THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 3 | Number 2 Article 4

2008

Analysis of Information Remaining on Hand Held Devices Offered for Sale on the Second Hand

Andy Jones
Information Technology Futures Research Centre, BT

Craig Valli
Edith Cowan University

Iain Sutherland
University of Glamorgan

Recommended Citation

Jones, Andy; Valli, Craig; and Sutherland, Iain (2008) "Analysis of Information Remaining on Hand Held Devices Offered for Sale on the Second Hand," *Journal of Digital Forensics, Security and Law*: Vol. 3 : No. 2 , Article 4.
DOI: https://doi.org/10.15394/jdfsl.2008.1041
Available at: https://commons.erau.edu/jdfsl/vol3/iss2/4

Analysis of Information Remaining on Hand Held Devices Offered for Sale on the Second Hand Market

Dr. Andy Jones[1,2]
Dr. Craig Valli[2]
Dr. Iain Sutherland[3]

[1]Information Technology Futures Research Centre, BT
[2] Edith Cowan University
[3] University of Glamorgan

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

ABSTRACT

The ownership and use of mobile phones, Personal Digital Assistants and other hand held devices is now ubiquitous both for home and business use. The majority of these devices have a high initial cost, a relatively short period before they become obsolescent and a relatively low second hand value. As a result of this, when the devices are replaced, there are indications that they tend to be discarded. As technology has continued to develop, it has led to an increasing diversity in the number and type of devices that are available, and the processing power and the storage capacity of the digital storage in the device. All organisations, whether in the public or private sector increasingly use hand held devices that contain digital media for the storage of information relating to their business, their employees or their customers. Similarly, individual private users increasingly use hand held devices containing digital media for the storage of information relating to their private lives.

The research revealed that a significant number of organisations and private users are ignorant or misinformed about the volume and type of information that is stored on the hand held devices and the media on which it is stored. It is apparent that they have either not considered, or are unaware of, the potential impact of this information becoming available to their competitors or those with criminal intent.

This main purpose of this study was to gain an understanding of the volume and type of information that may remain on hand held devices that are offered for sale on the second hand market. A second aim of the research was to determine the level of damage that could, potentially be caused, if the

information that remains on the devices fell into the wrong hands. The study examined a number of hand held devices that had been obtained from sources in the UK and Australia that ranged from internet auction sites, to private sales and commercial resellers.

The study was carried out by the security research team at the BT IT Futures Centre in conjunction with Edith Cowan University in Australia and the University of Glamorgan in the UK. The basis of the research was to acquire a number of second hand hand held devices from a diverse range of sources and then determine whether they still contained information relating to a previous owner or whether the information had been effectively removed. The devices that were obtained for the research were supplied blind to the researchers through a third party. The 'blind' supply of the devices meant that the people undertaking the research were provided with no information about the device and that the source of the devices and any external markings were hidden from them. This process was put in place to ensure that any findings of the research were based solely on the information that could be recovered from the digital storage media that was contained within the device.

The underlying methodology that was used in the research was based on the forensic imaging of the devices. A forensic image of a device is a copy of the digital media that has been created in a scientifically sound manner to a standard that is acceptable to the courts. This procedure was implemented to ensure that the evidential integrity of the devices was maintained, with the devices also then being stored in a secure manner. All subsequent research was then conducted on the image of the device. This was considered to be a sensible precaution against the possibility that information discovered on a device might indicate criminal activity and require the involvement of law enforcement. Following the forensic imaging of the devices, the images that were created were then analysed to determine whether any information remained and whether it could be easily recovered using commonly available tools and techniques that anyone who had purchased the device could acquire.

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

1. INTRODUCTION

In each of the last three years, studies have been carried out into the level and type of information that remains on computer hard disks have been offered for sale on the second hand market [1,2,3]. The results of this research revealed that significant volumes of information remained on them and with the increased use of hand held devices and the processing and storage capabilities, it was logical to examine whether information was also left on the digital storage media of these devices and if so, the nature of the information that could be recovered.

There has been a significant level of reporting in the newspapers [4,5,6,7] on the level of information that has been lost as a result of errors, accidents and thefts and of the potential problems and costs to the individual of identity theft.

The UK government is expending considerable resources on schemes such as Warning, Advice and Reporting Point (WARP) [8] and IT Security Awareness For Everyone (ITsafe) [9], both of which are aimed at improving information security and security awareness

There are numerous tools available to enable the effective removal of data from computer hard disks and it can be suggested that any data remaining on them can be attributed to poor information security policies, errors or ignorance. However, the situation with regard to hand held devices is significantly more complex.

2. HAND HELD DEVICES

For the purpose of this paper, the term hand held device is used to describe mobile (Cellular) phones, Personal Digital Assistants (PDAs) and Blackberry (RIM) devices. All three types of device will be discussed, however, in this research, only mobile phones and Blackberry devices were examined. While mobile phones are referred to as a generic group, the group is actually made up of devices that are from four separate groups. These are:

First Generation. The first commercially available mobile phones, these systems used analogue radio signals to transmit information. These were bulky devices, characterised by large batteries that were required because of the high power consumption required for analogue transmission.

Second Generation - Global System for Mobile communications (GSM) (2G). This was the next development in mobile telephony and transitioned to the use of digital signals, as these required less battery power and as a result, allowed for an increase in the talk time available and for smaller batteries. A secondary advantage of the use of digital signals was that it provided clearer signals. The 2G mobile phone was very good at transmitting voice calls, but had limited capability for transmitting or receiving data. The system uses a system known as CSD (Circuit Switched Data) to transfer data. CSD requires the phone to make a special connection to the network before it can transfer data, in a manner similar to that for making a voice call. Once connected, the user is billed for the time it takes to send the data and the transfer rate is relatively slow: 14.4 kbps (kilobits per second) for GSM 1800 networks (Orange and T-Mobile) and 9.6 kbps for GSM 900 networks (Vodafone and O2).

Second Generation Plus (2.5G). A development used to increase the flexibility of the 2G technology, with enhanced features comparable with those found on third generation (3G) phones, such as data transfer, GPRS (General Packet Radio Service) radio and EDGE (Enhanced Data rates for

GSM Evolution) capabilities.

Third Generation (3G). This is the new network providing greater efficiency than the 2G standard and allow for much greater data transfer speeds, typically, in the range of 5-10 Mb per second. This innovation allows for data such as video clips and music tracks to be downloaded. Services that are available through 3G include wide-area wireless voice telephony and broadband wireless data, all in a mobile environment.

The Research In Motion (RIM) Blackberry device is wireless hand held device that supports both voice and data communications. The device supports a range of services that includes mobile telephony, text messaging, web browsing, push e-mail and internet faxing. The device is one example of a convergent device, which together with the data services detailed above, is also capable of what are typically considered to be Personal Digital Assistant (PDA) type applications such as address book, calendar, to-do lists, etc. Some of these devices are not dependent on mobile phone service coverage and are capable of using the Wi-Fi system to connect to a network if required.

This paper assesses the information available on 1G and 2G devices as no 2.5 or 3G phones were easily available on the second hand market at the time that the devices were acquired.

3. THE DISPOSAL OF HAND HELD DEVICES

The relatively short life cycle of a mobile phone (as little as 12 months for a privately owned phone and approximately 24 months for a corporately owned device) means that there are a large number of used devices that are considered to be 'obsolete' and they may still contain relatively recent information at the point of disposal. Modern hand held devices contain some form of storage media, usually built into the device and possibly supplemented in the form of a removable memory card. In the latter case, these may have a significant capacity, as they are increasingly used for the storage of digital images, often from a built-in camera, music tracks and other files. Devices that have either an inbuilt capacity or are capable of supporting external memory storage devices of between one and eight gigabytes are not uncommon.

The disposal of obsolete hand held devices does not appear to be a subject that some organisations have given a great deal of consideration to in the past [10] . The situation is made more complex as most of the devices are provided by a supplier as part of the mobile communications service and the devices are not generally considered to have any intrinsic value to the organisation. When they reach the end of their effective life, in most cases somewhere between one and two years, they have little or no residual value and do not appear to be given any consideration with regard to the data that they may still contain.

Many large organisations currently dispose of obsolete mobile phones by

donating them to charities, which the charities then use them to generate revenue. It was discovered during the course of the research that a number of the organisations that the charities sell the mobile devices to have two main markets for the devices. The resellers identify their main markets as export to China and Nigeria, which are both regarded as areas posing a high threat to the security of information.

In addition, whereas the process for the disposal of computers is normally covered by the information security policies and procedures of the organisation, mobile phones, to date, have not normally been addressed. With the disposal of computer equipment, the removal of residual data can be addressed by the use of processes and procedures for the cleansing of the media using available tools. In the case of hand held devices, the problem is significantly more complex. The types of media that are used in mobile devices and the range of operating systems are considerably more diverse, for example Symbian, Widows Mobile, Linux. In addition, while computer hard disks have a limited number of standardised power and data interfaces, hand held devices have a huge range of both type of interface and they are changed by the manufacturers at regular intervals.

When a hand held device is sent for disposal, it is unusual for either the power or the data connector cables to be sent with it. As a result, any attempt to examine the device and securely remove data will only be possible from a centre that is well equipped and has the data and power connectors and the relevant software available. As a result, for a device with no residual intrinsic value, the likelihood of data cleansing taking place is low.

Organisations either have to adopt policies and procedure to clean and dispose of obsolete devices through their internal resources or obtain the services of a third party that would dispose of the devices on their behalf. If an organisation uses the option of employing a third party to undertake the data erasure from a hand held device, it is important that they also, periodically check that the procedures employed by that third party are adequate to remove the data to a standard that is acceptable to the device owners. If not, there is a likelihood that the hand held devices will sold on and be re-circulated in the public domain with some or all of the data present on the device and that it will be available to anyone using the manufacturer supplied backup and synchronisation tools. The final option for the safe disposal of the devices, which is the least satisfactory from a recycling or green perspective, is to destroy them, either through incineration or mechanical destruction. This has the issues of depriving the charities of potential income and also of not recycling equipment that is still of use, both of which will become increasingly unpopular in the future where it is increasingly seen as unacceptable for electronic devices, as indicated in the EU directive on Waste Electrical and Electronic Equipment (EU 2002/95EC).

For the individual, private device user, the options are similar. The choices are to either remove the data themselves, using the advice and information that is available (from a limited number of websites such as Wireless Recycler [11], or to find an organisation that they feel that they can trust to remove the data before they recycle the devices.

4. ANALYSIS OF CURRENT DISPOSAL PRACTICES

The research was undertaken to determine the type and volume of information that could be retrieved from hand held devices that were for sale on the second hand market. The results were based on the examination of 161 hand held devices that were supplied blind (the researchers had no foreknowledge of where the hand held devices had been obtained) to the research for the experiment. When the research was completed, the third party then supplied the researchers with the list of the sources from which the hand held devices had been purchased. The sources of the hand held devices included an on-line auction site, commercial organisations involved in the supply of second hand hand held devices and public auctions.

The devices that were supplied to the researchers were identified with a single sequential serial number. In order to maintain the integrity of the devices, in case they were required for further research, they were then forensically imaged and the subsequent analysis was carried out on the images. Tools, such as Paraben Device Seizure, XRY and the Susteen DataPilot Mobile Phone Forensic toolkit software were used for the imaging of the devices. The tools that were used for the analysis were the manufacturer's desktop interface and management software and hex editors, tools that any competent computer user would have access to and be able to use.

Of the 161 hand held devices used in the research, 82 could not be imaged as they were found to either have been physically damaged, had power problems as a result of batteries that were missing or had failed or were inaccessible as the data or power connectors could not be obtained. This research did not attempt to use more sophisticated tools or techniques as the research was aimed at identifying what information would be available to a reasonably competent and knowledgeable user with standard equipment and facilities. The 79 images created from the devices that could be accessed were used for the analysis. A number of specialised tools were used by the researchers, but to ensure forensic soundness and repeatability of the processes so that in the event of information being found that was related to criminal activity, any evidence was not contaminated.

The analysis of the hand held devices was carried out in a number of stages. The first was to determine whether or not the hand held device had any data that could be seen during an initial examination. This involved the simple step of loading the image of the hand held device and looking to see if there was any data present in the predetermined fields. Of the 79 hand held devices for

which images were successfully made, 36 were found to have data present. In three of the devices the SIM cards were still present. This was a cursory examination of the image to determine whether there was easily recoverable data present on the device that did not require the use of further tools or techniques. Further investigations were then undertaken into each of these hand held devices.

The second part of the analysis was to look for specific information that would allow for the identification of the user and their parent organisation. The device was also examined for further information such as the usernames, email addresses or documents, spreadsheets and databases. The purpose of this phase of the research was to determine the proportion of the devices that could be traced to an individual and also to the organisation.

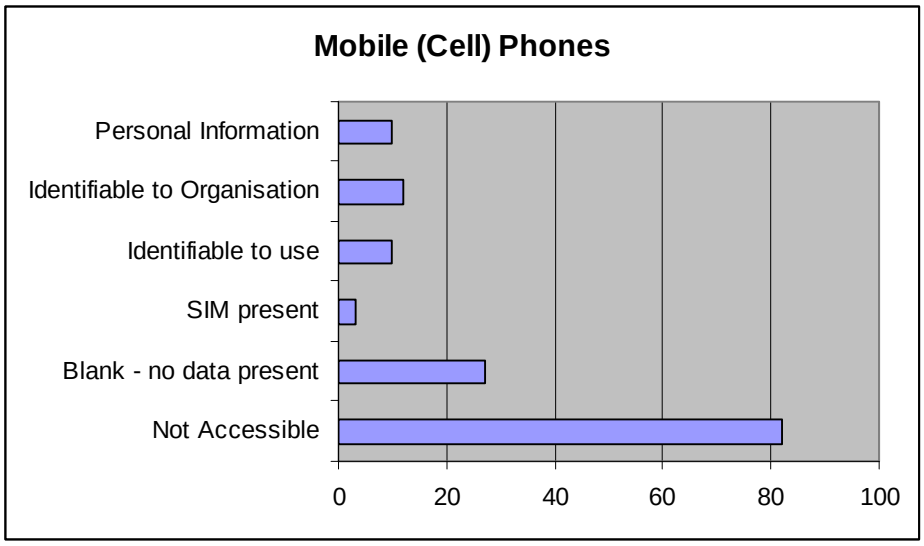
The results of the research were that, of the 135 mobile phones that were examined the following was revealed:

> Inaccessible due to device broken, battery not charging or no suitable connector cable: (82) 61% of the mobile phones were damaged, had batteries missing that could not be replaced or data connection cables could not be acquired for them. A number of the phones were extremely old 1G devices and power supply leads, batteries and data leads are no longer readily available.
>
> Blank: (27) 20% of the mobile phones contained no data that could be recovered using standard tools.
>
> SIM Present (3) 2% of the mobile phones still contained the SIM that the previous user had used.
>
> Identifiable to a user: (10) 7% of the mobile phones contained sufficient information to be able to identify the user of the device (phone number, address, user name).
>
> Identifiable to organisation: (12) 9% of the mobile phones contained sufficient information for the organisations to be identified.
>
> Personal Information: (10) 7% of the mobile phones contained information from which individuals could be identified. This information included SMS messages, greetings logos, address book entries and call histories.

Table 1 shows a comparison of the results for the mobile (cell) phones.

It became clear that while there is the potential for a level of data leakage from 1G and 2G mobile phones, it is limited. Information such as address books/contact lists might be lost as well as a number of SMS messages, but the loss of a significant volume of sensitive information is unlikely. Although no 2.5 or 3G phones were included in the research, it is thought that the potential for the loss of sensitive information will increase as the use of these devices becomes more widespread.

Table 1: Results from analysis of mobile (cell) phones.



The results of the research were that, of the 26 Blackberry devices that were examined the following was revealed:

Not working: (0) 0%. All of the devices were in working order.

Inaccessible due to device being encrypted: (7) 27%. While this figure seems to be low, it was apparent from the analysis that a significant number of the other devices that were examined has been cleared of data and reset. These devices had the common feature of 3 default messages being held on the system, one from the service provider and two from Blackberry. It was not possible to determine whether these devices had been encrypted before they were reset.

Blank: (10) 38% of the Blackberry devices contained either no data or only the default messages that are sent to all systems of this type.

Identifiable to a user: (4) 16% of the Blackberry devices contained identifiable usernames.

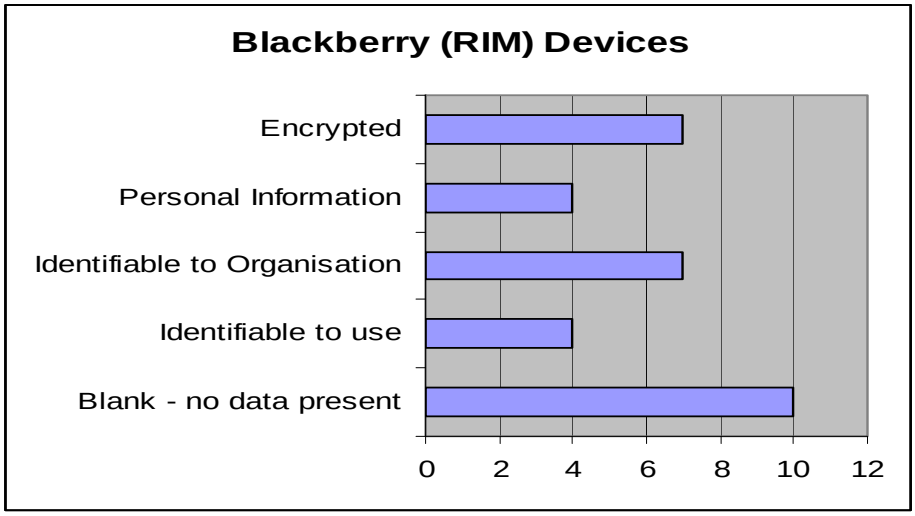
Identifiable to organisation: (7) 27% of the Blackberry devices contained sufficient information from which the organisations could be identified.

Comment: In a number of cases, this was actually not a shortcoming in the measures and procedures that had been implemented. When the devices were turned on, a number of them had been set up to display the ownership information on the first screen, a measure that has been adopted by some of the organisations to enable the recovery of the device if it is lost or misplaced.

Personal Information: (4) 16% of the Blackberry devices contained information from which individuals could be identified.

Table 2 shows a comparison of the results for the Blackberry (RIM) devices.

Table 2: Results from analysis of the Blackberry (RIM) devices



The level and types of information that was found on the hand held devices and the range of information that was available resulted in the individual owner and the organisation that they belonged to being easily identifiable in many cases. It became very clear at an early stage in the research that RIM Blackberry devices that had not been encrypted created a huge potential information leakage threat to both the individual and the organisation.

In one example, a device was examined that had been used by the sales director for Europe, the Middle East and Africa (EMEA) of a major Japanese corporation. It was possible to recover the call history, the address book, the diary and the messages from the device and the information that was contained in these provided:

- Information that enabled the structure of the organisation and responsibilities of individuals to be determined.
- The business plans of the organisation for the next period
- The identification of the main customers and the state of the relationships with them to be determined
- The travel and accommodation arrangements of the individual
- The relationship of the individual with their support staff

- Details of the personal life of the individual including family details including children and their occupations and movements, marital status, address, appointments and addresses for dental and medical care, domestic arrangements and dining and sporting activities.
- Bank account numbers and bank sorting code
- Car registration index

From this one device, it was possible to recover 249 address book entries, 90 email addresses and 291 emails.

A second Blackberry device had originally belonged to an employee of a financial sector company; a superannuation organisation. The device contained emails related to the farming community, a medical appointment, meetings, bereavement, performance reviews and also contained 19 names and addresses and call history.

A third Blackberry device belonged to an employee of another financial sector company, a superannuation organisation. The device contained emails related to the owner's identity and a change of their name, details of board meetings, meeting accommodation details, applications for the post of office manager, and comments on the suitability of the named and identified applicants and flight details.

While the last two of the devices detailed above did not contain a significant volume of information, they both originated in the financial sector and both contained details of a personal nature of the owner and other individuals that would have caused embarrassment or distress if it had become publicly known. The implications of the information on these devices becoming available to individuals who might make use of it for a range of illicit activities could potentially, have devastating consequences for an organisation or an individual. The potential cost of these data losses, both in financial terms and to the reputation of the organisation or the individual, could be high and it is clear that additional effort needs to be expended to ensure that this information is protected.

The loss or disposal of hand held devices that still contain significant amounts of information is not a new problem. In the year 2005-06 it was reported [12] that around 800 thousand mobile phones were stolen in the UK. A separate report from the insurance industry [13] covering the same period indicated that the number of phones stolen in the UK was closer to 1.3 Million and that the number reported lost was in the region of 1.6 Million.

5. POTENTIAL IMPACT

The potential implications for both the organisation and the individual of the information contained on the hand held devices being made available through either a lack of policy for the secure disposal of such devices within

organisations or a breakdown in security of the procedures for their disposal are significant. The most noteworthy ways in which such sensitive information might be exploited for are discussed below.

Industrial Espionage. For all of the hand held devices that could be identified as having originated in a commercial organisations, the potential cost of the information leakage is high. This is exemplified by the information recovered from the Blackberry device that had belonged to the employee of the Japanese company that contained information of business plans, staff and competitors, all of which would be of use to a competitor and the release of which is a potential embarrassment to the company.

Identity Theft. For the hand held devices that could be identified as having originated in an organisation or from an individual, there were a number that contained sufficient information to make it possible to carry out either identity theft or cloning. The type and volume of personal information varied, but in the majority of cases included names, addresses, telephone number and email addresses, together with contact lists, diaries and SMS and email texts.

Research that has been conducted in the USA gives estimates of the number of people that have suffered some form of identity theft as high as 10 Million people and the cost to business and consumers at approximately $53 Billion in the USA alone [14]. The same research estimated that the cost of 'repairing' an individual's identity was approximately $808 for each incident and around 175 hours of effort. It is estimated that the average monetary loss as a result of an identity theft is $31,356. A report produced by the Cabinet Office on data from 2002 in the UK puts the cost of identity theft at £1.3 Billion [15] and estimated that, in the UK, an identity will be stolen roughly every four minutes. The figures relating to the cost were updated in 2006 and the new estimate was £1.72 Billion [16]

Fraud. From the Blackberry device identified as having originated in the UK office of a Japanese organisation, there was sufficient information/data available to allow fraud to take place. The range and diversity of information that was recovered would be sufficient for a fraudster to either manipulate the information to advantage or to generate false documentation.

In the case of the hand held devices that had come from commercial organisations, there is an issue of the duty of care that they with regard to data that relates to the business and also the individual that had used the device. This is embodied in a range of legislation and standards, the most significant being the Data Protection Act (1998) (DPA) and the requirements for corporate governance that are expressed in regulations such as the Basel II accord or the Sarbanes Oxley and the Gramm-Leach-Bliley legislation from the USA. The relevance of the legislation from the USA is that the regulations apply to all organisations that conduct business with organisations based in the USA. In the UK under the DPA, any organisation that holds data from which an individual

can be identified must, in addition to registering the fact that they hold such data, also ensure that it is only used for the purpose for which it was obtained and that the information is afforded a reasonable and appropriate level of protection.

It is notable that the wording of the DPA that is used specifically requires that information shall 'not be disclosed' and that is 'shall be kept for no longer than necessary' in addition to the requirement for 'appropriate security measures shall be taken against unauthorised access to the data'. Clearly, from the fact that this information ended up on hand held devices being offered for sale on the second hand market, a number of organizations had failed to meet their obligations with regard to this legislation.

In the cases of all the hand held devices that had originated from the commercial sector, it would appear that the organisations have contravened the Data Protection Act and have failed in their duty of care to the business and the individuals. In the case of the two hand held devices that could be identified as having originated from the financial services sector it is probable that they have failed to satisfy one of a range of other items of legislation.

6. SUMMARY

It is clear from the results of the academic research that, in disposing of surplus and obsolete hand held devices, many organisations have failed to recognise their legal and statutory responsibilities and have not used good business sense. Once an obsolete hand held device leaves the control of the organisation then, if there is not a contract in place with a reputable organisation to ensure that the devices are purged of data, and the process has not been carried out within the organisation, the potential consequential loss of information is inevitable.

For the privately owned hand held device, it is not uncommon for them to be kept for a period in the home and then eventually for them to be disposed of by passing the on to a friend or relation, selling them on or donating them to charity. It is clear from the research that the hand held device that were examined that appeared to have come from private users contained a level of information that, while it could be embarrassing, was not sufficient to be damaging to their reputation or finances. However, this situation is likely to change as 2.5 and 3G devices that potentially contain significantly more data appear in greater numbers on the second hand market.

In summary, of the 161 hand held devices that were used during the research, 82 were not working or could not be accessed using the tools available. Of the remaining 79, 37 of the hand held devices contained no user data and on 42 some data was present.

There is a clear difference in the quantity and the types of information that were recovered from a 1G or a 2G mobile phone and that which can be recovered from a Blackberry device. The research revealed that despite the

availability of encryption as a set up option on the Blackberry device, four of them (15%), had not had this security feature enabled.

This failure to take adequate steps to protect the data or to subsequently remove it from the hand held devices has resulted in a number of these organisations not meeting their statutory and legal obligations. It is clear that the level of effort currently invested by an admittedly small, but still significant number of organisations in ensuring that they have removed information from hand held devices that are disposed of is totally inadequate.

7. RECOMMENDATIONS

A number of steps were identified by the research that could be implemented to improve the protection of information stored on hand held devices. The main steps are:

- Education and awareness training for the users.
- A system within the organisation for the secure disposal of mobile devices.
- The wider availability of tools and instructions for the removal of data from hand held devices
- A commitment from the organisations that accept donated hand held devices to ensure that they are data cleansed before they are sold on.

None of these measures, in isolation will improve the level of risk and potential exposure for the individual or an organisation. It is only when they are used in combination that a significant change will occur.

8. CONCLUSIONS

While it is difficult to predict what will occur in the future with any certainty, there is a strong probability that as 2.5G and 3G devices become more widely used, the level of information that is stored on them will increase significantly and the level of risk will more closely match that which currently exists for the Blackberry devices. It is unlikely that 2.5G and 3G devices will gain the same business market penetration, at least until the technologies and markets mature, but they will still pose and information leakage threat for the individual.

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.

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 analysis of the large number of hand held devices required for the research (a non trivial task), in particular, Paul Owens at the University of Glamorgan.

REFERENCES

1. Jones, A., Mee, V., Meyler, C., and Gooch, J,(2005), Analysis of Data Recovered From Computer Hand held devices released for sale by organisations, Journal of Information Warfare, (2005) 4 (2), 45-53.
2. Jones A., Valli C., Sutherland I.,Thomas P., The 2006 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market, Journal of Digital Forensics, Security and Law, Volume 1, Issue 3, 2006.
3. Jones A., Valli C., Dardick G., Sutherland I., The 2007 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market, Journal of Digital Forensics, Security and Law, 2008.
4. Young, T., HMRC breach warning to all departments, says watchdog, Computing, 21 Nov 2007.
5. Young, T., M&S breached Data Protection Act, Computing, 25 Jan 2008.

6. Choudhury, A. R., Local firms worried by data loss from mobile devices, The Business Times, 12 Nov 2007, http://www.asiaone.com/Business/News/SME+Central/Story/A1Story20071115-36895.html.
7. Ticehurst, J, Corporate data loss explodes on mobile devices, Information World Review,25 Nov 1999 http://www.iwr.co.uk/vnunet/news/2110216/corporate-loss-explodes-mobile-devices.
8. The WARP website, http://www.warp.gov.uk/ (accessed 20 May 2008).
9. ITSafe Website, http://www.itsafe.gov.uk/.
10. Cauley, L., Cellphone users complain about 'function fatigue', USA TODAY, 13 Feb 2007.
11. Wireless Recycler Website, http://www.recellular.com/recycling/data_eraser/default.asp.
12. HM Stationary office: Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (Supplementary Volume 2 to Crime in England and Wales 2005/06), Edited by John Flatley, 15 May 2007.
13. Free Mobiles 2U: Mobile Phone Safety Information, http://www.free-mobiles2u.co.uk/mobile_phone_safety_information.htm.
14. FTC totals cost of identity theft: $53 billion, 27 million victims, USA Today, 3 Sept 2003.
15. Home Office Identity Theft Steering Committee,2002 Cabinet Office Study,http://www.identity-theft.org.uk/faqs.html.
16. Editorial Team, The office - a hub for ID theft:15.3 million office workers in the UK may become victims of identity theft by over-trusting their colleagues, Insidemoneytalk, 10 Apr 2008, http://www.insidemoneytalk.com/news/she/she108.html.

AUTHORS

Dr. Andy Jones is the Head of Information Security Research at the IT Futures 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. 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.