

Upgrading your Information Assets - Think Information Security!

Samir K. Datt
samir@datarecoveryindia.com

Consider this scenario.

Monday 0830 hrs - A sense of suppressed excitement pervades the office as the first lot of executives comes into the office. Most of them uncharacteristically early. The new & powerful computers have arrived. The IT department has successfully deployed the new **ERP?** clients over the weekend.

Monday 0900 hrs – A global email arrives requesting everyone to check his or her data on the new machines. Everybody needs to signoff electronically that all data from their previous computers has been successfully transferred to the new ones before the old ones are disposed off.

Monday 0930 – 1530 hrs – The IT department support staff solves various small glitches. Some data, which still hasn't been transferred from the old computers, is now identified and requested from the IT support staff. A number of executives' signoff on the data availability issue.

Monday 1530 – till late - IT support staff methodically work through the "data to be transferred" list from users. One by one the data from each user's old **pc** is transferred to the new ones.

Tuesday 0900 hrs – Another mail from the Administrator, requesting users to check their data and signoff, arrives. Users are informed that the old computers will be disposed off by evening and no requests for old data will be accepted after 1400 hrs today. Users recheck their data and start signing off in large numbers.

Tuesday 0900 – 1400 hrs – The IT department waits for user requests for old data. Solves small problems and tackles other issues.

Tuesday 1400 hrs – A last and final call is made to all users to determine if their data has been transferred successfully. Minor issues are resolved.

Tuesday 1430 hrs – till late – The complete IT support team is involved in formatting the old computers hard drives. Doing a full format takes 30 minutes. For 300 computers this will take far too much time. Soon the IT team speeds up the procedure by doing a quick format. As each computer cleansing is completed – the computer is boxed and stored, to be carted away by the vendor who was awarded the upgrade contract. The vendor plans to sell the old computers to a school.

Wednesday 0930 hrs – The vendor trucks pull into the office premises and the old computers are carted away.

End of Story – or is it????

An extract of a recent news item on the [SifyNews](#) Site:

Laptop with India's battle plans lands Army officers in a mess

New Delhi, Feb 5

The Army is punishing officers who offered a military laptop to a civilian for repairs, which leaked the military's top-secret strategy for a major strike in Pakistan, officials said Wednesday.

Army spokesman Brigadier Sruti Kant said the incident occurred during the height of a standoff between India and Pakistan.

A tank regiment commander sent a laptop for repairs to a civilian technician not knowing the hard disk contained the battle plans of India's armoured formation in the region, they said.

The technician fitted a new hard disk into the laptop and sent the discarded unit to a local university, where students stumbled across the vast military data bank, classified top secret.

The SECURITY PERSPECTIVE

Let's look at this from an IT security perspective.

Today more and more critical data is stored on computers. Financial data, personnel data, strategies, battle plans, medical records, bank records, passwords, credit card information, personal information, PAN numbers, new product drawings & design, cutting edge research – just about everything confidential is stored on computer hard drives. Nobody wants their personal/corporate information to fall into the wrong hands.

Deleting data, formatting hard drives or even deleting the partition table from hard drives is just not good enough. Trained personnel using sophisticated tools can successfully recover data. All your very confidential information can easily be available to motivated personnel putting individual and corporate security at great risk.

Whenever a user upgrades a hard drive, buys a new computer or sends his or her computer for repairs – the user risks his/her information.

Data Recovery companies such as Ontrack Systems, Data Recovery India, Action Front, Vogon and Ibas specialize in the recovery of hard to get data. Data that most users believe is lost and gone can still be recovered using sophisticated tools and techniques available with these companies. Virus infected, encrypted, password protected data, deleted, formatted, physically dropped, fire damaged, flood damaged are just some of the cases these companies handle on a day to day basis.

With the ever-increasing concern for data security the need for “Data Sanitization” has been felt.

Data Sanitization can be defined as a process by which residual data on media is rendered unrecoverable. This is the digital equivalent of paper shredding.

There are three main methods of doing this:

1. **Physical Destruction** – Take a hammer to a hard drive and pound it to pulp. Shatter it to tiny pieces. This is a sure fire way to destroy data and render it un-recoverable. Naturally this makes drive unusable as well. This method is followed in the US by the Department of Defense for computers they consider “Highly Classified”. In some cases monitors are also physically destroyed to prevent burned out images of confidential documents (on the picture tubes) falling into the wrong hands.
2. **DeGaussing** – This is the removal of data from magnetic media by subjecting it to very high intensity magnetic fields. Degaussers are classified as Type I, II or III depending upon application and intensity of the magnetic field. After degaussing is completed a thorough verification is required to determine successful data elimination. Degaussing is also a destructive process as it destroys the servo track information on hard drives and makes them unusable.
3. **Data Overwriting** – This is a non-destructive process. Specialized software and hardware is available for this. Bulk erasers are available that can sanitize a number of hard drives at a time. These are extremely high speed and can be excellent from a security perspective. Data overwriting normally follows a predetermined pattern. Initially a particular information is written onto a drive in a single pass then a complimentary pattern is written in another pass and this process is repeated a number of times. In the end a specific data pattern is written on to the drive. A number of forensic disk sanitizing tools are available that sanitize a disk, verify the sanitizing and in the end produce a report certifying the sanitizing process.

The disk-sanitizing problem has been addressed by the US Department of Defense. They have created a “Cleaning and Sanitizing Matrix” that lists government-approved techniques for sanitizing drives.

A study carried out by Simon Garfinkel and Abhi Shelat (between Nov 2000 and August 2002) of the Massachusetts Institute of Technology (MIT) involved purchasing more than 150 “recycled” hard drives from open market sources. A forensic analysis of the purchased drives threw up some startling results.

Of the 158 drives they examined they found that only 9% had been sufficiently sanitized to make the data unrecoverable. In the remaining drives some of the data they found included:

- Love letters
- Pornography
- Credit Card numbers
- Information from a California Children’s hospital
- Corporate memoranda
- One of the drives was from an ATM machine and contained account numbers, dates of access and account balances.
- Numerous email communications

Though 158 drives may seem like a small number – the study brings to the fore the amounts of confidential information, which can leak out and fall into wrong hands.

What needs to be done?

❖ Education

As in most cases the need to educate users & IT personnel as to what comprises disk sanitization is a must.

❖ Availability of Tools & Service Providers

Internationally there are a plethora of tools and service providers that specialize in certified data destruction. This is a trend that is catching on in India and some futuristic Indian companies are providing this service as well.

❖ Information Security Policies

Organizations must adopt comprehensive information security policies with proper data sanitizing procedures forming a prominent part of them. There should be a clear-cut policy on sanitizing media that will be sold, upgraded, destroyed or recycled.

Till then – all our valuable information will be at risk.