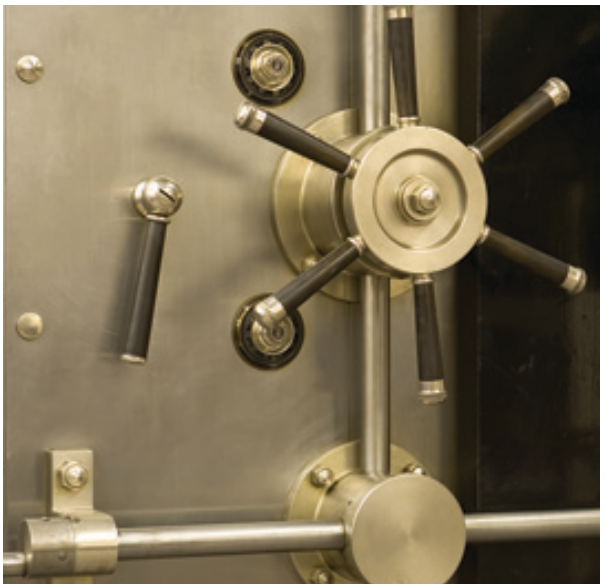
Plugging data leaks

hp

Data erasure and equipment disposal service from HP prevents those old bits from biting back.



In the past, it may have been prudent for companies to safeguard certain data that resides on a hard drive, but now it's the law.

A myriad of strict local, state and federal legislation introduced to protect investors, consumers and the environment means that organizations must be extremely careful, particularly when it comes to disposing of IT equipment that has outlived its usefulness.

As an example, federal laws include the Health Insurance Portability and Accountability Act (HIPAA), which sets out goals on keeping personal information secure in the health industry. If you find yourself in non-compliance to HIPAA data security practices, you may be exposed to a maximum fine of $250,000 and/or a maximum of 10 years imprisonment. There is also the Gramm-Leach-Bliley Act, which establishes financial institution standards for safeguarding customer information, Sarbanes-Oxley, and the Resource Conservation and Recovery Act (RCRA), designed to ensure hazardous waste is managed properly.

They may exist and they may have teeth, but a survey of senior executives commissioned by HP Financial Services

hp invent

(HPFS) and released in September 2005 concludes that 70 percent of respondents underestimate the cost of disposing PCs and an alarming 66 percent of executives with purchasing authority are unaware of the financial implications of ignoring environmental regulations when disposing of IT equipment.

The results come at a time when the International Association of Electronics Recyclers is predicting as many as one billion computers will become potential scrap by 2010. The National Safety Council, meanwhile, estimates there are 150 million old and abandoned PCs sitting in warehouses, storerooms and closets across the country.

In order to properly dispose of this equipment, the data ultimately needs to be wiped off the drive and the equipment must be disposed of in a way that will not cause environmental damage. The most common data destruction methodology is the Department of Defense or DOD standard, which provides three government approved techniques for sanitizing magnetic media. There are several ways to erase information. Which method you choose will ultimately come down to the sensitivity of the data that resides on your hard drives and the level of cost or effort you want to incur to properly destroy that data.

Once those decisions are made, organizations have to figure out how best to physically dispose of the equipment. Choosing a vendor carefully is imperative, as organizations may incur legal liabilities for a vendor's inappropriate practices. So before selecting a vendor investigate its knowledge of the law and its capability to operate therein as ultimately the most expensive component of equipment disposal for all parties can be the cost for failure to dispose of it and the data residing on the drives appropriately.

Jim O'Grady, who oversees HPFS' Asset Recovery business, says that the one thing companies often overlook is the content that resides on servers. "When they think about data security, they almost always think about PCs and laptops and totally disregard servers," he says. "This is extremely important and customers need to understand their vendor's capabilities for wiping those drives."

O'Grady recommends that organizations implement a program that goes well beyond just securing data on the hard drive. "Determining the right disposition strategy for end-of-use assets can be a very complex thing for companies to figure out, which is why old equipment ends up sitting in a warehouse," he says. "It's a big problem that many organizations are facing, and one that is going to get bigger as a result of all of the recent legislation."

HP offers a fee based asset recovery service designed to help take the confusion and fear out of the entire removal process. The service — that occurs either on the customer's premises; in a 165,000-square-foot HP facility in Andover, Mass.; or through any one of nine HP partners — includes data erasure and removal of all identifying information such as labels and tags. If customer data is particularly sensitive, hardware will be placed in special secure containers and transported by truck to an HP facility.

Once the drives have been erased, an electronic certificate of destruction is issued that contains the data wipe method used and the date of the procedure. "It provides organizations with the proof and peace of mind that information was removed securely," says O'Grady. "At the end of the day you need to find a reputable, trustworthy vendor. That is clearly the best way of protecting yourself."

To download a complimentary HP white paper "Mitigating Your Data Security Risk," visit: www.hp.com/go/transform

To view a web presentation about proper asset disposal, visit www.hp.com/go/transform21 and select "Hardware Disposal and Risk Management."

This article first appeared in the January 2006 edition of HP's Transforming Your Enterprise publication. The current edition of this publication is available at: www.hp.com/go/transform