



# Disposal Safegaurds

## Privacy at Risk: Protecting Your Outgoing Data

### Introduction

With security software spending estimated at \$50 billion globally in 2005, information technology professionals are clearly taking the problems of data privacy and identify theft seriously. While most companies have focused on preventing perpetrators from breaking in to their organizations, there has been comparatively little attention on protecting information that leaves the organization on retired information technology assets. Managers who dispose of these assets in an uncontrolled manner place their companies at risk of inadvertently disclosing sensitive information and/or violating federal privacy laws.

### The Problem

Many IT organizations have implemented policies requiring sensitive data to be removed from technology assets that are designated for retirement. However, there is rarely sufficient time or controls in place to consistently implement this process due to competing priorities such as deploying new equipment or software platforms. These competing priorities, along with a lack of understanding of the data security and legal risks involved, can cause organizations to seek "easy" or "quick" solutions to their asset retirement needs. This may ultimately put the company at great risk if they rely on consignment organizations with no expertise in data security or sham recyclers disguised as used equipment brokers who offer "free" recycling.

### Implications

The most obvious ramification of releasing proprietary corporate information is that it could assist competitors and other outside parties to identify potential customers, future products, and sensitive client correspondence. According to Special Agent David Mahon of the FBI's Denver Cyber Crimes Division: "People just don't seem to realize what a significant risk that is posed by the potential compromise of information security. I recently observed some IT equipment being removed from a Denver office building. When I asked the staff what

they planned to do with the hard drives, they indicated that they would probably just send them to a landfill. Not only is this against the law in Colorado, the information on those drives could easily wind up in the wrong hands. The FBI has recovered data that has been linked to criminal activity by both organized crime and groups that threaten homeland security."

The inadvertent disclosure of sensitive data may also violate a number of recently enacted federal laws that are intended to protect information privacy. These laws include: The Health Insurance Portability and Accountability Act ("HIPAA"), The Fair and Accurate Credit Transactions Act ("FACTA"), and the Gramm-Leach-Bliley Act ("GLB"). Violation of these laws can result in substantial criminal and civil penalties as well as significant negative publicity.

Two recent high profile cases illustrate the extent to which this legislation has created significant potential liability. In March of this year the FTC announced a consent judgment against BJ's Wholesale Club based upon the inadvertent disclosure of several thousand customer credit and debit card numbers. Earlier this month the FTC announced that it had entered into another consent judgment against shoe discounter DSW for failing to adequately protect sensitive customer information. Both settlements required the companies to obtain biannual independent security audits for the next 20 years and imposed ongoing FTC oversight of their information security practices. According to recent SEC filings, BJ's and DSW estimated their potential financial exposure relating to the security breaches to be in excess of \$6.5 million.

### The Evidence

In the course of our discussions with numerous IT professionals, LifeSpan has repeatedly encountered the following attitudes toward the disposal of technology equipment:

- "Just get the equipment out of here - - we need the space."
- "Find out who can get rid of this stuff for the lowest cost."
- "Donate it - give it away."

Often, little or no emphasis is placed on ensuring data security. Instead, cost containment and generating corporate goodwill are typically the main objectives of the individuals responsible for IT asset retirement. Overwhelmingly, their goal is just to get the older equipment and e-waste out the door with as little effort as possible.

In order to investigate the extent of the data security problem in Colorado, LifeSpan purchased 20 used hard drives from four different used computer dealers located both in the Denver area and online. Some of the vendors offered recycling services and all of the vendors advertised that the hard drives had been completely purged of all data. One retail operation even performed a Microsoft "format" as we waited to make our purchase. They represented that this procedure would eradicate any remaining data left on the drive. In fact, formatting a hard drive does not eliminate data.

Using a commonly available software tool called "R-Studio" (manufactured by R Tool), LifeSpan found that 80% of the drives purchased contained sensitive data, including:

- Credit Card numbers from point of sale logs
- Social Security Numbers from an employee accounting system
- Resumes and personnel files
- Customer lists
- Intellectual Property
- A corporate prototype database
- Complete Microsoft Outlook email and address files

## Solutions

Data privacy controls for expired IT assets should be subject to a thorough cost-benefit analysis. Here are some initial questions to consider:

- 1) Do internal or outsourced service providers have the necessary procedures and controls to check the efficacy of the data destruction process from transportation to actual destruction? Is the process being audited by a third party? What kind of a chain of custody procedures does the organization maintain? What type of photographic evidence is provided?
- 2) What is the value of resale material vs. the potential costs of a breach of data security? Reselling the equipment may not outweigh the value of ensuring privacy - hence some organizations prefer to recycle all of their end of life assets regardless of residual value.

- 3) Should you perform all of your data destruction activities in-house? If so, you should either physically destroy the drives or use disk over-write software. Commercially available programs such as Kroll-Ontrack's "Data Eraser" or LSoft's "Active Kill Disk" fill the drives with "0's." Physical hard drive destruction equipment is commercially available from companies such as Shred-Tech or SEM.
- 4) Could an outside organization provide an additional level of security for your internal data destruction process? If so, what physical destruction capabilities does the vendor have? In addition to software based destruction, can they physically shred all media containing data? Does the outsourced vendor have your best interest in mind - i.e. are they motivated to provide the appropriate services to your firm or are they simply looking to profit from the resale of equipment? Lastly, is the vendor protected by errors and omissions insurance in the event that data is accidentally compromised?

## Conclusion

Managing data security risk does not have to be difficult or expensive. It requires IT executives to:

- 1) Educate their organizations on the importance of maintaining information privacy.
- 2) Develop and implement programs that mitigate risk.

*Brooks Hoffman is V.P. - Finance & Operations at LifeSpan Technology Recycling*