or a PST file.

Additionally, mobile users must often synch their data manually when they return to the office. In many cases, their time in the office is hectic, as they are pulled in many directions for meetings, filing paperwork (such as expense or sales reports), and simply doing their jobs. They may not have the time to synchronize and back up their data, too.

There is also the IT staff's time to consider. Many backup solutions use tape for archiving and safeguarding data off-site. Restoration of lost data from tape is time-consuming and tedious (frequently requiring the mounting of many tapes to find the specific file or e-mail). If tapes are stored off-site, there is the additional time factor of physically retrieving the tape and bringing it to the office to locate the data.

While multiple tapes are mounted and searched to perform a retrieval, users lose time. If a file is lost permanently, there is additional time required to recreate the information. These factors combine to compound lost worker productivity.

Additionally, data can also be lost permanently if a backup tape fails or someone accidentally records over a tape.

Solution: SaaS Backup

Taking the risks, challenges, and potential problems related to improper backup into account, Ziff Davis Enterprise conducted a round-table discussion in February with senior IT managers and CIOs from financial services, government, entertainment, insurance, and various other organizations.

The round-table meeting focused on Software-as-a-Service (SaaS) backup.

While all of the attendees were familiar with SaaS, there were many different ideas presented as to how SaaS, in general, fits in with or differs from other services, such as outsourcing and management offerings. (See: SaaS at a Glance: How it compares to other services.)

SAAS AT A GLANCE: How it compares to other services

What's in a name? Where does SaaS fit in when compared to outsourcing and managed services?

Naturally, there is some overlap between the three.

Many tasks, such as desktop and server management, software installation, e-mail, and spam filtering, can be outsourced to a third party to offload the chores from an internal IT staff.

In many cases, these services are offered as managed offerings, which include service guarantees, customer service, and other options.

In contrast, SaaS is a way to offer an application—such as e-mail or backup—as a service. SaaS relies on a Web architecture rather than the traditional client/server model used to deliver many applications.

A SaaS effort might be home-grown and run on an organization's own Web servers, or it could be offered by a provider as a service (managed or otherwise).

Even with the diverse views as to how SaaS related to these other services, most round-table participants said they were already using SaaS in some form. For instance, one participant said his organization uses SaaS “when we have a small group that needs an application.”

Several managers noted the benefits as a reason they have adopted SaaS for some applications. “It is easier to use than setting up a [traditional] application and configuring a PC,” said one participant.

Some participants noted inhibitors to SaaS. “Our company culture prevents [its] use,” said one manager.

Interestingly, one traditional argument against

SaaS in the past has been performance. But none of the attendees raised this issue – perhaps due to the ubiquitous availability of relatively low-cost broadband services.

Others felt that their users would prefer SaaS over internal solutions. Even with internal service level agreements (SLAs), “there has always been a gentleman's agreement with internal IT departments,” said one manager. He noted that users are used to tiers of support. If a problem arises with an executive, IT jumps on it. If an office worker has a problem, their helpdesk ticket might sit idle for days before any action is taken. As a result, many of the participants believe users would like the idea of having a dedicated number of a SaaS service provider to call when problems occur.

Advantages of SaaS Backup

Overall, SaaS was widely embraced by the round-table participants. “We're using it more and more,” said a manager from a financial services company.

The basic premise with SaaS backup is that, whenever a user (in their office or in the field) connects to the Internet, data is backed up securely to a provider's servers. In fact, SaaS backup solutions are accessible anywhere over the Internet.

SaaS backup solutions are frequently easier to use than other, in-house backup solutions. They also automate the backup process, helping to ensure compliance with data retention laws while protecting critical information.

In this regard, several participants noted that SaaS backup would help with governance. “It could help with [data management] of both structured and unstructured data,” said one manager.

Mobile users are better protected using a SaaS backup approach, as their data can be backed up anytime they connect to the Internet. This is a huge advantage over waiting for the user to come into the office and synch their data to network drives manually. In fact, since most mobile workers routinely use WiFi hotspots and their home broadband connections to check Webmail (while not necessarily connecting to the corporate network), SaaS backup provides a much higher likelihood that critical files will be protected.

Another benefit of SaaS backup is that files, messages, and other data can be found and restored faster and easier than when using tapes. This removes one of the biggest problems with traditional backup: Time to restoration. “The main issue is how quickly you can get to off-site storage for retrieval,” said one manager. He noted that with tapes, companies must also factor in the time required to search multiple tapes for a particular item.

SaaS backup solutions deliver the comparable benefits of using a virtual tape library, but with the added protection of having the data stored on secure, off-site servers.

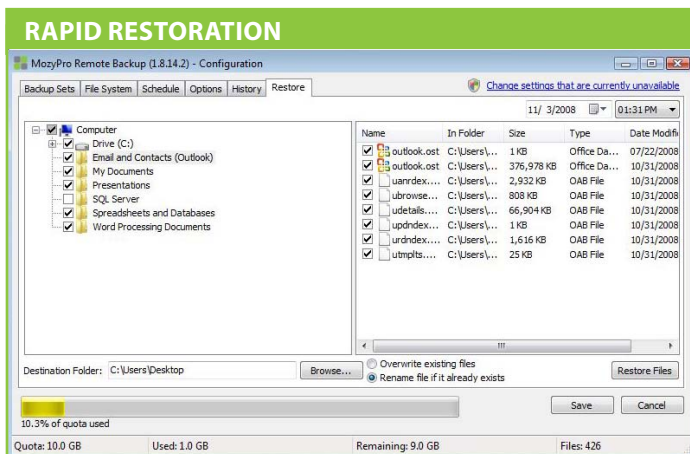
SaaS backup addresses both of these issues. Essentially, SaaS backup solutions deliver the comparable benefits of using a virtual tape library (namely, a solution that uses more reliable disk-based storage), but with the added protection of having the data stored on secure, off-site servers.

IT management chores are also reduced with SaaS, because fewer backup devices need to be maintained. “This would allow [the IT department] to focus on other work,” said one manager.

Points to Consider

When selecting and using SaaS backup solutions, several points must be taken into account to ensure the solution is the right fit for an organization.

One key factor is WAN performance. This will determine how quickly data can be moved between a user’s PC or IT department servers to and from a provider’s servers. With today’s broadband services, backing up and retrieving a single file poses no problems. However, there might be an issue if an entire server is being restored. Even so, in many cases, the WAN impact can be minimized. For instance, when it comes to Exchange servers, organizations often need to retrieve only a relatively small-sized snapshot file to restore messages. (Remember, none of the attendees raise performance as an issue with SaaS services.)



Through an easy-to-use interface, users or administrators can quickly select files and folders of data to be restored.

A second factor is cost. Participants said they would hope a SaaS backup solution would cost less than internal solutions. Round-table participants noted that they are aware of total cost of ownership issues and would factor in the cost to support internal backup devices and solutions and the time to manage tapes when comparing solutions.

Several attendees believed SaaS backup would help them gain control over backup costs. Such a service

would, “allow us to charge back departments based on what they use,” said one manager. “It provides a level of cost prediction,” said another. “When I prepare a budget, I would have detailed costs in front of me,” said yet another manager.

And a third factor is security. This was the key concern of the round-table attendees. Specifically, the participants said there would need to be strong and easy-to-use encryption to protect the data in transit. The encryption would need to be transparent to the end-user, as well. The feeling was that any complication might dissuade users from using a service.

Additionally, attendees raised concerns about data being hosted on a solution provider’s servers. “[Human resource] and customer information would need to be very carefully monitored,” said one manager. “Protection levels and monitoring must be incorporated into SLAs.”

Many of the participants echoed that thought. The general opinion of the group was that an organization’s compliance group would have to visit the provider’s facility and work with the provider to demonstrate procedures and systems were in place to meet whatever regulations were of concern to the particular company.

That said, some felt that a SaaS backup service might help them meet compliance and eDiscovery requirements better. “It would probably make compliance simpler, since all the data is in one place,” said one manager.

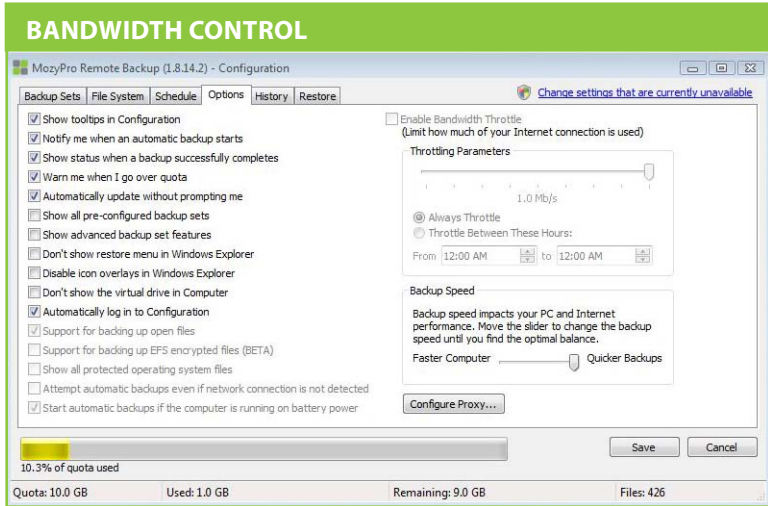
One additional point raised in the discussion related to SLAs. Managers said they would expect solution providers to offer SLAs on data retrieval times and other criteria.

Mozy as Your Technology Partner

To meet the growing demand for secure backup solutions, Mozy by Decho Corporation offers an easy-to-use, robust SaaS backup solution with MozyPro. The service can be used to support an individual, a small company, or the largest organization.

It uses client software, which, under an administrator’s control, is auto-installed on each device that is to be backed up. Backups are then managed via a Web-based administrative console. And users can easily restore files with the assistance of IT or on their own.

MozyPro meets the requirements cited by the round-table participants. For example, the solution offers 128-bit SSL encryption to secure data in transit. Data stored on Mozy™



Users can easily control how much bandwidth is dedicated to the backup process so other applications are not impacted.

servers is protected using 256-bit AES or 448-bit Blowfish encryption. And an organization can use Mozy's own private key or a key of its own to encrypt the data.

The service is designed to backup a wide range of systems, including desktops, laptops, and remote servers. To that point, the service is not designed for centralized data center backup.

MozyPro provides enhanced customer support, including 24 x 7 x 365 in-house phone and e-mail support, and e-mail notifications about end users' backup status.

MozyPro leverages super infrastructure expertise and extends it to a Web 2.0 architecture. The result is a highly available, reliable, and secure SaaS service that includes multi-tenant support, security and access management, billing, and metering.

MozyPro provides compelling customer value, including:

- Low monthly subscription rates
- No added capital expenditure for hardware
- Minimal administrative overhead
- Reduced per-gigabyte storage costs by virtue of deduplication technology
- Elimination of resource-intensive software deployments and costly, disruptive software upgrades.

As a result, MozyPro provides a TCO advantage of more than 30 percent over in-house PC backup solutions.

Given the increased demands on IT departments, the need to support a more mobile workforce, the value of data to corporations, and growing compliance requirements, MozyPro offers a cost-effective, easy-to-use, robust, and secure way to back up and protect corporate data. □

More information about MozyPro can be found at www.mozy.com/pro



Salvatore Salamone is an executive editor at Ziff Davis Enterprise. He is author of three business technology books and has been writing about information technology for 20 years. During that time he has been a senior editor at many major publications including *High Technology*, *Network World*, *Byte Magazine*, *Data Communications*, *LAN Times*, *Lightwave* (*The Journal of Fiber Optics*), and *InternetWeek*. He has also written articles for other industry magazines including *BCR*, *tele.com*, and MIT's *Technology Review*.

Mr. Salamone has been a frequent speaker at industry conferences and has helped organize and conduct industry roundtable discussions on a variety of topics. This included running panels and making presentations at numerous NetWorld+Interop, ComNet, CeBIT, and Comdex conferences. He also worked on, judged, and helped run "Best of Show" awards programs at these trade shows.