

On the Go: Protecting Corporate Data on Laptops, Mobile Desktops

– Christophe Bertrand of Veritas interviewed by Connie Chronis

Every year more than 1 million mobile desktops and laptops are stolen, damaged or destroyed. Data on desktops and mobile workstations contain valuable data, but lose that information, and it can result in the loss of hours - even weeks - of work and replacing it maybe impossible. What's a company to do? Christophe Bertrand, a senior product-marketing manager for client data protection at VERITAS Software, takes us through the steps of establishing a disaster recovery plan for laptops and mobile laptops.

Q: Why is so much data being lost from desktops and laptops?

A: As more business professionals utilize mobile workstations as their primary computers, more and more corporate information is being stored on those hard drives. According to Gartner, 60 to 80 percent of corporate data resides on PC hard drives. Laptops in the field are exposed to extreme environments from bouncing around on a plane to constant connectivity to the Internet. These keepers of corporate secrets are far more vulnerable to theft, natural disaster, hardware failure, Internet-borne viruses and human error. However, little attention is being paid to protecting these mobile workstations.

Q: What is the business cost for losing this data?

A: Besides the lost in productivity, time, hardware and possible customer opportuniues, the Computer Security Institute estimates companies spend tens of thousands of dollars to replace data after the loss of a laptop.

Q: What can a company do to protect its data?

A: Storage management plays a huge role in today's economy and there are many data protection solutions to choose from. For complete data protection, companies need to ensure that information is protected from the data center to the desktop and mobile laptop.

Q: Who is responsible for keeping this data protected?

A: Protecting corporate data was a straightforward job when all data resided on data center storage, which fell squarely into the realm of an operational support group. Today, however, with laptops, home and remote offices, mobile devices, distributed systems and corporate data centers, the lines of responsibility are far more blurred. Nowhere is that problem more acute than in the issue of backup and recovery. Where does IT's responsibility end? Does it include the PCs on all desktops, all laptops used in transit and all home offices as well? And how can IT manage that data when it's beyond the scope of central networks?

Q: But if a laptop is damaged or the hardware fails, can't the IT department just call a data protection company to restore the loss data?

A: Yes, you can always do that. But what if your laptop is stolen? There will be no data to replace if it has not been backed up on your company's server. Cost may be an issue. An average cost of sending hardware to a third party for data recovery costs about \$1,600. And this is not necessarily a proactive approach to protecting data in the first place. However, these services do wonders, but I would reserve them for last-resort scenarios.

Q: Why can't backing up a laptop just be a part of the regular server backup performed by the IT department?

A: Traditionally, corporate desktops and laptops have not been included in companies' data protection plans. The technology used for server backup is not necessarily the best or most efficient tool for backing up desktops and laptops, especially if those systems are remote or mobile. Unfortunately, this often translates to volumes of unprotected data, a huge risk factor for the user and the corporation.

Q: Aren't laptop backups part of the data protection solution companies implement for the overall company?

A: Although some organizations have implemented backup products that automatically backup desktops or synchronize desktop files that users leave on that are connected to the corporate network, this doesn't include those workstations that are out with the road warrior. So, those who are not on the corporate intranet - which includes remote offices, home offices and laptops - are left out of the overall company data protection solution. This strategy results in rapid growth of the back end repository without offering a complete disaster recovery solution.

Q: What are some good strategies for protecting desktops and laptops?

A: Keep in mind that your server backup solution will and probably should be different from your desktop and laptop strategy. Also remember that the typical desktop and laptop user will not be motivated to perform their own backups. To stay ahead of the constantly changing data on corporate PCs, look for a data protection solution that can be easily deployed by an IT department and offers minimal hassle to the user. Laptop users, especially, are often road warriors and will be opposed to any additional hassles that slow down their work on the road. A data protection solution should allow remote/mobile users to perform their normal tasks while a background runs transparently and quickly.

Q: What are the requirements for a distributed client backup/recovery solution?

A: Companies need a desktop and recovery solution that meets the following high-level goals:

- 1) Centralized management and protection of distributed data with minimal drain on IT staff and resources. Rapid recovery from a wide variety of failures
- 2) Flexibility to provide access to backups for mobile and distributed workstations and laptop users of all ability levels. This will allow users to perform restores on their own, as long as the solution is as automated and as easy as possible. It also must support both network and dial-up connections of varying quality.

Q: What must the solution be able to support?

A: Until recently, implementing an effective laptop and backup data protection strategy has been difficult - if not nearly impossible. The purpose of any backup solution is a fast recovery in case of problems. The solution must account for a wide range of possible scenarios, including:

- 1) Accidental loss, deletion or corruption of an individual file or set of files
- 2) System corruption because of improper software installation or a virus
- 3) Hard drive failure
- 4) The complete loss or destruction of the system.

The solution must be able to support everything from individual file recovery to “bare metal” restore to new hardware.

Q: What criteria should companies look for when they want to implement a software-based disaster recovery solution?

A: Companies should select software that is easy to deploy and easy to use, for both the IT administrator and the client. Scalability is also key, especially if your company is growing or the number of laptops is increasing. Disaster recovery should also be carefully evaluated. It is crucial that the disaster recovery features of the software can get a user back up and running with minimal loss of time and productivity.

For example, what if the administrator could rebuild a system exactly as it was last time it was backed up (including all the preferences and configurations) in a matter of a couple of hours? If you lose your laptop today on the East coast, and your home base is the West coast, you could get your new machine with all your data as of the last backup tomorrow via a next day delivery service. That’s disaster recovery!

Q: What other protection devices are out there? What can companies do to protect hardware from theft?

A: There are a number of other protection devices available to the road warrior. These include physical locks, encryption software and laptop insurance. Nothing replaces plain old common sense, however. Always keep your laptop case in sight when you go through the X-Ray machine at the airport, even if your loose

change makes the portal beep.

Q: Even if a company has a mobile data protection solution in place, does that automatically mean that a remote computer will be backed up?

A: A company must enact a data protection solution that will back up a remote workstation whenever the user dials-in. Recoveries must either be user-directed and/or managed, depending on whether the organization wants to use a Helpdesk infrastructure for simple file recoveries. A remote user cannot depend on a corporate MIS person to physically come out to their location and fix everything. MIS, always strapped for resources, requires a solution that can access remote users' machines and repair major problems, where required, from a major console.

Q: Any final tips?

A: People will keep experiencing small disasters with their desktops and laptops - machines will be stolen, desktops will fail, viruses will strike. The horror part of using mission-critical data can easily be fixed. There is light at the end of the tunnel - a hardware failure or a "forced" change of ownership does not mean it's the end of the user's data. Data protection technology has come along way to make it possible to reliably backup mobile data and recover it.
