



# LOCK DOWN

## YOUR COMPANY'S PHYSICAL SECURITY

Ensuring proper storage, handling and disposal of data media

BY DAN BAYHA

**W**ith so much to keep up with in realm of virtual security, it's not surprising that, for many IT professionals, the low-tech concept of *physical* data security is not exactly top of mind. Yet strong firewalls and passwords, while essential, are not the complete answer, because, more and more, security of electronic data is simply not limited to the "virtual" world.

Changes in technology, government regulations, and legal practices (electronic data discovery) demand changes in the physical handling practices of your data storage assets. There are many statistics on these topics, principles and best practices to improve these processes at your organization, plus guidelines recommended by experts in the field of security.

### QUICK, HOW MANY COMPUTERS ARE IN STORAGE AT YOUR COMPANY?

What about the number of defective hard drives and backup tapes tucked away in boxes and back rooms? Do you have even ballpark figures? Or know who's charged with getting rid of the systems? And if recycled, where did they end up? If not, you are hardly alone. Consider these statistics: in 2006, the National Association for Information Destruction (NAID) discovered that 12% of organizations surveyed were storing obsolete machines indefinitely. Worse still, they discovered that 53% of primary decision-makers in the U.S. had no idea what happened to obsolete or discarded equipment.

### THE RISKS

Data storage technology is pervasive. Hard drives can be found in office copiers and printers. Portable thumb drives and jump drives are worn around employee's necks as if they

were jewelry. Storage capacity for single small devices is reaching mind-numbing proportions. Seagate and Hitachi both offer terabyte (1 trillion bytes) capacity hard drives.

Four years ago, forensic data recovery was a niche business specializing in the recovery of lost data due to hard drive failure. Today it's a billion-dollar industry supporting the legal community's electronic data discovery efforts. Forensic data recovery has become an important law enforcement and national security tool. In the words of Rick Fuentes, NJ State Police Superintendent "Do not assume you can sufficiently erase digital evidence... Those pieces of evidence can be reassembled."

The message is clear that the amount of stored data is proliferating, and the tools available to recover lost or intentionally deleted data are readily accessible to entities that may not have your best interests in mind.

### HOW REAL ARE THE RISKS? A CAUTIONARY TALE OR TWO...

Communications giant Alcatel-Lucent is still reeling from the May 2007 loss of a single CD containing confidential information, including Social Security numbers of about 200,000 current and past employees. The Secret Service is now involved, trying to end this public-relations nightmare.

IBM had a similar snafu earlier in the spring of 2007, and had to take the embarrassing step of running ads in the local paper to recover lost backup tapes.

In early June 2007, the police department for Ewing Township in New Jersey reported a data exposure resulting from PCs they sold for a few dollars. A local gadfly purchased the machine and, using freeware data recovery software, recovered confidential crime-fighting strategies, police retri-

mands and all sorts of internal memos. This information was then posted on the Internet.

Think about the unique mixture of corporate and personal data likely to be found on many of your co-workers machines (and your own), not to mention laptops and PDAs.

### **THE TAKEAWAY FROM THESE BLUNDERS**

While some corporations and law firms have caught on to the idea that physical data security is equally important as (or possibly more important than) virtual security, many more will pay sharp attention now that Alcatel, IBM and others had to go public with their mistakes. And as shown by the Ewing police example, not only is the secure handling and transportation of physical data media critically important, but also *disposing* of them properly and thoroughly is crucial.

Sonja Robinson, Director, Forensic Lab Management at FTI Consulting, comments on the potential repercussions of mishandling company data: "The degree of damage depends on the company's industry. At the very least, if it is made

public that there's a data loss, public relations and stock prices may suffer. Reputation is critical in today's markets."

Bob Johnson, Executive Director of NAID, believes that higher-level decision makers need to be involved in these matters, not just people at the operations level. "The higher in the organization that this comes up, the more they'll have a full appreciation of the importance of these matters. Decision makers may not know what's being done with the computers and storage media, but they will know they have to get to the bottom of it."

Three suggested improvements to controlling your data storage assets:

**1. Keep track of all of your data storage assets in one place.** Data storage devices should be identified as soon as they are purchased. A database containing the device description, manufacturer, model and serial number should be generated. Identify the physical location and the person responsible for that device. Confirmation of the location of the device needs to be periodically performed. In the case of portable devices, confirmation of location should be done more frequently. The

---

**... not only is the secure handling and transport of physical data media critically important, but also DISPOSING OF THEM PROPERLY and thoroughly is crucial.**

---



confirmation should be in writing and verified by another company employee other than the responsible party. Notify all employees responsible for mobile data storage devices that the devices are subject to random audits. The device can be recalled at any time for examination of the hard drives for approved (and unapproved) software and stored data.

Upon the need for disposal, the devices should be sent to a centralized collection and inventory control location. The “to be disposed of” data storage assets should be checked against the inventory database. This control process allows you to place a security perimeter around all of your physical data storage assets. If an item enters your organization, you will track it while it’s within your organization and control its only legitimate exit.

**2. Centralize the control of your physical data storage devices.** The propagation of data storage devices has led most organizations to a de facto decentralization of control. The urgency of efficient physical data destruction rapidly dissipates as this control is delegated. For instance, an off-site data destruction provider will often ship secure containers to

## Transportation of physical data storage assets roughly is crucial.

their clients’ remote offices to transport items to be destroyed. It should not be the destruction provider’s responsibility to follow up on the return of the container; the organization’s centrally accountable party should make the destruction project a high priority. Centralizing the physical control promotes responsibility and consistency of process, which leads to a third point.

**3. Make your data storage control system a continuing process rather than a group of disjointed projects.** The physical handling of your data storage devices is an important part of your overall data retention policy. Your organization’s legal protection under the Federal Rules of Civil Procedure 37(f), - “safe harbor” data destruction provisions – depends on your procedures being a disciplined, repeatable and auditable process.

### WHAT ABOUT CONTROLLING MY DATA STORAGE ASSETS IN TRANSPORT?

In the case of the lost Alcatel-Lucent CD described above, this confidential information was lost not at the office, but instead went missing while being transported (by a leading delivery company) somewhere between the offices of two of the company’s vendors. So clearly, it’s not just physical security within your organization you need to worry about.

You also may need to assess a judgment about the security of affiliates, vendors and their employees.

Here are some ways to better ensure your data will arrive where it’s supposed to:

- Weigh the consequences of a transport failure. Given the losses discussed in this article, shipment of certain high-risk data storage devices may require extra control and protection.
- Choose a carrier that offers a range of shipping options. For ultimate security, select armored transportation. Armored transportation can offer a legal chain of custody for true auditability.
- Secure shipping containers with locks and security seals are always a good packaging option.

Steve Ferguson, Director of Global Sales and Marketing for Dunbar Global Logistics states: “I think that the express companies do an excellent job of moving parcels in an expedited manner, but they are not meant to be used as totally secured transportation provider. We do extensive background checks on all employees, insure that personnel have current photo id’s, maintain dual custody of parcels while in our possession, at each transfer point we “get a signature and give a signature”, and maintain ‘line of sight’ supervision. The common carrier or express company isn’t set up to provide that type of service.”

### SECURE DATA STORAGE ASSET DISPOSAL

Disposing of data storage devices and media is a fact of life. Defective products and technology upgrades generate a constant stream of “to be disposed of” items that require stored data to be destroyed. Whether you destroy the data in-house or not, you will still need to dispose of the item and that means it will leave your security perimeter.

Have you adequately destroyed all stored data? What additional (redundant) precautions can you take to assure absolute data destruction?

### IS SOFTWARE-BASED DATA ERASURE ADEQUATE?

Defective hard drives are a particular problem. Software erasure tools are not 100% effective. Forensics expert Robinson cautions: “These drives are often piled up on an IT person’s desk and are low priority items – people don’t get around to dealing with them due to other projects and daily emergencies. But if a drive walks out, it has just as much potentially damaging data as a working hard drive.” Worst of all defective hard drives may contain historic data that should have been deleted. Recovering this type of data is a particularly valuable find for forensic data recovery experts involved with litigation data discovery.

Another drawback of software erasure is that it takes an inordinate amount of time. Imagine how long it will take with the arrival of terabyte hard drives. No one likes spending hours of time on a mundane task that yields questionable results.

## GREEN, COST-SAVING AND ACCOUNTABLE — PHYSICAL DATA DESTRUCTION

To know for sure that data can never be exposed outside your organization, the only 100% effective choice is to physically destroy the hard drive and data media by shredding and then melting the fragments. This applies to hard drives (obsolete and defective), backup tapes, obsolete PDAs, cell phones, CDs and other data media.

Secure physical destruction requires large specialized equipment. This type of service will require the shipment of your “to be destroyed” data storage devices to a remote facility. Vendor due diligence is a critical component of the data destruction process. Visiting the destruction facility may not be practical. Fortunately NAID offers a highly respected secure data destruction certification program, which helps companies to find qualified providers.

You will want to seek a company which offers your organization an absolute, permanent, and auditable data destruction process that can take care of the entire disposal process, from collection of retired equipment, to secure shipping, to shredding into unrecognizable fragments, to the final step where fragments are smelted into source metals and plastics.

Some features to look for in finding a data destruction provider:

- NAID certified secure data destruction facility (AAA certification is the highest)
- Secure transportation options including locked containers for clients to keep onsite for storing obsolete equipment, plus options for courier and armored shipment of materials for disposal.
- Proof of absolute physical destruction which is assured by applying redundant destruction procedures (drives should be shredded and melted; tapes should be shredded and degaussed). Physical destruction is a permanent solution to the challenges of destroying ever-changing data storage technology.
- Auditable records including the tracking of individual serial number devices from your facility through the entire destruction process. These records can include Excel spread sheets, digital photographs and other methods. For an additional fee, the vendor may offer access to an online compliance library which is available 24/7/365 over the internet (password-protected).
- A structured process of collection, shipping and destruction which is tailored to the ever-changing and increasingly demanding task of destroying defective and obsolete data storage devices.
- A “green” environmentally-responsible disposal solution. Hard drives are 70% aluminum. The melting process is actu-

ally the recycling of the shredded particles for aluminum recapture. Look for a facility registered with the Federal EPA and their native state’s Department of Environmental Protection. Request that EPA compliance documentation be shown as part of the disposal process.

## TIPS ON RECYCLING YOUR COMPUTER EQUIPMENT

The foregoing discussion may have prompted you to think about what to do with the old machines when you’re going through the regular process of upgrading to new ones. As NAID’s leader Johnson says, “People simply don’t know what to do with the old machines. Computers are becoming obsolete after 2 years now – they are ‘in and out’ faster.”

To avoid mistakes like those made by the Ewing police department, don’t give old machines away at a discount to those who will take them off your hands or dump obsolete computers along with the regular trash. Find a local company which accepts computers, fax machines and printers as recyclables. Hard drives should be removed and shredded so there is no further chance for data exposure. No reusable computer should ever leave that facility with its original hard drive in place.

## CONCLUSION

Hopefully this article has given you a lot to think about when it comes to the increasing importance of physical data security. Although so far there is currently no federal regulation on the processes we have outlined here, NAID’s Johnson says that several data protection bills are circulating in Washington, so look for national legislation to come to fruition in the next two years or sooner to address information management and destruction.

In the meantime, act now at your organization to better secure your assets and reputation, especially if you now think physical data security is being perilously ignored or mishandled. As Dunbar’s Ferguson says, “Start by contacting the director of security of your firm. If you still meet resistance, all they need to do is look at any given day’s news. There seem to be stories almost daily of companies’ data that has been compromised. The cost of proper data handling is very small in relation to the cost of a problem.” We couldn’t have said it better ourselves. ■■

**Daniel F. Bayha** is VP and CFO of Back Thru The Future, a secure data destruction and electronics recycling company based in Ogdensburg, New Jersey. For more information, visit [www.backthruthefuture.com](http://www.backthruthefuture.com). Bayha can be reached at [dan@recyclepcs.com](mailto:dan@recyclepcs.com).