THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 3 | Number 1 Article 1

2008

The 2007 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market

Andy Jones
Security Research Centre, BT, Edith Cowan University

Craig Valli
Edith Cowan University

Glenn S. Dardick
Longwood University

Iain Sutherland
University of Glamorgan

Recommended Citation

Jones, Andy; Valli, Craig; Dardick, Glenn S.; and Sutherland, Iain (2008) "The 2007 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market," *Journal of Digital Forensics, Security and Law*: Vol. 3 : No. 1 , Article 1.
DOI: https://doi.org/10.15394/jdfsl.2008.1034
Available at: https://commons.erau.edu/jdfsl/vol3/iss1/1

The 2007 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market

Dr. Andy Jones[1,2]
Dr. Craig Valli[2]
Dr Glenn S. Dardick[3]
Dr. Iain Sutherland[4]

[1]Security Research Centre, BT
[2] Edith Cowan University
[3]Longwood University
[4] University of Glamorgan

andrew.28.jones@bt.com
Phone: +44 1473 646133
Fax: +44 1473 644385

ABSTRACT

All organisations, whether in the public or private sector, increasingly use computers and other devices that contain computer hard disks for the storage and processing of information relating to their business, their employees or their customers. Individual home users also increasingly use computers and other devices containing computer hard disks for the storage and processing of information relating to their private, personal affairs. It continues to be clear that the majority of organisations and individual home users still remain ignorant or misinformed of the volume and type of information that is stored on the hard disks that these devices contain and have not considered, or are unaware of, the potential impact of this information becoming available to their competitors or to people with criminal intent.

This is the third study in an ongoing research effort that is being conducted into the volume and type of information that remains on computer hard disks offered for sale on the second hand market. The purpose of the research has been to gain an understanding of the information that remains on the disk and to determine the level of damage that could, potentially be caused, if the information fell into the wrong hands. The study examines disks that have been obtained in a number of countries to determine whether there is any detectable national or regional variance in the way that the disposal of computer disks is addressed and to compare the results for any other detectable regional or temporal trends.

The first study was carried out in 2005 and was repeated in 2006 with the scope extended to include additional countries. The studies were carried out by

British Telecommunications, the University of Glamorgan in the UK and Edith Cowan University in Australia. The basis of the research was to acquire a number of second hand computer disks from various sources and then determine whether they still contained information relating to a previous owner or if information had been effectively erased. If they still contained information, the research examined whether it was in a sufficient volume and of enough sensitivity to the original owner to be of value to either a competitor or a criminal. One of the results of the research was that, for a very large proportion of the disks that were examined, there was significant information present and both organisations and individuals were potentially exposed to the possibility of a compromise of sensitive information and identity theft. The report noted that where the disks had originally been owned by organisations, they had, in most cases, failed to meet their statutory, regulatory and legal obligations.

In the third and latest study, conducted in 2007, the research methodology of the previous two studies conducted was repeated, but in addition to Longwood University in the USA joining the research effort, the scope was broadened geographically and the focus was extended to determine what changes had occurred in the availability of sensitive information might be occurring over time.

Keywords: Computer forensics, disk analysis, data recovery, data disposal, electronic data destruction, privacy.

1. INTRODUCTION

The first of a series of annual studies was carried out and published in January 2005, (Jones et al, 2005). The study was jointly conducted by the University of Glamorgan in Wales and Edith Cowan University in Australia and reported the details of research into the data that remained on a number of second hand hard disks that had been obtained on second hand markets. The research revealed that a significant proportion of the disks that were examined still contained considerable amounts of information, much of which would have been of a sensitive nature to the organisation or individual that had previously owned the disk. The research had been conducted in order to obtain an understanding of the amounts and types of information that remained on disks that had been offered for sale on the second hand market. Prior to the publication of the report of this first study, there had been limited investigation of the issues, with the most significant evidence being reported by (Garfinkel and Shelat, 2003). There had also been a small number of commercially sponsored investigations and newspaper reports on the subject of personal data being recovered from disks that had been disposed of that indicated ongoing problems with regard to residual data on disks. However, before the 2005 report, with the exception of the Garfinkel and Shelat paper, there had not been any significant extensive prior research into the topic.

The 2005 report identified that a large majority of the random sample of disks that were obtained still contained significant amounts of information that the researchers considered to be sensitive and which had the potential to cause embarrassment or financial harm, whether they had originally been in use within the corporate environment or by the home user.

The research that was carried out in the second consecutive annual study in 2006 was again conducted by the University of Glamorgan in Wales and Edith Cowan University in Australia, but this time the Security Research Centre of British Telecommunications also contributed to the effort. In the 2006 survey, the research of 2005 was repeated and expanded to include a number of additional countries. The report (Jones et al, 2006) on research conducted in the second annual survey revealed that for countries surveyed in both years there had been no significant changes from the prior year in the amount and sensitivity of information that could be recovered from the disk drives obtained from the second hand markets of those countries. Additionally, the results from the disk drives obtained from the second hand markets of countries that had not been included in the 2005 survey were broadly similar to the other countries that were included in both the 2006 and 2005 surveys.

The research undertaken in 2006 was sponsored by British Telecommunications (BT) and Life Cycle Services (LCS) who funded the purchase of the disks. The aim of the 2006 research was to determine whether there had been any change in the level or potential sensitivity of information that remained on the disks during the intervening period and also to gain an understanding of how the results that were obtained compared between the countries that had previously been surveyed and those that had not previously been surveyed. Both sets of research were conducted under the same conditions using commonly and easily available tools that had similar capabilities and the results were then compared. The outcome of the research was that a number of conclusions and recommendations were made on ways in which the removal of data from disks that were being disposed of could be improved.

This paper, the report on the third and latest survey, contains the results of the 2007 research which has again extended the scope of the countries included in the survey. The research in 2007 was again carried out by the University of Glamorgan in Wales, Edith Cowan University in Australia and the Security Research Centre of British Telecommunications, and this year, Longwood University in the USA also contributed to the effort. The research was again sponsored by British Telecommunications (BT) and had the same objectives as the research in the two previous years.

2. THE RESEARCH

To ensure that the results of the research provide a realistic and scientifically sound picture of the environment, a minimum sample size of 42 disks was obtained. All of the disks used in the research were purchased at computer auctions, computer fairs or through eBay in the respective regions. The disks were purchased discretely by a number of purchasers and were obtained for the most part either singly or in small batches in order to minimise the possibility of the sellers becoming aware of the purpose for which the disks were being obtained.

As with the research in each of the previous two years, the disks were supplied 'blind' to the researchers. The purpose of supplying the disks through this process is to present the disks to the researchers in a manner such that there is no information that might indicate the original source of the disks, such as the place that they were purchased or any external markings or labels. The only identifier on the disks as they were provided to the researchers was a unique sequential serial number. By supplying them in this way, any information that is recovered by the researchers can be clearly identified as having been the result of the data that was available on the disk.

The research methodology used was the same as that used in the earlier research (Jones 2005, 2006), with each disk being forensically imaged using commercial software and then stored in secure storage areas. The analysis was undertaken on the forensic images of the original disks. The rationale for this time consuming step was twofold. It was considered that there was a need to preserve the original media in an unaltered state and store it in a secure area in case there was a requirement to pass the disks on to the police in the event that criminal activity that was notifiable was discovered and the chain of custody needed to be preserved for an investigation by law enforcement. The second reason was to allow the research to be carried out in a non intrusive manner that did not affect or change the original data in case any anomalies were detected with the image and it was necessary to validate the data against a second image created from the original. As with the research in both of the previous years, this proved to be a sensible precaution, as two of the disks were found to contain material that necessitated them being passed to law enforcement for further investigation.

The tools used in the 2007 study to carry out the analysis of the disks were fundamentally the same as those used in the previous years (although the versions of the tools may have changed). The tools performed similar functions to the Windows Unformat and Undelete commands and a hex editor (which can be used to view any information that exists in the unallocated portion of the disk). Tools that perform this type of functionality are freely available: examples include Autopsy (Version 2.08) and the Linux based Helix software. These types of tools do not require significant levels of skill or knowledge to

affect the recovery of remnant data from storage media.

The objectives remained the same as in previous years: firstly to determine whether the disks had been effectively cleansed of data or whether they still contained information that was either visible or easily recoverable with the tools identified above. The second objective of the research was to identify whether information that would allow for the identification of the organisation or individual(s) that had used the disk's host computer and, if possible, additional information such as the usernames, email addresses or documents, spreadsheets and databases in order to determine the number of disks that could be traced to an organisation or an individual.

The results from the 2007 survey indicate that there has been very little change over time in the amount or sensitivity of the information that remained on disks that were made available in the second-hand market. Before discussing the results for the 2007 survey we briefly describe the analysis of the previous years.

3. SUMMARY OF THE PREVIOUS RESEARCH RESULTS

In brief, the results of the research in the previous years highlighted a number of issues. These included the fact that nearly half of the second hand disks that were obtained had had some attempt made to remove the data with the majority of those attempts proving unsuccessful. In fact, the vast majority of the second hand disks contained data that could easily be recovered. Approximately half of the disks still contained sufficient data to allow the previous owner, whether an organisation or an individual, to be identified and one fifth contained financial information relating to the organisations, including staff salary details, sales receipts and profit and loss reports. There were also a significant number of disks that had come from systems belonging to critical infrastructure providers such as power generation, water and telecommunications utilities.

The report of the 2006 research identified that, despite an increasing awareness as a result of publicity from a number of information losses and incidents of identity theft and the results of a number of surveys (Synovate, 2003; Price Waterhouse, 2006; Johannes, 2006) and increasing level of regulation, there was no indication that organisations had modifying their procedures to ensure the effective removed of data before the disposal of the computer hardware.

4. THE 2007 RESEARCH RESULTS

This section details the results for the study carried out during this year, covering the UK, the USA, Germany and Australia. As in previous years, the results of the study are broken down into the individual countries to enable comparison.

For the 133 disks obtained in the UK:

- Of 133 disks obtained, 59 (44%) were unreadable and failed to spin up.
- 28 (38% of the readable disks) were totally blank and no data could be recovered from them.
- Of the remaining 46 (62% of the readable disks),
  - 19 (41%) contained sufficient information for the organisation that they had come from to be identified.
  - 30 (65%) contained sufficient information for individuals to be identified.
- 8 (17%) contained information that might be considered as illicit.

For the 46 disks that were obtained from North America:

- 15 (33% of the disks) were physically damaged and could not be accessed
- 6 (19% of the readable disks) had been wiped and contained no data.
- Of the remaining 25 (81% of the readable disks),
  - 8 (32%) contained sufficient information for the organisation that they had come from to be identified.
  - 15 (60%) contained sufficient information for individuals to be identified.
- 8 (26% of the readable disks) contained illicit material.

Comment: Efforts had been made to remove the data from a total of 23 of the disks, but it had only been effective in 6 cases.

For the 42 disks that were obtained from Germany:

- 30 (71% of the disks) were not in working order and could not be accessed.
- 5 (42% of the readable disks) had been wiped and contained no data.
- Of the remaining 7 (58% of the readable disks),
  - 2 (29%) contained sufficient information for the organisation that they had come from to be identified.
  - 4 (57%) appeared to be from individuals. The source of the other disk could not been determined.

For the 79 disks that were obtained from Australia:

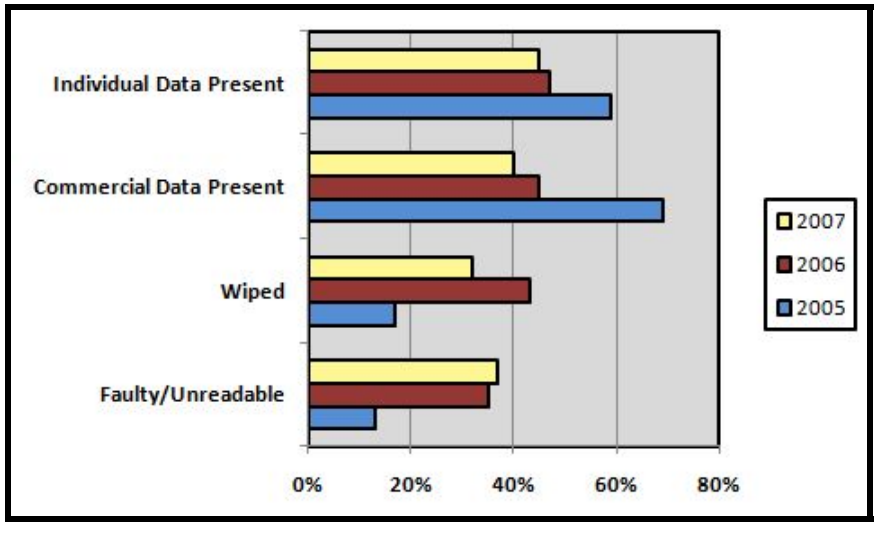
- 8 (10%) of the disks were physically damaged and could not be

accessed

- 23 (32% of the readable disks) had been wiped and contained no data.
- Of the remaining 48 (68%),
  - 22 (46%) could be identified as having come from commercial organisations and
  - 7 (15%) contained sufficient information for individuals to be identified.
- 6 (8%) of the disks contained illicit material

Table 1 shows a comparison of the results of the 2005, 2006 and the 2007 disk surveys.

Table 1: Comparison of Study Results by Year



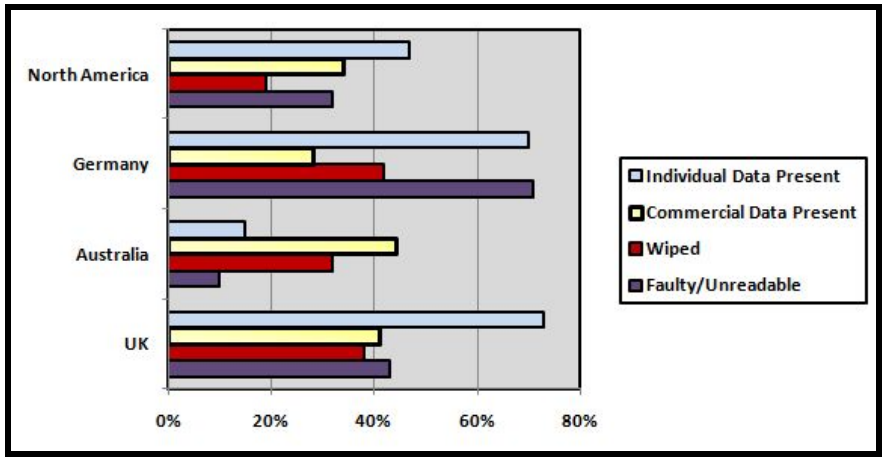
Note: The results for the wiped disks are given as a percentage of the disks that were readable.
Note: The results for data present are given as a percentage of readable disks that had not been wiped.

The results of the 2007 survey appear to indicate that, after a significant variance in some of the results between 2005 and 2006, the 2007 results are more consistent with those obtained in 2006. Between 2005 and 2006, there was a significant increase in the proportion of disks that were faulty and also an increase in the number of disks that had been wiped effectively. The results from the 2007 survey are more consistent with those obtained in 2006, with the exception that the number proportion of disks that had been effectively wiped

dropped significantly (from 45% to 33%).

There was a slightly reduced proportion of the disk that could be attributed specifically to commercial organizations but the proportion of disks that contained personal information remained within one percent of the 2006 results. One possible explanation for this may be that individuals are increasingly using the same computer for both personal and corporate information, as the technology becomes increasingly ubiquitous. The table below shows a comparison of the results from the disks obtained in the different regions.

Table 2: A Comparison of the Results from the Disks Obtained in the Different Regions



Note: The results for the wiped disks are given as a percentage of the disks that were readable.
Note: The results for data present are given as a percentage of readable disks that had not been wiped.

The results of the 2007 survey that were obtained from the individual countries have again revealed a small number of what appear to be significant disparities. The first is that the number of disks that were unreadable varied from 71 percent in Germany to 8 percent in Australia (In 2006 the figures were 75 percent in Germany and 6 percent in Australia). The consistency of the figures over the two surveys would indicate that the markets for second hand hard disks are significantly different in the two regions. The second disparity that was noted was that while the proportion of the disks wiped in the UK, Germany and Australia range between 32 and 42 percent, the results from the USA give a significantly lower figure at 19 percent. While this figure is much lower than that in the other regions, it is a significant improvement in the figure of 8 percent that was obtained in the 2006 survey in the USA. This is the third

set of results from the UK and Australia and the second from the USA and Germany. While it is still too early to draw any conclusions on possible trends, the results would appear to indicate that the situation has stabilised and a comparison of results from 2006 to 2007 shows a great deal of consistency, with the exception of the issues raised above.

Once again, a surprisingly large range and quantity of information that could be potentially commercially damaging or a threat to the identity and privacy of the individuals involved was recovered as a result of the survey. An indication of the quantity and type of material that was recovered in 2007 from the disks that originated in commercial and academic establishments included:

- From three disks that originated from an company managing entertainment establishments in the USA there were Social Security numbers, personal phone numbers, wage info of employees and a Corporate Telephone directory. There was also information on the corporate policy with regard to employees serving jury duty and the employee expectation of privacy with regard to e-mail communications.
- From a company that provides sprinkler systems in the USA, there was information on social security numbers for employee applicants and the results of drug tests, lists of clients that included names and contact values and details of monthly sales and the cost and profit per contract.
- From the computer of an attorney in the USA were details of a Last Will and Testament, several Bank Account numbers, a number of Federal ID numbers for the estates (of deceased) and Social Security numbers of deceased individuals and details of Several Property Settlements (Divorce cases).
- From the computer of another attorney who worked in the corporate tax dept of a bank in the USA were Login id's and passwords for various personal accounts and personal credit card information and a number of legal documents which appeared to be for family members. The PC that the hard disk had been used in had apparently been given to the bank employee (by a bank employee with the same name) as compensation. The user of the disk apparently ceased to be an employee with the bank when the corporate tax dept was moved to another city as the result of a merger/acquisition.
- From an undetermined source, one disk contained copy of a Petition in the Family Court of the State of New York, Dutchess County, for Grandparent Visitation with the notation "FILED UNDER SEAL – CONTAINS CONFIDENTIAL INFORMATION CONCERNING MINORS." The petition contained information regarding the sexual

molestation of a minor.

- Data from a disk that appears to originate from the National Health Service in the UK relates to Hospital / medical data that can be attributed to a specific group of hospitals. The information retrieved included patient medical data including histology reports and other information for a number of individuals and a telephone contact list for the group of hospitals. There was also data present that indicated the interests of the users of the system in terms of their web surfing habits.
- Nine disks were recovered that had belonged to a Furniture Warehousing company based in the East Midlands of the UK. The information recovered included the Company logo, letters to customers, the names of staff, internal telephone numbers, a number of (expired) Credit Card Numbers, a letter threatening court action and Pornographic material.
- A disk that had originated at a Queensland Real Estate agent in Australia contained a wide range of confidential documents that related to real estate based transactions. These included, but were not limited to, bank account details, credit card details, eviction notices, rent arrears notices, property sale and transfer details with the appropriate signatories. There was also a limited amount of hardcore pornographic pictures contained on the hard disk. Analysis of the Internet activity history indicated frequent surfing of hardcore pornographic sites in addition to standard business-related activity.
- One disk that had been used by a medical services provider in Australia contained personal medical records, including addresses, next of kin details, phone numbers and other information that would be contained in a medical record. In addition, there were letters to patients and credit card and banking details of the patients. This case represented significant exposure of patients personal and financial details.
- A disk that had belonged to an insurance company in Australia contained documents with names and addresses, vehicle types, registrations, vehicle identification numbers and policy expiry dates for a motor vehicle insurance company. There were also files with large amounts of information on many policy holders, which also contained customer invoices as well expired policy notices. This creates a significant exposure on several levels not only could these details be used to commit fraud but also allow a car thief to readily target selected cars for theft. The vehicle identification numbers and other details could also be useful for individuals who steal and re-birth

(clone) high value or high performance cars.

- A set of disks that were obtained from Ebay that contained data indicating that they were from a large multi-national mining company that were less than 1 month old when they were acquired. The disks contained a large amount of corporate documents and would be problematic and embarrassing for the organisation should they have fallen into the wrong hands for either profit through advantage or by fraudulent means. It should be noted that these drives were specifically advertised as coming from a large corporate customer in the sales promotion on eBay.
- A hard disk that originated in a major international merchant bank and stock brokerage firm in Australia that contained information on computer account details, VPN connection details and other password files. The disk also contained sensitive network information that could be used to perform reconnaissance or attack these networks and was last accessed in July of 2006.
- This hard disk readily booted when installed in appropriate Sun server hardware and the partitioning configurations of the hard disks concerned indicated that they were primary operating system drives in servers.
- A laptop disk that had been used by a senior academic in the Information Systems school within an Eastern States based Australian university not only had the expected student results and communications but also, as a result of the academic's position in the school, contained confidential minutes of departmental meetings, strategic planning and course development initiatives being undertaken. In addition, the material included confidential information on staff and covered a sensitive ongoing industrial relations issue.
- Two disks were recovered in the UK that contained sufficient information to be able to determine that they had originally been used in schools, one of them a primary (elementary) school. There was no student or personal information recovered from either of these disks

The type of material that was recovered from the disks that originated from home PCs included:

- A disk from the UK that contained the name and address of the user together with letters relating to a number of phone complaints. There were also bank account numbers and sort codes, together with passwords for on line accounts.
- A disk that had belonged to a gentleman from the Birmingham area of

the UK that contained details of his employment in a government department, his CV, his email addresses and a collection of pornographic images and references to 'hard core' pornography and email from a 'swingers' club. Also on the disk was a password and login ID for an (online) video store.

- A disk from Australia that came from what appeared to be a religiously devout household due to the profile of web sites visited. The disk also contained sexually explicit photographs of an adult male member of the household.
- A 20Gb laptop hard drive from Australia that initially appeared to be blank because the first 8Gb of the drive appeared to have been erased. However, the remainder of the disk was not. The disk still yielded confidential documents and personal information from the remainder of the hard disk. It would be reasonable to assume that the utility being used to erase the disk did not go beyond the 8GB limit either because it was a trial version of software or was faulty with respect to the 8GB limit on hard drive size.
- Illicit information including downloaded audio and video files. A number of cases of pornographic material were encountered and also two case of paedophile material (these have been referred to the police for further investigation). In addition, one disk contained evidence the use of BitTorrent and the illegal downloading of movies.

With the increase in the availability, use and reliance on computers and the services that they enable has come the ability and requirement to store, process and transmit increasing volumes of information, a proportion of which will be sensitive. While the technology has kept pace with the requirement to protect this information to an appropriate level and to remove it effectively, the failures seem to be attributable to a lack of corporate policies and procedures for the disposal of obsolete equipment and individual awareness of the impact of storing such information and procedures for ensuring that it is removed when it is no longer required.

The subject of the disposal of disks that have not been effectively sanitised of sensitive data is not a new issue, but recently has become more of a concern as evidenced by the frequency of reports in the public press. The subject has first made the news in 1993 in an article in the Canadian Globe and Mail (Canadian Globe and Mail, 1993) and has been periodically reported in the intervening years to date, including, notably, a report (Calvert and Warren, 2000) that appeared in 'The Daily Express' regarding the disposal, by the Morgan Grenfell Asset Management merchant bank, of a disk that contained details of Sir Paul McCartney's bank account. In 2005 (Jenkins, 2005) reported that that a number of IBM RS/6000 servers that had formerly been owned by the

Australian Sydney State Transit Authority had been released from the agency with operating systems and data intact. The data included the source code for ticket machines used on Sydney's buses and ferries. It is notable that until 2005, the subject only made the mainline news once every two or three years.

There have been an increasing number of reports of the loss of sensitive information as a result of accident or theft. In 2006 there were two reports that appeared in the Register, the first (Vance, 2006a) report was about the loss of a laptop computer by Ernst and Young that contained information including details such as the social security numbers of its customers, including that of the Sun Microsystems CEO Scott McNealy. The second report (Vance, 2006b) was on the loss, by Wells Fargo, of a computer containing sensitive data including customers' names, addresses, Social Security numbers and Wells Fargo mortgage loan account numbers.

In academia, a paper presented at a 1996 conference (Gutmann, 1996) discussed the subject of the secure deletion of data. A second paper by (Gutmann, 2001) examined 'Data Remanence in Semiconductor Devices' and then another paper (Garfinkel and Shelat, 2003) examined ways in which disks could be 'sanitized'. In 2004, an article (Leyden, 2004) published in the Register reporting that a mobile security group called Pointsec Mobile Technologies had purchased a hard disk for £5 through eBay that contained a customer database and the current access codes to what was supposed to be a secure Intranet of a large European financial services group. Another report in 2004 (Valli, 2004)

Finally in 2005, there were a number of reports including:

- One in May (TechWeb News, 2005) indicating that 70% of second hand hard disks still contained data and one in September (BBC News), which reported the information found by Disklabs on 100 disks that they had obtained.
- There has been an upsurge of publicity on the problem of identity theft and the level of exposure that the whole topic of protection of personal information has received over a number of years. In addition there has been an increasing availability of suitable tools[1] that can ensure the safe erasure of information. Given this publicity, the capability to address the issue and the increasing general level of computer literacy, it seems strange that the general level of awareness of the potential problems related to the disposal of computer equipment is so poor.
- There is also increasing national and international legislative pressure addressing issues from the protection and appropriate handling of

[1] Such as the Blancco tool which is approved for use by the UK Government.

personal information to issues of corporate governance which should have the result that organisations in the public and commercial sectors have little or no excuse for failing to ensure that all types of sensitive information is removed effectively from Information Technology equipment before it is released for disposal. The new legislation appears to stem partially from a need to introduce measures to address the changing environment and also, possibly, to meet the requirement to secure the Critical National Infrastructures of the individual countries.

- For disks that have originated in computers that have been for personal use in the home environment, the situation is entirely different. There has been a massive and rapid expansion in home computing and an improvement in graphic user interfaces (GUIs). The GUI makes the use of the computers more intuitive, but at the same time means that tasks are carried out in the background in a manner that makes them transparent to the user. This results in the user not being aware of the information that may be stored on their devices, where it is likely to be stored or how to remove it and be sure that the removal has taken place. People do not seem to correlate the warnings that they get about their online activities and the personal information that they expose and the need to remove it before they dispose of their personal computers.
- This can have a significant impact if the home system is used to access a corporate network or to complete work related tasks. This can result in data being stored on systems over which the corporate organisation has no control. A significant number of disk drives that were examined did contain a considerable mix of corporate and personal data. Sometimes this was the result of a user utilizing a corporate system for personal purposes and sometimes it was the result of a user accessing corporate data from a personal home system. In a small number of cases, it was the result of a user that was a one-person organization using the computer for both personal and business use, such as an attorney. The problems of a user inappropriately using a system for both personal and corporate use could be addressed through the implementation and adherence to corporate computer security enhancements and acceptable use policies.
- In this year's study one of the faulty disks was opened and examined. The heads had come to rest part way across a platter. The heads were manually reset to the park position, this was carried out in a normal air-conditioned environment i.e. No special clean room technology was used in accordance with the objectives of the disk study, that this should be an activity that a technically competent user could perform

without recourse to specialised equipment. Once reassembled the disk then functioned normally. The disk had a complete file system. This suggests either the user sold the disk as faulty or the disk was damaged in transit. In either case no attempt had been made to remove the corporate data that was present on the disk. This suggests disks considered dead or faulty should be put through the same disposal practices as disks removed from a working system.

In summary, as in previous years, a number of disks were found to contain sensitive corporate and personal information. The potential effects of these organisational and individual failures to remove sensitive data are that this type of information continues to be accessible to the type of people who may seek to exploit it.

5. CONCLUSIONS

While the improvements in the results that were detected in 2006 have largely been confirmed, it was disappointing to not that the percentage of disks that have been effectively wiped has actually reduced significantly (from 45 percent to 33 percent) in the 2007 survey. It is still to early to draw any conclusions with regard to trends but, with only a 33 percent of disks that could be accessed having been effectively wiped, it reasonable to comment that this is an area where there is significant potential for improvement

The results of the 2007 survey reinforce the observation made after the 2006 survey with regard to the proportion of disks that were purchased that could not be accessed, with an overall 37 percent of the disks being faulty (the 2006 survey gave a result of 36 percent). For the second year the results from disks purchased in Germany were remarkable with 71 percent of the disks obtained there being faulty.

It is clear from the results of this research that there is an ongoing requirement for organisational awareness, education and training programmes for appropriate staff to ensure that staff can fulfil their corporate responsibilities when Information Technology equipment are leaving their control. There is also an argument for an increased involvement by government in the form of leadership and legislation to implement an environment that is supportive of measures to improve information security. For the home user there is an ongoing and increasing requirement for programmes to inform and educate them of the problems that may occur when they dispose of computer equipment and the measures that they can take to avoid potential losses.

6. RECOMMENDATIONS

In the 2006 survey report, six recommendations were made with regard to the

types of measures that organizations and individuals could take to reduce the quantity of sensitive information that is inadvertently given away when computer devices and the hard disks that they contain are disposed of. These, in brief, were:

1. **Education -** A public awareness campaign by Government, the media, commerce and/or academia.
2. **Risk Assessment -** Organizational risk assessments to determine sensitivity of the information on disks.
3. **Best Practices -** The introduction in organizations of procedures to ensure that computer systems and computer hard disks are disposed of in an appropriate manner.
4. **Physical Destruction -** Where appropriate, the physical destruction of the disks.
5. **Electronic Data Destruction (EDD) -** Access provided by the information and communications technology industry to the tools and facilities to enable individuals to effectively remove the information from their computers.
6. **Secure Access -** The full encryption of hard disks to ensure that information could not be easily recovered.

All of these recommendations are repeated and in addition, it is recommended that;

7. **Asset Tracking** - It is also suggested that organisations may more effectively secure their data if asset tracking is conducted at a storage device level. This would require that asset tags are placed on individual disks rather than the computer system unit to ensure safe disposal as increasingly systems are offered with more than one physical storage device.
8. **Legal -** Responsibility assigned to those charged with receiving discarded or damaged hard disks and disks considered dead or faulty should have the same disposal practices applied to them as disks removed from a working system.
9. **Cell Phones -** Because of the increased use of text messaging, cell phones and the storage that they utilize should be treated as sensitive and their disposal should be handled in the same way as hard disk drives.

CONTRIBUTING ORGANIZATIONS

British Telecommunications (BT). BT is one of the world's leading providers of communications solutions serving customers in Europe, the Americas and Asia Pacific. Its principal activities include networked IT services, local, national and international telecommunications services, and higher-value broadband and internet products and services. In the UK, BT serves more than 20 million business and residential customers with more than 30 million exchange lines, as well as providing network services to other licensed operators.

Edith Cowan University (ECU). The Security and Intelligence research cluster of the School of Computing and Information Science at ECU conducts research into all aspects of Computer and Information Security from the technological aspects of computer forensics and network security to the 'softer' side involving issues such as perception management and information policy. At present, its research theme is 'deception'. The group has numerous doctoral, masters and honours candidates. Its main areas of interest are information operations, computer/network forensics, RFID security, mobile computing security, honeypots and the use of deception in security.

Longwood University (LU). The University offers interdisciplinary programs in Homeland Security and in Digital Forensics, Security and Law. Longwood University's program in Homeland Security offers students an interdisciplinary exposure to the global economic, cultural and political issues relevant to homeland security. It's Digital Forensics, Security and Law program brings together students from Information Systems, Criminal Justice and Computer Science.

University of Glamorgan (UoG). The Information Security Research Group from the Faculty of Advanced Technology at the UoG has a strong and well established theme in the areas of Computer forensics, Computer Network Management and Computer Network Defence. The Information Security Research Group is focused on the issues associated with the design and development of early warning systems that are capable of detecting and responding to a variety of cyber based attacks, and on the issues associated with computer forensic science. The research is conducted mainly in the two specialised laboratories of the group, the Network Security Laboratory and the Computer Forensics Laboratory. The research feeds into the undergraduate and postgraduate degree schemes in forensics and computer systems security offered at the university.

ACKNOWLEDGEMENTS

In addition to the individuals named as authors for this paper, we would like to acknowledge the people who assisted in the imaging and analysis of the large

number of disks required for the research (a non trivial task). The people involved were:

Andrew Blyth, Nick Pringle, Paula Thomas, Theodore Tryfonas, Andrew Woodward

REFERENCES

American Forces Press Service (2006), Current Service members Possibly Affected by VA Data Loss, 6 June 2006.

BBC News (2005), Data dangers dog hard drive sales, BBC, 12 September 2005.

Calvert, J, Warren, P (2000), Secrets of McCartney Bank Cash Are Leaked, Daily Express, 9 February 2000, pp 1–2.

Canadian Globe and Mail (1993), Disk Slipped Into Wrong Hands, Canadian Globe and Mail, 2nd August 1993.

Garfinkel S.L, Shelat A, (2003), Remembrance of Data Passed: A Study of Disk Sanitization Practices. IEEE Security & Privacy, Vol. 1, No. 1, 2003.

Gutmann, P. (1996), Secure Deletion of Data from Magnetic and Solid-State Memory, Sixth USENIX Security Symposium Proceedings, San Jose, California, July 22-25, 1996.

Gutmann, P. (2001), Data Remanence in Semiconductor Devices, 10th USENIX Security Symposium, Washington, D.C., August 13-17, 2001.

Jenkins, C. (2005), Govt data sent to auction. The Australian, 2nd August 2005.

Johannes, R. (2006), The Demographics of Identity Fraud: Through education and vigilance, banks can prepare and protect those most vulnerable, Javelin Research, http://www.javelinstrategy.com/uploads/607.R_2006_IDF_Demographics.pdf, Aug 2006.

Jones, A., Mee, V., Meyler, C., and Gooch, J,(2005), Analysis of Data Recovered From Computer Disks released for sale by organisations, Journal of Information Warfare, (2005) 4 (2), 45-53.

Jones, A., Valli, C., Sutherland, I., and Thomas, P,(2006), The 2006 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market, Journal of Digital Forensics, Security and Law, (2006) 1 (3), 23-36.

Kerber R (2006), Firm will settle with state over data loss: Missing laptop had information on thousands, Boston Globe, 12 December 2006.

Leyden, J. (2004), Oops! Firm accidentally eBays customer database, The Register, 7 June 2004.

Price Waterhouse Cooper (2006), DTI Information security breaches survey 2006, http://www.dti.gov.uk/industries/information_security Sept 2006.

Synovate, (2003), Federal Trade Commission – Identity Theft Survey Report, Federal Trade Commission, June 2006.

TechWeb, (2005), Seven-In-Ten Second-hand Hard Drives Still Have Data, TechWeb News, 31 May 2005.

Valli, C. (2004), Throwing out the Enterprise with the Hard Disk, In 2nd Australian Computer, Information and Network Forensics Conference, We-BCentre.COM, Fremantle Western Australia.

Vance A (2006a), Ernst & Young fails to disclose high-profile data loss: Sun CEO's social security number exposed, The Register, 25 February 2006.

Vance A (2006b), Wells Fargo fesses up to data loss: Lightning strikes twice for HP man, The Register, 12 May 2006.

AUTHORS

Dr. Andy Jones is the Head of Security Technology Research at the Security Research Centre at British Telecommunications (BT) where he leads the research into the risk management methods, anomaly detection and computer forensics. In addition he sits on the Government GIPSI committee and the management board of the Tiger Scheme (a professional validation scheme for people carrying out penetration tests) and holds a post as a visiting adjunct at Edith Cowan University in Australia, where significant research is being carried out into wireless networking, RFID vulnerabilities and computer and mobile device forensics.

Dr. Craig Valli is the Head of School of the School of Computer and Information Science. He has more 20 years experience in the IT Industry and consults to both government and industry on network security and forensics issues. He is the Chair of the Australian Digital Forensics Conference and Co-Chair of the Australian Information Security Management Conference. Craig is also a Co-Editor of the Journal of Information Warfare and Editor of the Journal of Network Forensics. He has over 30 publications to his name on security related topics. His research and teaching interests include Network Security, Honeypots, Intrusion Detection Systems, Compute Clustering, Computer Forensics, RFID Wireless and SCADA Security.

Dr. Glenn S. Dardick is an Assistant Professor of Information Systems within the College of Business and Economics at Longwood University. He has over 33 years experience in the IT Industry and began working with microcomputer storage media 27 years ago while serving as an original member of the IBM PC development team. Dr. Dardick is responsible for the Digital Forensics, Security and Law program at Longwood University teaching Digital Forensics

and IT courses at the undergraduate and postgraduate levels. Dr. Dardick frequently consults with attorneys in matters concerning Digital Forensics and IT. He has testified in Federal, State and Sectarian courts within the United States. Dr. Dardick is also the Editor of the Journal of Digital Forensics, Security and Law and serves as the Chair of the annual ADFSL Conference on Digital Forensics, Security and Law.

Dr. Iain Sutherland is a Senior Lecturer at the Faculty of Advanced Technology the University of Glamorgan. He has been involved in a variety of research projects in the area of information security including secure XML transactions, and reverse engineering metrics. Dr. Sutherland's main field of interest is computer forensics, he maintains the University's Computing Forensics Laboratory. Dr. Sutherland has acted as an investigator and consultant on both criminal and civil cases. In addition to being actively involved in research in this area and supervising a number of Ph.D. students, Dr. Sutherland teaches computer forensics at both undergraduate and postgraduate level on the university's computer forensics degree schemes.