

## Avoiding the Rising Consequences of Data Loss



By ROBERT F. GERACE  
PRESIDENT & CEO  
CRC, INC.

**F**INES? JAIL? A CAREFREE VACATION ON THE BEACH? MORE AND MORE, YOUR CHOICE DEPENDS ON WHETHER AND HOW YOU BACK UP ALL OF YOUR DATA, BOTH AT HEADQUARTERS, AND AT EVERY HOME AND REMOTE OFFICE. Certainly, if you're a GMA FORUM reader, chances are extremely high that you conscientiously conduct yourself in such a way as to not end up incarcerated. Yet in our experience, each day countless executives are, unknowingly, one step away from handcuffs. That one step is a data loss event.



*The people responsible for compliance in your organization certainly know that SOX requires your company to save electronic communications for at least five years, and Basel II requires banks to maintain three to seven years of history. You may want to pull them aside and ask, "Are we really in compliance, including every employee laptop and home office?"*

**THE RISK IS HIGH. WHY? IN A WORD — OR RATHER, AN ACRONYM, 'HIPAA.'** These five letters stand for "Health Insurance Portability and Accountability Act of 1996" (HIPAA, Title II). This act is serious business. Essentially, any company that handles medical records is in BIG trouble if its people lose them, disclose them unnecessarily, sell them, or are unable to produce them in the event they are ordered to do so through discovery or audit.

**THE CONSEQUENCES?** In addition to reduced stock value, lost sales revenue, lost customer confidence, and financial penalties, it is actually possible to end up being personally charged. [Source: *ESG Impact Report, Compliance, February 2006*]

Moreover, other new laws are coming on line quickly. For example: not disclosing a data loss event can end up costing some companies up to \$150,000. [Source: *Byte And Switch, December 2005*]. In February 2006, Morgan Stanley offered to pay \$15 million to resolve an investigation into its inability to retain email messages. The company admitted that its backup tapes had been overwritten. [Source: *Reuters/Computerworld, February 2006*]. And in *Zubulake vs. Warburg*, a gender-discrimination suit, the judge ruled it legitimate to presume that since Warburg lost backup tapes, it was unable to provide data and emails. Zubulake was awarded \$20 million, as the data loss was probably damaging to Warburg's case.

**HERE'S THE BIG PARADOX.** Most executives believe that they are well protected with multi-million-dollar data centers and a fully staffed data security team. And indeed they *are* protected — *at their corporate headquarters*. But what about your remote sites — remote and branch offices, work-from-home sales people and merchandising managers...all those laptops? The hard truth is that regulations like Basel II, HIPAA, and Sarbanes-

Oxley apply to the entire enterprise, and there are no exceptions made for the remote data mentioned above. Miss the boat on protecting *all* of your organization's data, and you could face violations and penalties, despite your otherwise-compliant organization.

Traditionally, remote offices have been backed up to tape. Only the largest organizations have the resources to have trained technical staff to implement and watch over the backup process — which is very dangerous, because tape backups tend to be extremely unreliable. Often times, the most junior member of the remote-or-branch office is assigned 'tape duty' to change out the tape every night and take the tape home.

Frequently the tapes are not changed, or are left on a dashboard in the heat or cold. Further, tape backup jobs fail regularly. Jammed or broken tape, tape read or write errors, jobs that run so long that they prevent the next cycle from running, and many other problems cause jobs to fail. And with no way to monitor the information about failed jobs and/or tapes that were not changed, the remote office is only one disaster away from a data loss event.

**LAPTOPS ARE EVEN WORSE.** Many times, the idea is that when a mobile worker is in the office, s/he is supposed to copy important files to a shared directory on a server. Sometimes it happens; sometimes it doesn't. Many organizations have no reliable method to even back up laptops and home offices — let alone any way to monitor whether it happened or not.

Even the servers in many large organizations are still vulnerable to tape problems. Even with adequate staff and the best tape equipment on the market, many tape backup solutions have not pro-

gressed to the current industry standards of *continuous data protection* and *message level restore*. (Both explained below.)

To summarize all of the above, however, it is fair to say that **almost every organization is currently exposed to some level of risk, and that risk can cause penalties that run from fines payable by the company to jail time for its executives.**

Those responsible for compliance in your organization certainly know that SOX requires companies to save electronic communications for at least five years, and Basel II requires banks to maintain three to seven years of history. You may want to pull them aside and ask, “*Are we really in compliance, including every laptop and home office?*” While most often the answer is, ‘No’, fortunately, there is a comprehensive solution.

Starting with a foundation of *disk-to-disk backup* (D2D), where all information is **stored on a secure vault**, all of the problems above can be solved.

Building on that foundation, we begin with *continuous data protection* (CDP). CDP provides the ability to **constantly back up changes to servers**. The moment a file is saved, it is copied to a local device and, immediately after, to an off-site device.

*Message level restore* (MLR) is the **ability to restore individual email messages**. This ability is a significant development; prior to MLR, administrators were faced with an all-or-nothing restore of an entire mailbox from some number of hours ago. Today’s state-of-the-art technology allows an executive to delete a message, and restore *only* that message one minute later — with or without the help of IT staff — by a simple point and click.

**HERE’S ONE PLAN OF ACTION:** Start with your **internal data centers**. If not implementing CDP and MLR, start immediately. Next, ensure that data is sent offsite. While some regulations specify at least 300 miles away, many companies feel safer with data that is at least 1,000 miles away from its source.

Be sure, however, that whatever solution you deploy also allows a “*local restore*” capability, as most data-loss events are caused by humans deleting and overwriting files — or servers crashing.

None of the above will likely cause a complete restore from a remote site; so having several generations of local copies will ensure quick restores and minimal loss of business.

Next, be sure that the technology you use to get data off site uses “*delta-blocking*” technology. Such technology sends only the parts of files that change, and re-constructs files at the alternate location. This technology will ensure the lowest use of bandwidth (*i.e.*, expense) to move data off-site, and will ensure fast restores of small to moderate amounts of data. (For large amounts you can always fly data in from the remote site.)

**NOW THAT WE ARE SURE THAT YOUR DATA CENTERS ARE UP TO DATE, LET’S TACKLE THE ACHILLES HEEL** — the remote, branch, and home offices — along with all those laptops.

■ Let’s start with the **remote and branch offices**. What you need here is an automated agent (preferably only one agent for the entire set of computers) that implements both CDP and MLR as well as delta blocking.

Combine that with an automated solution to securely determine what changes, encrypt it using the industry’s strongest encryption (AES 256), and send the changes off site as they happen.

Insist that the agent software sends email notifications upon successful and unsuccessful backups, and also provides tools for your network administrative staff to monitor all locations from one point.

Finally, have your network administrators (or your data protection company) consult with each remote office at least once monthly to ensure that they have not made changes in the way that they store their data (*i.e.*, installed new or upgraded programs), and coach the offices to inform IT of any proposed changes.

This problem is now solved.

■ Next, let’s talk about **home offices and laptops**. Most companies would be shocked to know how much of their data is on a PC that someone’s children play on. Much data, intellectual property, and creative work belonging to the company is distributed on these PC’s, and the company has no way to obtain this information in the event





## FORUM OPINION / Data Loss

---

*Most companies would be shocked to know how much of their data resides on an employee PC that children use.*

one of those PCs crashes — or junior spills sticky juice on the keyboard of a laptop.

Thankfully, this problem too is easy to solve. An agent can be installed on each home computer and/or laptop, and data belonging to the company can be selected for backup. Any time the home office computer or laptop is connected to the Internet (even via a dial-up connection) all of the latest changes to the data are backed up to a vault automatically.

IT administrators can also monitor this process, and contact employees who have not backed up in some specified time period to back up their computers.

ONCE ALL OF THE ABOVE IS IMPLEMENTED, COMPLIANCE BECOMES EASY. Data becomes **easily recoverable** — not only is there an extremely high probability that you *have* it (certainly, it rises to the level of a “business reasonable effort”), but you will also be **able to recover it fast enough to satisfy regulators and auditors** (small amounts can be recovered instantly, and huge amounts can be recovered as fast as a jet can fly).

Further, assuming you have selected the right partner for the software, you have **controllable disposition of data** — whereby you can certify destruction of all copies of data that you are required to destroy.

NOW, YOU MAY BE WONDERING HOW THE COST OF D2D COMPARES TO TAPE. The answer is that it depends on your partner or provider of your software or service. Higher-end systems allow a set of decreasing costs for data that ages. While yesterday's data may be business-critical, certainly last year's data becomes critical only in the event of discovery or audit.

For that reason, you may rightly assume that you have no need to pay for instant disk-recoverability of last year's data.

In fact, some compliance standards mandate a 30-year retention of data. CDs and DVDs would be the only way to economically store data that old.

Higher-end companies recognize these facts, and don't force you to pay top dollar for any data other than that which you consider to be business-critical. As data ages, it can be moved to progressively “slower to obtain” methods of backup, with each step progressively less expensive.

High-end software that de-duplicates (does not store more than three copies of any one file on the vault) further reduces costs.

When managed in these ways, the D2D option works out to about the same cost as tape — adding invaluable functionality with none of the liabilities.

D2D WITH OFFSITE VAULTING IS HERE, AND IS NOW A PROVEN BUSINESS SYSTEM. Enterprise-sized companies with greater than 10 terabytes (10 trillion bytes) of de-duplicated, compressed and business-critical data will most cost-effectively purchase and host their own solution.

For those with less, it may be more cost effective to hire a service provider, and pay a monthly fee ranging from hundreds to thousands per month for the service.

Whichever way you decide to go, you will be able to rest easily, knowing you have taken the proper and prudent steps to secure your data. ■