Who is Reading the Data on Your Old Computer?

Vivienne Mee
Rits Information Security
Citywest Business Campus
Co. Dublin
Vivienne.Mee@ritsgroup.com

ABSTRACT

Researchers at Rits Information Security performed a study in how the Irish population disposes of their old computers. How would you dispose of your old computer, or how would the company you work for dispose of their old computers?

The majority of Irish homeowners, would bring their old computers to local civic amenity centres, give it away to a relative or sell it on to another party.

Some organisations would give their old equipment to a staff member, as a gift gesture, others may simply discard in the local civic amenity site.

What is wrong with the methods currently being used for discarding of our old PCs?

With this question in mind, Rits Information Security embarked on a study to highlight the problems home users, and corporate users face when discarding retired PCs.

In this paper, Rits Information Security describes research in which a number of hard disks were taken from computers after they had been released for resale on Irish online auction sites. The research that was undertaken involved an analysis of the disks to determine if any information remained on these disks, and whether the information could be easily recovered using commonly available tools and techniques.

From this analysis, a number of disks could be traced to specific organisations, including large financial institutions, various consultancy firms, numerous small trade organisation, auctioneers, and insurance brokers. In addition to these, a number of computers were found to have originated from the home environment.

The results indicate that careless disposal of computers and storage media in the Republic of Ireland is a significant problem. Very few of the disks tested had undergone a thorough or efficient cleansing process. The level of information that could be recovered from the majority of the disks tested would have proven useful for corporate espionage, identity theft, blackmail, and fraud.

Keywords: Data protection Act, Forensics, secure disposal, legislation, recovered data

1. INTRODUCTION

In Ireland, a problem arises for the disposal of redundant computer hardware. This problem is faced daily by the home user, governments, industry and academia. Computers have a useful life span of only two to three years. After this period of time they become obsolete with little or no second hand market. As the computers are no longer valuable, the proper disposal of the information from these computers is considered an insignificant factor for the general user. Whereas for industries and governments, the costs of removing the data from the systems and ensuring all data is properly removed before they are disposed of can be a significant factor.

Large organisations tend to dispose of obsolete equipment either through their own procedures or by use of third party organisations. It is clear from the results of the disk study that many organisations have neglected their responsibilities and good business sense in disposing of the data correctly.

It is also common practise of organisations to give computers as gifts to members of staff. It is evident from the research that either "work from home PCs" were given to the staff or that computers from the office environment were given as gifts to the personnel. Often, when this is the case, a simple new operating system is installed over the old operating system, and given to the staff member. This however, does not remove all data from the PC therefore the data can easily be retrieved. The computers still contain business or personally sensitive information.

Home users tend to discard their PCs in the conventional manner, in the general purpose rubbish bins, taking them to local civic amenity sites or by selling them on to other private buyers or in some cases, by trading them in or selling them at auction. Home users believe they do not have any data that would be of use to anyone or have taken the steps of "deleting" the files from the computer. Home users are not aware of the implications of the data that can be retrieved from their computers.

The research on the disks that originated from individuals' personal computers revealed information that could be used for identity theft

This is not just a problem identified in Ireland. In 2003, two MIT students, Simon Garfinkel and Abhi Shelat, performed a study into disks available on the second hand market in the United States of America. The study was to become part of Garfinkel's PhD thesis. The study started out with the students buying 158 used hard drives from computer stores, small businesses and eBay, the online auction site(Bruce, 2004). The students recovered a vast amount of financial information and personal information of the disks.

From this study, similar disk studies have been taking place yearly since 2003, in the United Kingdom, Australia, Germany and other countries with the aim to cause awareness amongst the public of the importance of secure disposal.

In January 2005, a joint report was published by the University of Glamorgan in Wales and Edith Cowan University in Australia detailing the investigation of a number of second hand hard disks. The investigation revealed that a large number of the disks examined still contained significant volumes of sensitive information (Jones, A., Mee,V .,et al, 2005).

In 2006, British Telecommunications (BT) and Life Cycle Services (LCS) published a report from disks acquired from not only the UK and Australia, but also disks from Germany and North America. Again these disks were purchased at computer auctions, computer fairs or through E-bay in the respective geographic areas (Jones A, Valli C, Sutherland I and Thomas P, 2006).

This paper describes the research carried out in Ireland in 2007 that repeated the research performed in previous years in the other countries mentioned. It is the first known study of its kind in Ireland. This paper contains all of the initial results found of the research, reporting the types of data that was found along with the implications of such data.

2. THE RESEARCH

A number of disks were acquired from various Irish online auction sites, computer fairs and second hand shops. In total 26 disks were obtained. This seems quite a small number in relation to the number of computers are sold each year in Ireland. In the UK the same study was performed in 2005 and 2006, in which approximately 111 and 200 respectively disks were used. In comparison to the UK this small number was deemed adequate considering the geographical size of Ireland.

In 2004 it was estimated that the PC market in Ireland was estimated to be 2.011 million PCs in 2004. This has grown by an estimated 15% annually. However, there are no statistics available for how many of these PCs that are disposed of annually in Ireland. One can estimate that the life of a PC can be estimated as 3 years in the corporate sector, with perhaps 5 to 7 years for the home user. In Australia an estimated 1.6 million computers are disposed of annually (Scott, 2007)

The objective of the research was to determine whether there was any information on the disks that was visible or recoverable with readily available tools. These tools used for the research performed similar functions to the Windows Unformat and Undelete commands, and a hex editor that allows the user to view information that existed in the unallocated portions of the disk. These tools are available to anyone who potentially could obtain the disks.

The research was undertaken using forensically sound methodologies. Each of the hard disks were forensically imaged, and then placed into secure storage. Any further research was carried out on the image of the original disk. While some may query this methodology, as the disks were essentially not computer evidence but discarded equipment, it was thought to be essential practice as it allowed all the research to be performed in a non-intrusive manner, therefore, it did not affect or change any of the original information obtained. It also was used as a precautionary step, as in the research performed in 2006 by BT, material found on two of the disks necessitated them being passed to the police for further information (Jones 2006). In this research, no material was considered necessary to be passed onto the Garda Síochána (Irish Police – law enforcement).

Once all the disks were imaged, it was then possible to start the analysis. Each of the disks were analysed using the tools outlined above. The analysis was broken into two phases.

The first phase of the analysis was to identify whether or not the hard disk had any data that was visible during the initial examination. This involved loading the forensic image and looking to see if a file structure was present. Of the 26 disks, 20 disks were found to have file structures present. This phase was just an initial look at the disk images, no further tools or techniques were used in this phase.

The second phase of the analysis was to look for specific information on the disks that would allow for the identification of the user or organisation from where the disk originated. This included usernames, organisation names, email addresses, or documents and databases. The purpose of this phase was to establish the amount of the disks that could be traced to the individual or organisation.

3. RESEARCH FINDINGS

Of the 26 disks that were obtained for the research, 5 of the disks had mechanical faults and were not accessible. The remaining 21 disks were fully functional, and the following was revealed:

> *Totally blank:* (0/21) 0% of the disks was totally blank and contained no file structure or data. This implies that no disks were securely wiped.
>
> *Attempts of Removal of data:* (8/21) 38% Attempts of removal was clear. This was a simple format, a simple delete or where a new installation of an operating system was performed. All of the data on these disks was recoverable, and all data was clearly found. (13/21) 62% of the disks had no attempts of data removal.

This is similar to previous study in the UK in 2005 where it was clear that an attempt of data removal was clear for 48% of the disks.

Operating System: (18/21) 86% of the disks analysed had an installation of the Windows operating system. (2/21) 9.5% of the disks had an installation of the Apple Mac operating system, whereas (1/21) 4.5% of the disks operating system was unrecognisable. This could have been due to the attempts of removal, however, information was still extracted from these disks.

Organisation identifiable: (7/21) 33% of the disks originated from the corporate sector, which the organisation could be identified. These ranged from large financial institutions, marketing consultancies, auctioneers, electrical companies, heating and plumbing companies, legal solicitors and mobile communication companies. Information included customer's names and addresses, invoices, financial records of past jobs, emails, organisation charts and other relevant documents relating to the organisation.

In the UK study in 2005 57% of the disks originated from the corporate sector, and in 2006 47% of the disks were identified as corporate.

Personal Information: (13/21) 62% of the disks were identified as personal computers, or home user PCs, where (1/21) 5% were unrecognisable.

In the UK study in 2005 and 2006, 59% and 49% respectively hard disks contained information that was user identifiable.

From the 62% of the Personal computers, (7/13) 54% of the Personal Computers could identify their previous owner, this included names, addresses, phone numbers, date of birth, and in some cases even bank records, and Revenue and Social Insurance (RSI) number.

(2/21) 10% of the disks contained RSI numbers. Of the 10% of the Disks, (1/2) 50% was from corporate sector and (1/2) 50% was from private home user.

Financial: (5/21) 24% of the disks contained credit card information. (3/21) 60% of these disks that contained credit card information originated from the corporate sector. Alarmingly one of these disks contained a spreadsheet of at least 300 credit card details, along with expiry numbers, names and addresses. This disk came from the corporate sector that was involved in the organisation of sponsorship for a large charity event held in Ireland.

Passwords: (10/21) 48% of the disks contained passwords. These ranged from passwords to online sites, email sites, mobile phone sites,

etc.

Illegal Material: (12/21) 57% of the hard disks contained illegal material. Of the 57% of the hard disks, (3/12) 25% of the disks were originating from the corporate sector and the remaining (9/12) 75% were from home users.

The extent of the illegal material was from illicit photographs, references to illicit sites, or pirated material. Illicit in this context is used to mean images that may be considered to be pornographic. Pirate material may be considered to be pirated music or movies, downloaded illegally from online sources.

Period of Life: (20/21) 95% of the disks could identify the period of time when the system was in use. These dates dated from 1994, to as recent as 2006. (1/21) 5% of the disks dates could not be identified.

The types of information recovered from the disks were quite detailed and specific. A document retrieved from one disk that originated from a marketing consultancy revealed over 300 names, addresses and credit card details from sponsorship of a large charity event held in Ireland.

A number of other small organisation's disks revealed RSI numbers for their staff, along with VAT numbers, emails containing invoices to customers and also quotations for future work. One particular disk included installation details of electrical work, and also manuals for electrical services installed at various sites around the country, some of which were academic institutions, and civic offices.

Another disk found originated from an insurance broker. The disk had full installation of various insurance quotation packages. This disk also revealed lists of potential customers, with contact names, addresses and phone numbers, along with quotation prices. Bank details for this insurance broker were also found on this disk.

Day to day running of a solicitors office notes were found on a disk believed to be originated from a leading employment law firm. The disk may have been from the office administrator, as notes were found, and letters of correspondence to clients were also found. These letters contained information regarding various employment law cases, along with names, addresses and contact details of the clients involved.

A mobile telecommunications company disk was also found. This disk contained various emails to clients. Various credit card numbers, along with names and addresses were found belonging to business customers. Lots of network information was found on this disk, along with internal IP addresses. One email gave full details, along with username and passwords, for an internal website. It was evident that this machine was used in the customer

service department of the company.

4. IMPLICATIONS

There are many implications resulting from the data retrieved from the research. These include, and are not limited to:

Identity theft – The level of information available on the disks that belonged to the corporate sector and individuals could make it possible for identity theft or cloning. This information ranged from name, address, RSI number, email address, online banking details, credit card numbers, date of birth and other passwords to online mobile phone accounts etc. In Ireland in 2006, an estimated 15,000 people suffered from some sort of identity theft, and cost to business and consumers of approximately €250 million a year (MxSweep, 2006). Many Personal CVs were found, these could also be used as a great source of information for identity theft.

One of the disks revealed information regarding a user using an online networking site. The information revealed a member chatting on an online chat room, relating to pregnancy. In recent reports in Ireland 2 in 5 people who use social online networking sites, have been victims of Identity theft, as people put too much personal information on their sites (Breaking News, 2007). These sites include the popular Bebo, and Facebook.

ID theft does not only happen to individuals. In May of this year, M&S in Northern Ireland became a victim of Identity theft security, when one of their laptops was stolen. The laptop contained salary details, addresses, dates of birth, national insurance and phone numbers of some 26,000 employees has been stolen from a printing firm, which was tasked with the job of writing to workers about pension changes (Leyden, J, 2007).

Fraud – In many cases, the range and dept of information found belonging to the corporate sector would allow a fraudster to either manipulate the information to advantage or to generate false invoices, as many invoices were found on the disks. Other types of fraud could generate false documentation, such as quotes, references or letters of qualifications from the information revealed on the disks.

Blackmail – Of the PCs which contained inappropriate material, the users could be identified, and hence this information could be used to blackmail the user as they were downloading or browsing pornographic material, and in one instance, while at work.

Industrial Espionage – The level of information gathered concerning the day-to-day running of various organisations, along with financial figures, customer details, organisation charts, a competitor would be able to perform a very accurate analysis of the financial capability of a number of operations run by

the organisation. The potential financial cost of this information, becoming known could potentially be rated as high.

Legislation neglect – Some of the disks that originated from the corporate sector had various levels of information regarding client data. As part of the corporate sector, dealing with clients, they have a responsibility and duty of care for this information from both the business perspective and the individuals in question. The duty of care is incorporated in a range of legislation, the most obvious and relevant area being the Data Protection Act.

With all of the disks originating from the corporate sector, 33% in total, it is certain that these were in breach of the Data Protection Act and have failed in their duty of care to the business.

5. CONCLUSIONS

The results of the research mirror the results found in the USA in 2003, and the UK and other countries where the research has also been performed in 2005 and 2006. This shows that it is an ongoing problem not only in Ireland, but in all parts of the world.

The table below shows a comparison of the results of the 2005 and the 2006 disk surveys in the UK along with the results of the study performed in Ireland in 2007.

Table 1: Comparison of results of the 2005 and 2006 surveys

	2005*	**2006***	**2007**
Total Number of Disks UK	116	253	
Total Number of Disks Ireland			26
Faulty/Unreadable	13 (13 %)	90 (36 %)	5 (19%)
Wiped	17 (16 %[1])	73 (45 %[1])	0 (0%[1])
Commercial Data Present	60 (70 %[2])	42 (47 %[2])	7(33%[2])
Individual data present	51 (59 %[2])	44 (49 %[2])	13 (62%[2])

[1] Percentages are of the readable disks
[2] Percentage of readable disks that had not been wiped
* Results taken from UK 2006 report (Jones, 2006)

This research should make general computer users and members of the public aware of the implications of careless disposal procedures. In the cases of the organisations disposing of their information, members of the public should enquire about the standards and procedures in place for the disposal, as the system could contain their information.

Home users should take adequate measurements to dispose of their data also in a manner whereby they are not at risk for their information to be accessed by a fraudster.

A simple format or deletion of files will not remove information from the PC hard disk. Large organisations should be aware of the proper disposal of information methods, as it is necessary by legislation. If they have these practises already in place it is clear that their procedures are not being managed properly.

Hard drive wiping tools are available, both commercial and freeware, that will adequately overwrite the data on the hard drive. These wiping tools offer user's options of overwriting every sector on the hard drive from once to a hundred times. These tools overwrite every sector of the hard drive with binary 1's and 0's. There are tools available that meet government security standards even overwrite each sector multiple times for added protection. These tools can be found widely on the Internet.

Home users and corporate sectors should use such wiping tools before they dispose of their hardware.

ACKNOWLEDGEMENTS

The author would like to thank all those involved in making the research for this paper possible. These include, Rits Pondera who made the disks available for the research, Rits Information Security personnel who helped and supported the research, and University of Glamorgan making previous years statistics available for this paper.

AUTHOR BIOGRAPHY

Vivienne Mee is the leading author of this research paper. Vivienne joined Rits Information Security, Dublin in March 2007, as a Computer Forensic Consultant. Before joining Rits, she studied for a number of years up to Doctorate level in Computer Forensics in the University of Glamorgan in Wales. While at the University of Glamorgan, Vivienne also took part in various research studies and work in their forensic lab.

At Rits Information Security, Vivienne has completed forensic assignments for blue chip and government clients. Vivienne manages the Computer Forensic Laboratory and is responsible for procedures development and process management.

REFERENCES

Bruce, L., 2004, "Removing Financial Data from your Computer", http://www.bankrate.com/brm/news/advice/20030711a1.asp, Date accessed: 03/04/08

Jones, A., Mee,V .,et al, 2005, "Analysis of Data Recovered from Computer Disks released for Resale by organisations", Journal of Information Warfare, Vol 4 (2) 45-53

Jones A, Valli C, Sutherland I and Thomas P, 2006, "The 2006 Analysis if Information Remaining on Disks Offered for Sale on the Second Hand Market", Journal of Digital Forensics, Security and Law, Vol. 1(3) 23

Leyden, J, 2007, "M&S in ID theft flap over stolen laptop", http://www.theregister.co.uk/2007/05/09/printing_security_flap/, Date accessed: 14/08/07

Breaking News, 2007, "MySpace users warned about identity theft", http://archives.tcm.ie/breakingnews/2007/07/22/story320025.asp, Date Accessed: 14/08/07

MxSweep, 2006, "Fear of online identity theft could cost Irish businesses up to €250 million a year ", http://www.mxsweep.com/phishing-identity-theft.html, Date accessed: 14/08/07

Scott, R., 2007, "What Happens When your Computer or Gadget is Defunct?", http://www.24hourtrading.co.uk/blog/what-happens-when-your-computer-or-gadget-is-defunct-284/, Date accessed: 03/04/07