



Hard drive disposal – The overlooked confidentiality exposure

Contents

- 2 Abstract**
- 2 Background**
- 3 Computer recycling**
- 4 Continued use of recycled IT assets**
- 4 Choosing the right technology**
- 5 Measuring the financial impact**
- 6 Cost and risk reduced**
- 6 Outsourcing hard drive sanitisation**
- 7 Value recovery: taking the next step**
- 7 Conclusion**
- 8 For more information**

Abstract

In every industry, IT managers face increasing pressure to assure the confidentiality of corporate, client or patient data. In addition, companies and managers in certain specific industries must comply with local country laws requiring strict standards for handling, distributing and using confidential client, corporate or patient information.

While there are methods and products to aid in data storage and transmission security as the data moves through the system, assuring confidentiality of data on desktop or notebook computers when they leave the premises to be disposed of presents a different set of challenges and exposures. In this brief paper, we lay out some of those challenges and attempt to demonstrate the value of third-party disposal.

Background

Data confidentiality has always been an issue of ethical concern. But with the recent enactment of laws to protect the privacy of individuals' health and financial records, it has become a legal concern as well.

Most IT managers have some kind of strategy in place for securing customer information within their networks and, especially in the healthcare industry, controlling data interchange with vendors to assure patient privacy. The market offers various products and services to assist managers with these challenges. Many offer ways to integrate confidentiality and compliance into daily operations. But there always comes a day when a given desktop or notebook computer is retired, and that's when an IT manager can lose control over protecting the confidentiality of that data. Provisions and controls need to be established to ensure that the data on those (retired) hard drives cannot be made available to others.

Highlights

With greater value recovery, asset liquidation becomes increasingly attractive.

Computer recycling

More and more computers are coming offline every day, and more are being recycled than ever before – in fact, more are being recycled than most people expected.

According to a Carnegie-Mellon study, it was predicted in 1991 that 150 million computers would be sent to landfills by 2005. However, the growth of the computer recycling industry since then has changed that number in a very significant way. The new prediction is that, by 2005, 150 million computers will be *recycled* (versus being sent to the landfill). Thus, these systems are not being scrapped as was originally predicted, but are continuing to function in the IT environment.

Already, it appears that this projection will be exceeded. According to Gartner Dataquest, about 150 million used hard drives were sold via secondary sales markets last year. At the same time, roughly 200 million new hard drives were shipped. That means that for every ten new hard drives that enter the market, seven used ones are resold.

There are a number of reasons for this market activity. The economic environment characterised by low interest rates has created incentive to finance new equipment. Meanwhile, PC technology has advanced to a point at which older machines continue to command reasonable prices. With greater value recovery, asset liquidation becomes increasingly attractive.

The only way, other than destruction and scrap, to prevent this kind of inadvertent file sharing is to sanitise the hard drive before it reaches the next owner.

Continued use of recycled IT assets

Many small businesses and individuals liquidating their computers or returning them at end of lease do so with little thought as to the data contained on the hard drive. They simply delete their files before giving up their machines. Users reformat their hard drives, sometimes believing, incorrectly, that data is destroyed in the process. They have three reasons for believing this to be the case – first is the somewhat frightening screen in Windows and DOS warning that ‘ALL DATA ON DRIVE C: WILL BE LOST.’

The second reason for believing that reformatting actually deletes data is that reformatting audibly exercises the hard drive mechanism and takes a long time. And third is semantics – the word ‘format’ implies that some kind of new grid is being constructed, as if the hard drive were a farm and we were magnetically re-plowing the fields into new rows.

But the DOS warning really only tells us that we can’t get the data back with the tools at hand. The thrashing during format is a comprehensive scan for bad sectors. And formatting is really just writing a new root directory, FAT table, boot blocks and a few test sectors.

Choosing the right technology

The only way, other than destruction and scrap, to prevent this kind of inadvertent file sharing is to sanitise the hard drive before it reaches its next owner. There are two ways to do this.

One is to ‘erase’ the hard drive with the kind of bulk eraser, or degausser, used for magnetic tape. The problem is, the degaussing field is strong enough to physically ruin the hard drive. This is, therefore, the same thing as destruction, and may be a good choice if the next destination is the smelter or a landfill.

As local country laws continue to pass and enforce regulations for electronic data security in various industries, IT managers must act quickly to adopt and implement appropriate hard drive sanitation practices.

The other solution is to perform ‘data overwrite.’ One type of data overwrite is to write zeroes to every block on the hard drive, or fill the hard drive with random patterns. While this would prevent earlier data from being read by the operating system, specialised equipment can read the original data.

Other types of data overwrite have been developed, many based on the so-called ‘Gutmann patterns’ of overwrite data developed by Peter Gutmann of the University of Auckland. In fact, Gutmann patterns are generally featured as elements of commercial sanitising programs. These programs, most priced somewhere between \$50 for individual licenses and about \$500 to \$2,000 for professional versions, are capable of providing reasonable assurance that data will be unrecoverable under most conditions.

Measuring the financial impact

There are two critical factors that all companies need to consider when making a decision about hard drive sanitisation practices – cost and risk.

The cost of running sanitisation programmes on a fleet of computers can be prohibitive. Even in smaller organisations, the number of hard drives that need to be cleansed can be unmanageable. Most IT managers do not have the hours or staff to accomplish such a task without impacting other core business responsibilities. Should a company choose to circumvent these costs and simply destroy their hard drives (many of which could be reused), they dispose of equipment that still has market value.

At the same time, companies need to recognise the significant risk associated with breaches of private information. When companies don’t properly sanitise exiting storage devices, they expose themselves to myriad public relations, legal and business repercussions should any confidential data be leaked. IT managers must act quickly to adopt and implement appropriate hard drive sanitisation practices.

It may well be that the most convenient option for disposing of computing equipment is to turn it over to a reliable third-party asset disposal vendor.

Cost and risk reduced

It may well be that the most convenient option for disposing of computing equipment is to turn it over to a reliable third-party asset-disposition vendor. With privacy laws and data-recovery technology in a constant state of development, demonstrable compliance may ultimately be built on diligence in the selection and application of tools and vendors.

All together, there are two main factors to consider:

- *The need for documented diligence in the effort*
- *The need to be confident that computers you no longer need do not become liabilities because of un-sanitised or improperly sanitised hard drives.*

What a company does today may be scrutinised tomorrow – which means long-term viability is important to consider. To summarise, your choice of third party for hard drive sanitisation should be based on confidence in that vendor's technical capabilities, integrity as an organisation and staying power over the long haul.

Outsourcing hard drive sanitisation

The question of how to balance cost and risk has many organisations looking for outside help. For a growing number of companies, the answer is to outsource their entire sanitisation and asset disposition process. Using a third-party vendor helps them achieve three major goals – appropriate sanitisation of exiting hard drives, avoidance of cost/mitigation of risk associated with in-house sanitisation and disposal, and extraction of residual value from hard drives with useful lives.

Many companies have found that using a single vendor for the entire disposal cycle is convenient and highly cost effective.

IBM Global Financing's Asset Recovery Solutions offers customers hard drive sanitisation and cleansing services to ensure the appropriate overwrite of company data. Depending on the residual value of the equipment, we also provide remarketing services for a customer's used equipment.

Asset Recovery Solutions disposes of assets without market value in accordance with local country laws, and also issues a Certificate of Destruction that lists all machines processed and certifies that they have been destroyed. And last, but not least, Asset Recovery Solutions frees up valuable space by removing obsolete technology from a customer's inventory.

Value recovery – taking the next step

Hard drive sanitisation is a significant and important process. But it is just the beginning of the asset disposal challenge. Your obsolete hardware still needs to be inventoried, stored and sold, or destroyed. Many companies have found that using a single vendor for the entire disposal cycle from hard drive sanitisation to final resale or ISO 14001 certified destruction is convenient and highly cost-effective. In some cases, companies can simply trade their hardware (and the headaches of disposal) for a check for fair market value (FMV) less management fees.

Conclusion

The law is providing ever stricter standards of customer data confidentiality, with health and financial services industries on the leading edge of compliance requirements. There is no way to predict what data recovery tools will be widely available in the future, nor the exact nature of future laws. It is certain, however, that companies will be held accountable for protecting confidential data by shareholders, customers, employees and the press.



IBM United Kingdom Limited

1 New Square
Bedfont Lakes
Feltham
Middlesex
TW14 8HB
United Kingdom

The IBM home page can be found at **ibm.com**

IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks, or service marks of others.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program or service is not intended to imply that only IBM products, programs or services may be used. Any functionally equivalent product, program or service may be used instead.

IBM hardware products are manufactured from new parts, or new and used parts. In some cases, the hardware product may not be new and may have been previously installed. Regardless, IBM warranty terms apply.

This publication is for general guidance only. Information is subject to change without notice. Please contact your local IBM sales office or reseller for latest information on IBM products and services.

IBM does not provide legal, accounting or audit advice or represent or warrant that its products or services ensure compliance with laws. Clients are responsible for compliance with applicable securities laws and regulations, including national laws and regulations.

© Copyright IBM Corporation 2005
All Rights Reserved.

While network wide and interchange data-security products, protocols and procedures address information within the company and its confidentiality sharing partners, sensitive, non-public customer/patient data can make its way to the outside world via discarded computers and hard drives. To prevent these security breaches, hard drives must either be destroyed or comprehensively overwritten by sophisticated sanitising products.

Most companies don't have the time or resources to sanitise large numbers of hard drives, and may choose to have a third party perform this service for them. Third-party disposition services offer sanitising and provide Certificates of Destruction. The most convenient third-party agreements also provide cost-effective resale/disposal services.

In all, this means you may reasonably expect the following as you shop for a disposal partner:

- *Capability*
- *Reliability*
- *Documentation*
- *Staying power*
- *Final asset disposition.*

When you find all these qualities in a vendor you're comfortable with, you'll rest assured that you – and your customers – are safe.

For more information

To learn more about IBM Asset Recovery Solutions, contact your IBM representative or visit us on the Web at:

ibm.com/financing/europe