



## **Dispose of High Tech Gear Properly** **By Robert Houghton**

Not that long ago, equipment disposal from the data center was easy—just ask for bids. Buyers would write a check and make the obsolete stuff disappear. That was before it became a federal case for electronics to end up in a landfill, and before privacy regulations made a data breach worth millions in fines and remediation costs. Mostly because of compliance risks, good equipment disposal practices have become a strategic part of infrastructure management. The little known bonus is that IT asset disposition best practices can also provide new ways to realize a material financial upside.

First, do no harm. Electronic scrap is regulated in most developed countries as hazardous waste, and it must be responsibly managed. Items without value as operating units or parts must be recycled back to constituent materials, but in the United States less than 20 percent of corporate equipment is actually recycled. Most of the balance is exported to developing countries where materials recovery is a manual, usually hazardous, process that ends up polluting the local environment. Though perfectly legal under U.S. law, exporting e-waste is unacceptable for a growing number of companies seeking to be responsible global citizens. Rather than a “certificate of destruction,” which is usually a meaningless if not fraudulent document, companies must require auditable proof of the kinds and quantities of materials recovered from their e-waste and to whom those materials were marketed. And, recycler operations and records must be audited—not just once at the beginning of the relationship but routinely and in detail.

Certifiably destroying all data on servers and storage devices is a difficult and failure-prone process, and data centers sometimes rely on procedures that simply do not work. Formatting drives destroys the file system but leaves data easily recoverable. Degaussing with a magnetic field often fails to completely destroy data. And, physical destruction by hammering, drilling or other violent behavior, may disable the drive mechanism but does little to actually destroy the data resident on hard drive platters. What does work is: 1) overwriting every sector of every drive with a pattern of obliterating data, 2) verifying the success of that process, then 3) producing an audit trail that proves the successful sanitization of each hard drive by HDD serial number. A limited number of sanitization utilities exist that are compatible with all the common drive types in a typical data center environment, so comprehensive testing before putting a data erasure application into production is important. Inoperative hard drives must be physically destroyed, and shredding is the best method. The final step is to archive the verification and audit data; in the event of a suspected breach, the real value of a good process is its ability to prove the outcome of that process when it matters. A note for companies that lease their equipment: the lessor is responsible for proper disposal under environmental regulations, but the lessee remains responsible under privacy laws for data destruction.

To optimize the returns from the disposition process, resale of the equipment should be considered the tail on the dog, not the main act. In order to capture fair market value, it is particularly important to have accurate and detailed information about each item, including

its configuration and operating/cosmetic condition. Large servers and storage devices may be worth more if they are de-installed by the OEM and certified for maintenance, but not always... check in advance. Trade-in programs are sometimes very good deals, but often are a means for the OEM to play a shell game with margin. Always check the fair market value of equipment before agreeing to any trade-in offer. And, some older equipment may be worth more at the component level than as an operating unit, so disassembly should be considered.

Years ago, data center equipment retained its value much longer than its distributed cousins. Now equipment values can be expected to fall 80 percent to 90 percent three years after installation. Companies attempting their own remarketing must stipulate in the sales contract that the equipment is sold "as-is, where-is", and that the buyer is responsible for proper recycling of all scrap materials. Under federal law, liability for improper disposal is joint and several, meaning that the seller stays on the hook for responsible management of e-waste.

The data generated by a good disposition practice, properly used, is at least half the value of the program. The granular detail from the data destruction and e-waste recycling processes is essential to managing compliance risk. Corporate finance must update fixed asset records for compliance with Sarbanes Oxley and to ensure that property tax assessments are ended. IT must remove equipment from any contracted maintenance program. Asset management may be able to repurpose software licenses and must update asset repositories to reflect the end of both the hardware and data lifecycles. Because the potential value of reuse can be significant, equipment should always be evaluated for possible redeployment elsewhere in the enterprise, and inventory data should be made widely available to stakeholders in IT. Because of the sheer volume of data involved, leveraging its full value requires as much automation as possible; integration of the asset disposition data streams into all relevant systems is important to driving costs down.

Rigorous management of the asset disposition process can be challenging and is always expensive. Outsourcing the entire retirement process to a specialist service provider can significantly reduce both costs and risks, and it provides companies a means of transferring some of the attendant liabilities to the vendor. When selecting an outsource vendor, companies should evaluate the service provider's financial strength and insurance coverage, technical capabilities and operational maturity. Because failure of critical procedures such as data destruction can be catastrophically expensive, reviewing the vendor's operational procedures in detail and evaluating their quality controls is essential. Performing audits of their operation to verify conformance with procedural standards is an essential part of due diligence.

*Robert Houghton is president of Redemtech, [www.redemtech.com](http://www.redemtech.com).*