Annual ADFSL Conference on Digital Forensics, Security and Law 2009

May 21st, 1:00 PM

Why are we not getting better at Data Disposal?

Andy Jones
Head of Information Security Research, Centre for Information & Security Systems Research, BT, Adjunct Professor, Edith Cowan University

Scholarly Commons Citation
Jones, Andy, "Why are we not getting better at Data Disposal?" (2009). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 7.
https://commons.erau.edu/adfsl/2009/thursday/7

Why are we not getting better at Data Disposal?

Prof. Andy Jones [1 2]
[1]Head of Information Security Research,
Centre for Information & Security Systems Research, BT
[2]Adjunct Professor, Edith Cowan University

ABSTRACT

This paper describes two sets of research, the first of which has been carried out over a period of four years into the levels and types of information that can be found on computer hard disks that are offered for sale on the second hand market. The second research project examined a number of second-hand hand held devices including PDAs, mobile (cell) phones and RIM Blackberry devices. The primary purpose of this research was to gain an understanding of the reasons for the failure to effectively remove potentially sensitive information from the disks and handheld devices. Other objectives included determining whether there were regional variations in the results and whether there had been any changes in the results detected over time. From the research it was possible to develop advice on the measures that could be adopted to reduce the level of data being inadvertently released into the public domain.

Keywords: Disk Study, mobile device, security data destruction, disk erasure

1. BACKGROUND

In the last few years there has been an ever increasing level of media attention on high profile data losses such as the Feb 2009 Kaiser Permanente[3] loss of a data file containing details of names, addresses, dates of birth and Social Security numbers that resulted in 30,000 California employees having to be notified of the release of personal information, the Feb 2009 Parkland Memorial Hospital[4] loss of a laptop computer that may have contained the names, birthdates and Social Security numbers of 9,300 employees and the UK Ministry of Defence (MoD) [5] loss of a portable computer drive containing the names, addresses, passport numbers, dates of birth and driving licence details of around 100,000 serving personnel across the Army, Royal Navy and RAF, plus their next-of-kin details and the details of 600,000 potential services applicants and the names of their referees.

These incidents have served to highlight the damage that can be caused as a result of a data security breach, whether malicious or accidental. Unfortunately, the high profile nature of these incidents has, in some ways, diverted attention from a number of the underlying issues. At the same time that these high profile data breaches are occurring, a huge number of less prominent or significant losses are not highlighted in the press. Some of the reasons for this are that the losses go undetected or unreported and also that the individual cases are not of themselves, newsworthy.

It is increasingly clear that the levels and types of information that are given away on a daily basis when equipment that contains digital storage media such as computers, PDAs, mobile phones etc. is

[3] Michael Barkoviak, Daily Tech, Kaiser: Employee Data Breached, Identity Theft Reported, 8 Feb 2009, http://www.dailytech.com/Kaiser+Employee+Data+Breached+Identity+Theft+Reported/article14196.htm

[4] Sherry Jacobson, Dallas News Laptop theft at Parkland Memorial Hospital could imperil employee information, 09 Feb 2009, http://www.dallasnews.com/sharedcontent/dws/news/localnews/stories/021009dnmetparkland.3574199.html

[5] Rosamond Hutt, The Independent, MoD stunned by massive data loss**, 10 0ct 2008,** http://www.independent.co.uk/news/uk/home-news/mod-stunned-by-massive-data-loss-957099.html

disposed of at the end of its useful life is one of the primary causes of the ongoing issues.

2. FINDINGS

Research has been carried out during the last four years to determine the levels and types of information that individual home users and organisations have inadvertently made available to the public when they have disposed of computers and hand held devices. The hand held devices looked at in the research included devices such as mobile (cell) phones, RIM Blackberries and PDAs that contain either disks or solid state storage. This research has been undertaken by a partnership between industry and academia that has been led by British Telecommunications with academic partners at Edith Cowan University in Perth, Australia, the University of Glamorgan in Wales and Longwood University in Virginia, USA.

Over the four year period of the study more than 1000 disks have now been examined together with 160 hand-held devices. The results of the research have provided an insight into the consistently poor level of protection that organisations and individuals give to the information that is contained within them when they dispose of these types of equipment.

The purpose of the research was to obtain a better understanding of the volumes and types of information that were left, in an easily recoverable form, on magnetic media that was offered for sale on the second hand market.

Prior to this research, there had only been limited journalistic reporting on the problems that had been associated with the incorrect disposal of data. One of the earliest known reports was from 1993 when there was an article in the Canadian Globe[6] relating to the discovery of a computer hard disk that was reported to contain information on the employees of a small company. Another article in 2000 in the UK Daily Express reported the discovery of banking information regarding Sir Paul McCartney[7].

There had also been limited academic research on the subject, including a paper by Garfinkel and Shelat in 2003[8]. However, there had been no long-term scientific investigation to determine whether the issues relating to the problems regarding the safe disposal of equipment were changing in response to the developing technical and regulatory environments. The disk studies over the last four years have focussed on the levels and types of information that have been found on computer disks that were obtained on the second hand market in a number of countries. The hand held device research took place for the first time in 2008. This was in response to the realisation that the increasing processing power and storage of these devices means that there was a possibility that they were subject to the same issues of unsafe data removal as computers.

The results of the research have been widely reported and publicised, but indicate that little has changed with regard to the level and type of information that is being found on the media and devices. During the research the only tools that were used to gain access to the data on the disks were those that are commonly available and could be used by any competent computer user. For the mobile devices, the tools used were the software that was available from the device manufacturers and free tools.

Throughout the research period, the information that has been found came from a wide range of sources, including government, the financial sector, the legal profession, academia, healthcare, the automotive, agrochemical and other industries, the leisure sector, the retail sector and individual's personal computers and devices.

The results of the study revealed that information from which the organizational that had previously

[6] Canadian Globe and Mail (1993), Disk Slipped Into Wrong Hands, *Canadian Globe and Mail*, 2nd August 1993

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

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

owned the disks could be identified was recoverable from 52 percent of the disks and that information from which an individual could be identified was recoverable from 51 percent of the disks (some of the disks contained both personal and organization information). Only 31 percent of the disks in the study had had the data deleted to a standard where it could not easily be recovered.

In the study into the data that could be recovered from hand held devices the results showed that while no data could be easily recovered from 51 percent of the devices, 23 percent of the devices that were working and could be accessed contained organizational information and 19 percent of the devices contained personal information.

One example of the type of data that was recovered was patients' records of individuals that were being treated for cancer that had been left on the disk from a computer that originated at a healthcare organisation. The psychological damage that the publication of this type of information may have had on the individuals concerned could have been significant.

Another example that came from a disk that was acquired in France that appears to have originated from the Embassy of another European Country. This disk came from a Linux system and contained corporate information relating to 'Cidale' (*Centre for Information and Documentation*) belonging to the Embassy which is located in Paris. This disk contains a wide range of material including details of the network configuration and security data, internal IP addresses, security logs, a domain key for Dotnetflux and the minutes of internal meetings.

Yet another example was disk that was obtained in the USA contained documents relating to Test Launch Procedures from a Government Contactor. Also on the disk were a number of design documents, documents relating to the subcontractor, security policies, blueprints of facilities and personal information on employees and SSN.

A disk obtained in the USA contained information relating to $50 Billion currency exchange proposals that referred to a 15% transaction fees. The currency exchange was between US dollar and Spanish Euros and there were also million dollar bank transfer documents. The disk also contained information including bank account numbers and details of business dealings in a number of countries including Venezuela, Tunisia, and Nigeria. Amongst the information recovered was correspondence from an individual that appeared to be a member of the US Federal Reserve Board which suggested that the acquisition of a Bank Guarantee might not be forthcoming because of some 'questionable' circumstances.

The potential damage that would be caused by this type of information being available to anyone who cares to look for it, without them having to invest any significant effort or specialised tools, could be serious for any organisation or an individual. For a business, the exposure of information such as their current business plans to a competitor could have a detrimental effect on the business's potential profitability or future. For an individual it could lead to identity theft, embarrassment and exposure to potential blackmail attempts.

3. ENVIRONMENTAL FACTORS

There are a number of factors that contribute to the failure to destroy or effectively remove of data from computer hard disks and hand held devices. One is that the storage capacity of computer disks has continued to increase over time at a rate that is close to exponential (exponential growth is described in Moore's Law). Evidence of this has been observed over the period of the research. The storage capacity of the disks purchased over the period has increased from an average of between 20-40Gb in the first year to between 200-300Gb in the past year. Another is the changing use of laptop computers and handheld devices, where there has been an increasing demand for devices that support an increasingly mobile population. A third factor has been the greater availability of high quality and the increasing speed of mobile communications which have developed to support the demands for computing capability on the move.

These have all contributed to increasing volumes of data being transmitted and stored on an ever wider range of devices. One effect of the increasing availability of storage capacity has been that people both in their employment and in private use have been less likely to destroy data that is no longer required in order to maintain storage space on the media.

4. LEGISLATIVE CHANGES

As the computing and networking technologies have developed to provide new and enhanced capabilities, legislation such as the California state law on disclosure and the UK Data Protection Act has been introduced to meet the changing environment. An effect of the new legislation is that any organisation that holds information from which a person can be identified is now required to have put measures in place to adequately protect the information. Organisations in many sectors such as Government, finance and healthcare also have sector specific regulations, such as the Basel II accord for the financial sector and HIPPA for the healthcare sector. Other regulations such as the Sarbanes Oxley Act have been introduced to improve corporate accountability, but these also have a beneficial effect in the protection of sensitive information. These legislations and regulations have been developed to ensure that the measures that are put in place for the protection of information are adequate and that suitable audit measures are used to ensure that the measures are being followed.

5. CAUSES OF FAILURES

The research and follow up activity with organisations and individuals that could be identified from the recovered disks and devices identified a wide range of reasons for the data being released to people not intended to have access to it. Amongst the most common causes that were isolated were the theft of the device, accidental losses, failures in procedures and negligence. The main cause of the failure to properly dispose of the information in most organisations was attributed to poorly worded and managed third party arrangements where a disposal or recycling company had been contracted to dispose of the equipment and remove the data. In all of the cases that were investigated, there were arrangements in place by the organisation for the third party to destroy the data. In a small number of cases the third party had failed to take any action to remove the data. However, in most of the cases, the third party had fulfilled this requirement to destroy the data from the devices by the use of the Windows format command or a tool that had a similar effect. The underlying causes of this problem were twofold: First, the wording of the contract with the third party did not specify the standard to which the data should be destroyed; Secondly, the organisation did not have in place measures to test that the destruction of the data had been effectively carried out to the required standard.

Any competent information security professional and most competent computer users would know that the use of the Windows format command does not actually destroy the data, it only removes the file structure which is normally used to access it. In an attempt to support users who make mistakes, Microsoft also created an Unformat command which allows the file structure to be recreated with relative ease. While it could not be proven during the research and subsequent follow up investigation, it is clear that the actions taken by some recycling companies have clearly met the contractual requirements of the disposing organisation (destruction of the data to an unspecified standard). The fact that the data could subsequently be recovered appears to be a result of them carrying out their contract in the most cost effective manner (in terms of the cost of specific tools and manpower. It is known that for central government and a number of other organisations, the contracts with the third party recycling organisations mandate the use of specific tools and processes for the destruction of data on media and devices and include the right to inspect the processes and test their effectiveness.

For disks and devices from private individuals, the main reasons for the failure to adequately destroy the data was that of ignorance of the potential value of the information that was contained in them or the potential impact and a lack of technical knowledge. The majority of private users do not have easy access to the knowledge, skills and tools that could be used to adequately destroy the data.

RECOMMENDATIONS

From the research there were a number of measures identified that can be taken to ensure that information is destroyed effectively and does not end up in the public domain. For computer disks, the measures include:

- Education of users - Public awareness campaigns by Government, academia, the media and within organisations.

- Best Practice - The development of best practice within sectors and its adoption by organizations to ensure that computer hard disks are disposed of in an appropriate manner.

- Risk Assessments – Organisations need to carry out risk assessments to determine the sensitivity of the information on computer disks and determine the measures that need to be taken for its effective removal.

- Tools– The development of, and access to, data erasure tools such as Blancco[9] and access to facilities to enable individuals to effectively remove the information from their computers.

- The use of Encryption - The full or partial encryption of hard disks to protect sensitive information and to ensure that, in the event of the disks being released into the public domain, information could not be easily recovered. The types of tools that can be used to achieve this include software such as TrueCrypt[10] or PGP whole disk encryption[11] or hardware encryption devices such as the Secure Data Vault[12].

- Asset Tracking - organisations could improve the effectiveness of the security of their data if asset tracking is conducted at the hard disk level. This would require that asset tags are placed on individual disks rather than the computer system unit to ensure appropriate disposal.

- Allocation of responsibilities – Responsibility should be assigned to all of those involved in the process of the disposal of hard disks, including those that are damaged or have failed. Disks that are not working or faulty should have the same disposal practices applied to them as disks that are working correctly.

- Physical Destruction - Where appropriate, if the sensitivity of the data demands it, the physical destruction of the disks using services such as the Ultratec Secure Data Erasure service[13] or that offered by DataTerminators[14] should be considered.

[9] Blancco - http://www.blancco.com/en/frontpage/

[10] TrueCrypt - http://www.truecrypt.org/downloads.php

[11] PGP Corporation, Whole disk ensryption - http://www.pgp.com/products/wholediskencryption/index.html

[12] Secure Systems Secure Data Vault - http://www.securesystems.com.au/

[13] Ultratec Limited - http://www.ultratec.co.uk/

[14] DataTerminators - http://www.data-terminators.co.uk/

For mobile devices such as PDAs or mobile (cell) phones, the measures that should be considered include:

- Education of users - Education and awareness training should be developed and delivered to improve user awareness.
- Development of Best Practice – The development within organizations of best practice for the appropriate disposal of the information on mobile devices.
- Data Erasure Tools – Ensure that access is available to the tools and instructions such as model specific data removal information[15] for the appropriate removal of data from hand held devices.
- Contracts – Ensure that the chosen recycler[16] or organisations[17] that accept donated hand held devices guarantee that the devices are data cleansed before they are sold on and have procedures in place to ensure that they are carried out.

In isolation, it is unlikely that these measures will reduce the level of risk of the potential exposure of sensitive information to the individual or an organization. It is only when the appropriate measures are used together that any significant change is likely to occur.

FUTURE WORK

It is planned that this research will continue into both the computer disks and hand held devices. The research into computer hard disks will continue unchanged, but future research into hand held devices will be concentrated on 2.5 and 3G devices, RIM Blackberries and PDAs. The reason for this change is that the initial research has determined that the risk of information loss from 2G devices low due to their limited functionality and storage capacity. In addition, these devices will be progressively replaced by the more function rich 3G type devices.

[15] Recellular Free Data Erasure tools - http://www.recellular.com/recycling/data_eraser/default.asp

[16] PHS Datashred - http://www.recyclemycomputer.co.uk/recycle-mobile-phones.htm

[17] Birmingham Focus on Blindness - http://www.birminghamfocus.org.uk/html/display.php/id/419