ELSEVIER

COMPUTER FRAUD & SECURITY

ISSN 1361-3723

March 2005

Featured this month

Organizations discard computers with vital IP on disks

More than 100 disposed disks, that were released from random organizations for reuse or recycling were analysed by University of Glamorgan for sensitive data. The disks were scrutinised to reveal if there was any important information left on the disks that could link the discarded equipment to an organization, reveal usernames or financial data. The researchers managed to link more than half of the disks easily to the organization's of origin. These included a pharmaceutical company, a major leisure services company, a university and a school. The findings were alarming and potentially devastating to an organization or individual. Some of the disks contained enough valuable information to enable industrial espionage, identity theft, fraud, blackmail or network intrusion. A disk from a major leisure service company came from the finance department and gave a very accurate financial forecast, which would be of great interest to a competitor or financial analyst. **Turn to page 4...**

Choicepoint: sued, defrauded and share price quartered

Choicepoint has suffered a major fraud, been hurt by a painful share plunge and now its executives are being investigated by the SEC.

The share price of Choicepoint, the US data aggregator, has plunged by 20% due to the discovery of an elaborate identity fraud. Shareholders have responded to the drop by filing a class-action lawsuit against the company and its executives.

The cause of the downfall? — a group of identity thieves who set up fake companies and registered as Choicepoint customers to obtain vast amounts of confidential US citizen data last year. Social security numbers and place of birth details enabled the fraudsters to commit identity theft.

In response, Choicepoint is withdrawing the sale of citizen information that contains sensitive data except where it is of direct benefit to consumers.

Choicepoint CEO, Derek BV Smith said "We apologise again to those consumers who may be affected by the fraudulent activity." The identity attacks against people are still being investigated.

To try and rectify matters further, the company has created an independent office of Credentialing, Compliance and Privacy that will report to the Board of Directors' Privacy Committee.

Despite the positive efforts to clean up the mess, the company is also being investigated by the Securities and Exchange Commission for hasty share sales. The SEC are probing stock sales by CEO, Derek Smith and president, Douglas Curling for a $16.6 million profit after they allegedly learnt of the data security breach at Choicepoint.

Contents

Editorial office:
Elsevier Advanced Technology
PO Box 150
Kidlington, Oxford
OX5 1AS, United Kingdom
Tel:+44 (0)1865 843645
Fax: +44 (0)1865 853971
E-mail: s.hilley@elsevier.com
Website: www.compseconline.com

Editor: Sarah Hilley

Production/Design Controller:
Esther Ibbotson

02065
Printed by:
Mayfield Press (Oxford) LImited

Al Qaeda buys cyber criminal expertise

John Charlton

Al Qaeda will likely be more active in cybercrime.

That's the warning from Peter Warren, co-author of a recently-published book, Cyber Alert which charts and explains the rise and rise of cybercrime.

"They're trying to recruit experts in [the appropriate] technology to help overcome their money supply issues". Action taken by the authorities since the 9/11 terrorist attacks has stemmed much of the organization's flow of money.

The book says Al Qaeda has turned to organized crime groups for their money laundering expertise. It quotes a Russian cyber crime expert, a Dr Galeotti, who says: 'on the whole they [Al Qaeda] are looking to buy in expertise rather than depend on people they have indoctrinated because it is easier and quicker and there are less links.

'Al Qaeda is paying three times what Russian organized crime is charging the Cosa Nostra, which means paying interest at about 75%.'

The book also claims – quoting a 'senior former intelligence source' – that Al Qaeda recruited 'top-grade' computer experts to hack on its behalf against Western targets.

According to the source, Al Qaeda tried to recruit computer professors from Eastern Bloc countries, with the aim of taking them to African countries, from where they were supposed to hack into key Western targets. These included systems controlling airports and power and water supplies.

Close shave for Japanese bank

Brian McKenna

Israeli police have foiled an attempt to defraud Sumitomo's City offices of £13.9m. They arrested a man who tried to benefit from information got from keylogging software. Yeron Bolondi, 32, is charged with money laundering and deception.

Meanwhile, as recently as 8 March the UK payments body APACS released online fraud figures for the first time. These show that losses due to phishing and key-logging trojans amounted to £12m in 2004 — less than the Israeli's alleged attempted fund transfer.

The *Financial Times* broke the Sumitomo story on 17 March, reporting that rumours of an £220m attempted theft have been circulating in police and corporate circles since late last year.

Takashi Morita, head of communications at Sumitomo in Tokyo, said the company had not suffered any financial loss as a consequence of the robbery attempt.

He said: "The case is still in the middle of investigation so we cannot comment further.

The UK's National Hi-Tech Crime Unit, which works closely with the Israeli police, has been credited by the BBC with the original discovery of a wider plot.

The IT security supplier community was fast to comment. Symantec's Richard Archdeacon said: "We have seen a meteoric rise in cyber fraud that specifically targets confidential data. It's information warfare".

Computer Associates' Simon Perry said: "The use of keystroke logging software in this case, sends a strong message to all companies that anti-spyware technology is now a first line defence against cyber-crime". CA said, in a statement, that this was 'the first recorded instance in the UK of key-logging being used for large-scale online theft'.

Meanwhile, Gary Clark, VP EMEA at Safenet, expressed surprise and intrigue that username and password seemed, in this case, to be good enough for banking security in the City. "If there aren't real moves to two-factor authentication, or putting in PKI infrastructures that is scary", he said. "Moreover, maybe we are only hearing about this because it was prevented".

Police scour Internet for spammers to indict

Sarah Hilley

Law enforcement agencies have uncovered more than three thousand spam cases, in an international investigation which, they say, could lead to court prosecutions.

The spammer trapping exercise, led by international anti-spam effort, the London Action Plan (LAP) covered 26 countries, with the vision of prosecuting spammers under various anti-spam laws.

Christine Wade, Director of UK Consumer Regulation Enforcement said: "We will work in conjunction with our partners from the LAP to enforce the law against spammers."

More than 138,000 messages from trap accounts, spam filters and existing agency accounts were analysed to extract emails, which could merit further investigation.

The Web trawl revealed that the most common categories of spam were spam promoting software and computer equipment, pharmaceutical drugs, porn, financial services and miracle health cures.

UK ISP group, LINX, are supporting the police's spam sweep by hosting a secure website for the exchange of information during the investigation and giving technical advice.

Malcolm Hutty, LINX regulation officer, said, "Spam costs ISPs a considerable amount of money because they have to provide the capacity to carry all this email traffic which the recipients do not want. We are therefore keen to assist overseas law enforcement agencies [defeat spam]."

But very few of the emails handled by UK ISPs come from the UK. This is thanks to strict provisions prohibiting their customers from sending spam. Any customer sending spam via their networks is promptly stopped, warned Hutty. "ISPs that ignore community standards risk losing the co-operation of their peers."

In brief

US Government collude on Microsoft

Government agencies in the USA are now able to improve the security management of any Microsoft products they may use – at no extra cost.

Thanks to an initiative led by the US Air Force, results and information about patch downloads and security issues will be shared with other agencies, hopefully standardizing security and ending discussions on how to configure Microsoft's products across the US Government.

Bank loses tapes for 1.2m workers

US senators and federal workers could have their identities stolen following the alleged theft from the Bank of America of computer data tapes with the personal information of 1.2 million government staff. The lost data included social security numbers and account information for a government credit card programme.

Patrick Leahy, one of the senators whose data was on the tapes, has led calls for a Senate inquiry into the need for more regulation of companies that buy and sell personal data.

Where did all the worms go?

The popularity of worms has dropped thanks to the use of newer Windows systems.

The increase in use of systems such as Microsoft XP alongside firewalls have prevented traditional worms such as Sasser from having the same effect as they did in the earlier part of this decade. The new threat is from email worms and those contained in instant messages. As well as technological reasons for their non-appearance, it is thought that malware spreaders are looking for easier ways to wreak havoc.

ID cards doomed to fail?

A new report published by the London School of Economics has criticised the UK Government's proposals for the planned ID card.

A survey of over 100 academics has damned the proposals as being "too complex" and "technically unsafe", claiming that the costs will be massively over budget and that the objectives can be achieved by other means.

Windows could put power at risk

The increase in use of Windows based systems in power and utility plants is posing a risk to security and opening the doors to hackers.

Recent attacks have seen hotels flooded and gas pipes being taken over for hours at a time. While plants are discarding proprietary systems for Windows due to costs and maintenance, the threat of subversion is increasing as a result.

ID theft gang caught

Twenty-eight people have been charged with perpetrating an online fraud scam that is responsible for the theft of £2 million. Scottish police raided over 40 addresses after months of investigations. It is thought that the gang used simple tricks such as stealing thrown away documents and watching people type in PIN numbers as well as phishing.

Computer Associates code released

Hackers have released code which can exploit a vulnerability in Computer Associates' systems.

The code was released just two days after a patch was issued by CA to cover the hole, which relates to a management tool in their Licence Client and Server software.

Fine for Frenchman's exploit

A Paris court found Harvard University researcher, Guillaume Tena, guilty of publishing a vulnerability and a proof-of-concept virus for Tegam's Viguard anti-virus product on his website. He received a €5,000 suspended fine.

French-born Tena highlighted holes in the French anti-virus product and justified his actions in an online diary. Tegam is now pursuing a €900,000 civil case against Tena.

Brazilian phishing master netted

Brazilian police have arrested the suspected leader of a phishing gang that stole USD 37 million. Valdir Paulo de Almeida allegedly led a phishing group that used a Trojan horse to steal money from online banking customers. Last year more than 50 phishers were arrested.

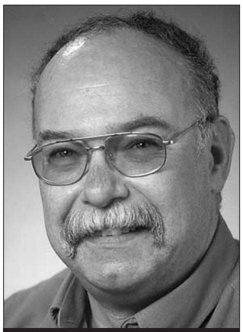
Trusted Computing pushes forward

Dell, HP and IBM have started to sell computers with trusted computing hardware. However, Microsoft technology that will take advantage of the hardware will not be available until the release of Longhorn next year.

Gumshoes track shoe shopper ID thieves

The US Secret Service is hunting hackers who stole the credit card and sales data of customers at 103 of 175 DSW Shoe Warehouse stores owned by Columbus, Ohio-based, Retail Ventures. The firm said the data was stolen over the past three months, but didn't know how many customers were affected.

How much information do organizations throw away?



Dr Andy Jones

Dr. Andy Jones, Security Research Group, BT, Martlesham Heath, UK

The newspapers[1,2,3] have been warning us for some time of the dangers and costs of identity theft and the problems that it causes for individuals that are affected by it. At the same time, the UK Government is publicising initiatives such as Warning, Advice and Reporting Point (WARP)[4] and IT Security Awareness For Everyone (ITsafe)[5] aimed at improving information security awareness. It is therefore somewhat disturbing that recent research from universities in the UK and Australia has revealed that organizations that are entrusted with personal and corporate information seem to be failing to take adequate measures to protect it.

The research was undertaken to determine whether disks that are being sold on the second hand market have been adequately cleaned so as to make it impossible to recover the data that they had held. The results of the research were stunning and revealed that the majority of the second hand disks that were examined had had little or no effort made to remove the data that they contained. The disposal of obsolete computer equipment and the hard disks that they contain has been an increasing burden on most organizations for a number of years. The reality is that when they reach the end of their effective life, in most cases somewhere between 18 months and three years, they have no value and there is actually a cost associated with disposing of them.

In the past, large organizations have been able to 'gift' them to charities and schools, which can, at little or no cost to the organization, both enhance their standing in the local communities and remove a disposal problem at the same time. Unfortunately, now, the liabilities that may be incurred on health and safety grounds have made this impractical. So what can they do with the obsolete equipment? They have a number of choices. The first is to undertake the cleaning of the disks and disposal of the equipment themselves through their internal resources. The next option is that they can find an organization that will take the computers off their hands (normally for a fee) and dispose of them. The third choice, if they have considered the problems and believe that there is a requirement, is that they can employ one of the major, reputable, computer recycling companies that use government approved tools and have reliable and tested procedures in place to ensure that all data is completely removed. The final option, which may seem a draconian step to take, is to remove all data storage media from obsolete equipment and destroy it, either through incineration or mechanical destruction.

All of these options presume that the organization has given some consideration to the problem of data that remains on the obsolete equipment, and this is a reasonable expectation in larger organizations that have dedicated IT and security staff. But what about the smaller organizations that only have a few computers and no dedicated support or security staff? Where can they get advice from and how high on their list of priorities is the disposal of equipment that has no resale value?

How do organizations that use third party companies to dispose of their old equipment know what will happen to it after it leaves their ownership? Do they check that the processes they have in place are effective and that their data is fully wiped from these disks? Are the disks re-circulated into the public domain with the data present on the disk, available to anyone with the most rudimentary skills to read?

All organizations will hold a range of private and sensitive data on their information systems. This will range from employee information such as names, addresses, national insurance numbers, contact telephone numbers, staff numbers and salaries (bank account details) etc; customer information including names, addresses, telephone number, purchase history; business plans; accounts; research information and many other details.

It is clear from the results of the academic research that, in disposing of surplus and obsolete equipment, many organizations are neglecting their legal and statutory responsibilities and good business sense. Once a computer leaves the control of the organization then, if the disks have not been thoroughly cleaned, either through the use of internal or external resources, then the consequential loss of information is inevitable and potentially disastrous.

At the home user level, most people discard their PC's in the conventional manner, in rubbish bins, by selling them on to other private buyers or, in some cases, by trading them in or selling them at auction. They believe that they do not have any data that would be of use to anyone or they have taken steps to "delete" any sensitive files.
It is clear from the research that the small sample of disks examined that appeared to have come from individuals' personal computers contained a

level of information that could be embarrassing to that person or potentially damaging to their reputation or financial standing. There was potentially enough information available from the majority of these disks to allow for identity theft and impersonation or, in two cases, blackmail.

The research that was undertaken was a study to determine the amount of information that could be retrieved from a set of hard drives that were offered for sale on the second hand market. The research that was undertaken in the UK took place at the University of Glamorgan and was based on a total of one hundred and five hard disks that were supplied blind (the University and the researchers had no foreknowledge of where the disks had been obtained) for the experiment by a third party. When the first phase of the research, which was to see if there was sufficient information available on the disks to identify the organization that the disk had originally come from and, if possible, the name of the main user, was completed, the benefactor that had supplied the disks disclosed a list of the sources from which the disks had been purchased. The sources of the disks included eBay, public computer fairs and auctions and one of the major recyclers of computers for industry and the government.

The disks supplied to the researchers were identified with a single, unique identification number. In order to maintain the integrity of the disks, in case they were required for further research, each of the hard drives was forensically imaged. The subsequent analysis was carried out on the images. Tools, such as EnCase by Guidance Software, and the 'dd' command in the Linux based Knoppix software were used for the forensic imaging and the tools used for the analysis were the Windows operating system and hex editors - tools that any competent computer user would have access to and be able to use.

Of the one hundred and five disks supplied for the research, 13 could not be imaged as they were found to either have been physically tampered with and were no longer readable or it was not possible to image the hard drive using the tools that were available. No attempt was made to use more sophisticated 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 92 images created from the readable disks were used for the analysis.

The first stage of the analysis was to determine whether or not the hard disk had any data that was visible during an initial examination. This involved the simple step of loading the image of the disk and looking to see if there was a file structure or individual files present. Of the 92 hard disks for which images were successfully made,74 hard disks were found to have files present. Of the remaining 18 disks, 16 appeared to contain no data at all. This was a cursory examination of the image to determine whether there was easily recoverable data present on the disk that did not require the use of further tools or techniques. Further investigations were then undertaken into each of these disks. Of the 18 disks that appeared to be blank, a more thorough check was made and 16 of the disks were found to be totally blank.

The second stage of the analysis was to look for specific information that would allow for the identification of the organization that had used the disk and, if possible 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 disks that could be traced to the organization or an individual.

The results of the research were that, of the 92 disks that were examined the following was revealed:

Totally blank:

(16/92) 17 percent of the disks were totally blank and contained no file structure or data. When the source of the disks was revealed at the end of this phase of research, it was found that 12 of the 16 disks were those that had been supplied by the recycling company (the only 12 from that organization).

Attempts made to remove data:

(44/92) 48 percent of the disks appeared to have had superficial attempts made at the removal of the data. These efforts ranged from the simple deletion of files, to a formatting of the disk, to a new install of an operating system over the existing operating system.

Identifiable to organization:

(52/92) 57 percent of the disks contained sufficient information from which the organizations could be identified. The information available made it possible to identify organizations that included a large leisure services industry organization, a pharmaceutical company, a financial services firm a surveyor, a number of colleges and universities and a primary school.

Identifiable to a user:

(49/92) 53 percent of the disks contained identifiable usernames. A number of these disks contained multiple usernames.

Personal information:

(47/92) 51 percent of the disks contained details from which individuals could be identified. This information included, in one case, a complete database of customer records, and employee information including the names, addresses, contact details and national insurance numbers for individuals in some of the organizations. On disks that were identified as having originated from home user/small office disks there was a wide range of information such as family information, VAT numbers and personal communications.

Financial information:

(18/92) 20 percent of the disks contained financial information relating to the organizations, including staff salary details, sales receipts and profit and loss reports.

Network information:

(7/92) 8 percent of the disks contained details regarding the network infrastructure of the organizations. This information included server names, proxy numbers and other IP number details.

Possible illicit material:

(4/92) Despite widely accepted anecdotal evidence to the contrary, only four percent of the hard disks had references to material that could be considered to be illicit. This was in the form of either illicit photographs or references to sites that appeared to contain illicit material. Illicit in this context is used to mean images that may be considered to be pornographic.

Security and anti-virus software:

(3/92) During the initial, cursory examination of the disks, only 3 percent of the disks appeared to contain any security or anti-virus software installed. A further, more detailed, examination of all of the disks would be required to confirm this apparently low finding.

Passwords:

(1/92) During the initial, cursory examination of the disks, 1 percent were found to contain passwords that were stored 'in clear'. This result arose from an observation of a password during the initial check of one of the disks.

The level and type of information that was found on the disks and the ability to quickly and easily identify it to organization and individual was, in some cases, surprising. In one example from a major leisure service organization, for which a batch of 16 disks was found, a number of the disks that were examined had originally been used by the finance department. This included those that appeared to have been used by the finance manager and their assistant - disks were named FMANAGER/STOCK and FASSISTANT/FMANAGER, which contained detailed documents on their property holdings: the

> **"The disks were easily identifiable to an organization or individual"**

names, addresses and telephone numbers of members of staff: wage information: balance sheets: incident reports: profit and loss balance sheets and expenses details, some of which was less than three months old at the time that the research started. Another example from a large financial institution gave details of confidential memos marked 'for internal use only', staff directories and staff profiles. Other information that was recovered from one of these organizations included correspondence on customer complaints and information on when tapes for CCTV cameras should be replaced.

From the disks that were recovered that could be identified to academic organizations, there was a large amount of personal information, including course work and exam results – actual and predicted, letters of reference for individuals, together with template letters and logos.

One disk that was recovered was found to have originated in a primary school and was particularly disturbing in that it contained a significant level of information that related to children that could be identified. This information included reports on student progress throughout the year, a report that related to a bullying incident and one that related to medical treatment for another child.

Examples from privately owned systems included a database of passwords from the system of one (identifiable) user and emails relating to an extra-marital affair, where the participants could be identified.

Whilst all of this may be amusing to some people and could not, of course, happen in your organization, the implications are potentially devastating to an organization or an individual. If this information had fallen into the hands of individuals or groups that intended to make use of it, there was enough information available to enable a number of different types of crime.

Looking at the potential cost, both financial and to reputation, of these data losses to the organization, it is clear that much more needs to be done to ensure that this 'goldmine' of information is protected.

The disposal or loss of disks that still contain significant amounts of information is not a new problem. As early as 1993, a report in the *Canadian Globe and Mail*[6] reported that a used hard disk that had been sold to an Edmonton man contained two years worth of detailed and confidential personnel files on 166 employees of an Alberta organization. In 2000[7], a report appeared in 'The Register', a UK based online news site, about the disposal by the Morgan Grenfell Asset Management merchant bank, of a disk that contained details of Sir Paul McCartney's bank account. Again, in 2004,[8] the same news site reported that a mobile security group called Pointsec Mobile Technologies had obtained a customer database and the current access codes to what was supposed to be a secure Intranet of a large European financial services group from a hard disk that was purchased for £5 through eBay.

The implications of this information being made available to people who may exploit it, through either indifference by the respective organizations or a breakdown in security or the procedures for the disposal of equipment are significant. The range of crimes that the information might be exploited for are discussed below.

Industrial espionage:

For all of the disks that were attributed to commercial organizations, the potential cost of the leakage of this type of information is high. For the leisure service industry organization (a household name in the UK), the leakage of information that was found, most of which could be attributed to its finance department, can be considered nothing short of potentially disastrous. To a competitor, a potential supplier or a financial analyst, the level and detail of information would allow for a very accurate analysis of the financial viability of a number of operations being run by the organization. It also provided details of turnover, stock levels and the names and contact details for staff. The disks that had belonged to a financial institute gave information including directories of staff, staff profiles and business plans, all of which would be of high potential value to anyone outside the organization.

Identity theft:

On the disks that had belonged to business organizations, to academic institutes and to individuals, there was enough data available to enable identity theft or cloning. The level of personal information varied and included names, addresses, National Insurance numbers and email addresses, and in one case included passwords for a number of accounts/applications. Other research that has been conducted in the USA estimates that the number of people that have suffered from some form of identity theft in the USA alone at 10 million and put the cost to business and consumers at approximately $53 billion. The same research estimated that the cost to the individual of 'repairing' their identity is approximately $808 for each incident in addition to around 175 hours of effort. The first of the UK reports referred to earlier puts the cost of identity theft at £1.3 billion and estimated that, in the UK, one person's identity will be stolen every four minutes.

Fraud:

From the disks identified as having originated in the leisure service industry organization and at least one academic institute, there was sufficient information/data available to allow fraud to take place. In the case of the leisure service industry organization, the range and depth of information would allow a fraudster to either manipulate the information to his/her advantage or to generate false invoices and in the case of the academic institute, the logos and templates would allow the production of authentic looking false documentation, such as references or letters of qualification.

Blackmail:

At least two of the disks that were examined contained information that would put the owner/user in a position where they might be vulnerable to blackmail. One of these disks was from a personal PC, which contained details of an extramarital affair where the owner could be clearly identified and the other was from a corporate PC, again, where the user could be identified, that had been used to download what appears to be pornographic material.

Hacking/ network intrusion:

A number of the disks contained quite significant detail about the network infrastructure of the organizations, including server names, IP numbers, proxy numbers and other network information. This information is normally hidden to the outside world by the perimeter defences (firewalls) of an organization, but, if it was made available to a potential hacker, it would certainly improve their chances of a successful attack and in at least two cases would have made a hacking attack possible.

In the case of the disks that had come from corporate or academic systems, there is the issue of their duty of care regarding the business and the interests of the shareholders and also with regard to the individual. This duty of care is embodied in a range of legislation, but probably the two most relevant and obvious areas are 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

> **"There was enough data available to enable ID theft"**

and the Gramm-Leach-Bliley legislation in the USA. The American legislation may seem to be irrelevant to UK companies, but in fact they apply to all organizations that wish to do business in the USA. The DPA mandates that any organization 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. The wording of the relevant section of the DPA is:

A data controller shall, as respects personal data kept by him, comply with the following provisions:
(a) the data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly,
(b) the data shall be accurate and, where necessary, kept up to date.
(c) the data—
(i) shall be kept only for one or more specified and lawful purposes,
(ii) shall not be used or disclosed in any manner incompatible with that purpose or those purposes,
(iii) shall be adequate, relevant and not excessive in relation to that purpose or those purposes, and
(iv) shall not be kept for longer than is necessary for that purpose or those purposes,
(d) appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.
(2) A data processor shall, as respects personal data processed by him, comply with paragraph (d) of subsection (1) of this section.

It is notable that the wording that is used specifically requires that it shall 'not be disclosed' and that it 'shall be kept for no longer than necessary' in addition to the requirement for 'appropriate security measures shall be taken against unauthorized access to the data'. Clearly, by the fact that this information ended up on disks being offered for sale on the second hand market, a number of organizations had failed to meet their obligations with regard to this legislation. When the organizations were contacted, subsequent to the research, the leisure services organization claimed that the reason that the disks were available to be sold was that they had been stolen from their premises. This may or may not be true (they initially presumed that the disks were from laptop computers and were less than willing to confirm that they had reported the theft to the police, although the number of disks involved (16) would have meant that it had been a significant theft), but it does not make any difference. If the disks were, in fact stolen, it means that the physical security that the systems were afforded was inadequate. The corporate governance requirements place a responsibility on the management of an organization to protect the interests of the shareholders. If they fail to adequately carry out these duties, then they can be held liable and called to account.

In the cases of all the disks that had originated from the corporate or academic areas, it would appear that the organizations have contravened the Data Protection Act and probable that they have failed in their duty of care to the business. In the case of the disks that could be identified as having originated from the financial services sector, the Financial Services Authority (FSA) would be likely to take action against the organization for failing to take due care of the information.

In summary, of the 105 disks that were supplied for the research, 13 could not be accessed using the tools that would be available to a computer literate user. Of the remaining 92, 16 of the disks contained no data. Of these, 12 were subsequently found to have come from Life Cycle Services, a computer recycling company[9] that has a comprehensive process for the removal of data from systems that are recycled. The source of the other four disks that had also obviously gone through an effective data removal process could, of course, not be determined, as there was no information present to indicate the source. Of the remaining 76 disks, some data was present on all of them. Of these disks, only 44 had had any attempt made to remove the data present. The effort that had been made to remove this data from these disks was at the level of deleting it or carrying out a format of the disk.

This failure to take adequate steps to remove data from the disks has resulted in a number of these commercial and academic organizations not meeting their legal obligations. It is clear that the level of effort currently invested by a large proportion of commercial and academic institutes in ensuring that they have removed information from disks that are disposed of is totally inadequate.

As a final comment, the reaction of the organizations, which were contacted subsequent to the research, varied widely. While all of them, quite correctly, required sufficient information to confirm that the disks had indeed originated in their organizations, the financial services organization, the pharmaceutical company and the academic institutions all accepted that they had had a breach of security and initiated investigations to discover where their procedures had been failed. The reaction from the leisure services organization was completely different. On being informed that the data had been recovered, they responded immediately by stating that the disks had been stolen and that they had lost a number of laptop computers. This was interesting as the disks that were used in the research were from desktop systems. When asked to verify that the disks had been stolen, they were unable or unwilling to provide a police crime number for the crime. Their reaction did not appear to be to try to understand what had happened and address any procedural shortcomings, but to attempt to suppress any mention of their name or potential publication of any research results in which they were mentioned.

There is a clear requirement for the education and training of the relevant staff within a wide range of organizations to inform them of the potential problems that arise from the failure to adequately erase the information from disks and systems that are leaving their control and to make them aware of the potential costs to their organizations of this failure. When organizations dispose of surplus and obsolete computers, they must ensure that whether they are cleaned through internal resources or by third party contractors, that they check that the procedures that have been put in place are effective.

References

1 Eamonn O'Neill, Data Rape, The Scotsman, 30th March 2002

2 Bown, J, Protect yourself against the identity theft epidemic, The Sunday Times, 06th February 2005

3 Lettice, J, Home Office tackles ID fraud. By hiring one, The register,19th January 2005

4 Warning, Advice and Reporting Point (WARP), http://www.warp.gov.uk/

5 IT Security Awareness For Everyone (ITsafe), http://www.itsafe.gov.uk/

6 Disk Slipped Into Wrong Hands, Canadian Globe and Mail, 2nd August 1993

7 Cullen D. (2000), Paul McCartney account details leaked on second user PC, The Register, 9th February 2000, http://www.theregister.co.uk/2000/02/09/paul_mccartney_account_details_leaked/

8 Leyden J. (2004), Oops! Firm accidentally eBays customer database, The Register, 7 June 2004, http://www.theregister.co.uk/2004/06/07/hdd_wipe_shortcomings/

9 Life Cycle Services Ltd, Allington House, 3 Station Approach, Ashford, Middlesex, TW15 2QN, http://www.lifecycleservices.co.uk

Author Contacts:

Email: andrew.28.jones@bt.com

Tel: (0044)01473646133

About the author

During a full military career Andy Jones directed both Intelligence and Security operations and briefed the results at the highest level and was awarded the MBE for his service in Northern Ireland. After 25 years service with the British Army's Intelligence Corps he became a business manager and a researcher and analyst in the area of Information Warfare and computer crime at a defence research establishment. In Sept 2002, on completion a paper on a method for the metrication of the threats to information systems, he the defence environment to take up a post as a principal lecturer at the University of Glamorgan in the subjects of Network Security and Computer Crime and as a researcher on the Threats to Information Systems and Computer Forensics. At the university he developed and managed a well equipped Computer Forensics Laboratory and took the lead on a large number of computer investigations and data recovery tasks. He holds a Ph.D. in the area of threats to information systems. In January 2005 he joined the Security Research Centre at BT to take up a post as a research group leader in the area of information security.

Whose computer is it anyway? (part II)

A genuine new paradigm, or just a better way of doing things?

Matthew Pemble

Matthew Pemble

The intellectual property of computers and the data they contain does have a considerable bearing on information security, whether it hampers widespread industry cooperation or leads to fierce court battles.

Introduction

In the first part of this article last month, I looked at the way the current legislative environment affects what we mean by "ownership". In this part, I wish to look mostly at the effects the various non-commercial/open-intellectual property movements are having on information security concerns.

There have been many previous attempts to explore the impact of the "new" models of Intellectual Property Rights on the wider world of information technology, but most of the attempts to examine the specific impact on information security have come from either the marketing departments of the big vendors or the ranks of the open source evangelists. More significantly, these tend to concentrate on single issues; for open source, that of vulnerabilities; and for commercial software, that of trust. Detailed and realistic discussion of the pros and cons of either of the extremes, or any of the middle ranking options is rarely attempted. Coupled with the increasing pressure that the commercial and legal sector Intellectual Property lobby is placing on international legislatures,[1] it is vital that the proper advantages and disadvantages of both regimes are carefully considered and discussed.

There have clearly been distinct Information Security issues with the current (closed source) IPR model. To take a personal example, I have had a credit-card size RSA SecureID token pretty much since I joined the bank – we use it for our dial-up RAS solution and it is more than acceptable. Last year, an IT security forum, FS-ISAC, gave me another SecureID for accessing their website – this time one of the smaller form-factor key-fob type. I went to our security admin team and asked if I could use my new token with our RAS and, after getting the appropriate key files from the ISAC admins, our ACE server admins had a go at making it work. Some considerable waste of everybody's time later, we were informed that there is a fundamental incompatibility between the North American and European versions of either RSA SecureID or ACE Server. This, so we were informed, was due to the fact that the RSA patent (the RSA algorithm apparently being used somewhere within the product) was not applicable in Europe. Therefore the software implementations had to be different. An interesting explanation, but almost certainly a vendor partial truth.[2] Not only had the RSA patent expired by the time the code versions in use were released, but even before that it was beneficially owned by the company that produced the software.

But enough of my personal problems with incompatibilities (deliberate or otherwise). These issues have wider industry effects. These incompatibilities of various implementations of authentication and encryption protocols[3] has hampered the implementation of cross-Internet end-to-end security. In addition the political need for Microsoft to present an alternative to Java has led to significant weaknesses in fundamental security.[4]

There are significant environmental changes in the way the practicalities in the use and abuse of computer law are progressing. Two key drivers are the increasing militancy of the very-large content providers and publishers. Both are engaged in the (totally justifiable if often extremely poorly handled) enforcement of their existing legal rights. But much more worrying is their legal and extra-legal campaign to extend their current rights both into perpetuity and into other contexts and cross-jurisdiction.

The second significant factor is the rise in importance of the "common ownership" movement – expressed in information technology mostly through the various "Free and Open Source Software" initiatives.

Software

One of the great successes of the late 1990s and the first half of this decade has been the rise of the Open Source community, both in the specific terms of software and also in the linked domains of literary and other Intellectual Property. Determining how this enthusiastic and dedicated community will co-exist with the established (or entrenched?) legal, commercial and Intellectual Property Rights communities is proving to be one of the more interesting dramas currently playing out, whether in court or in the media.

For many years IPR software protection internationally has been based on the principle of copyright. This is indicated by such legal decisions as "Computer Assoc. Int'l, Inc. v. Altai, Inc.", (US Appeal Court case from 1992[5]) and "Gates Rubber Co. v. Bando Chemical Industries Ltd", (US Appeal Court case from 1993[6]).

The specific expression, normally in source code, of any particular program has been protected, but the ideas and concepts behind the program have not. Copyright, remember, is a long-lasting but limited protection, compared to the deeper but much shorter protection of patents.

> **"The MS Java alternative has led to fundamental security weaknesses"**

The issue of wider use of patents, for protection of software, has been a considerable battle ground between the USA and most of the rest of the world. The general concept of "methods patents" has long been an international battleground, and this remains so. But the issuing of patents specifically for software methods,[7] is now a matter of real controversy. This has not been aided by the patents community itself, which (admittedly due to endemic government under-funding as well as sheer commercial greed) has been applying for and awarding patents for which considerable prior art existed, as well as being as in contravention of national and international patent law.

The fundamental issue for any manufacturer is the necessity to ensure that any invention, product or software program is either not "patent encumbered", or where patents exist, is properly licensed. Large organisations can afford patent lawyers or, more importantly, have their own suite of patents, which they can use to enter into (or even force) cross-licensing deals. In the statements of many of the politicians and lawyers, protection of the "small business" is an important reason for allowing software method patents. This ignores a number of key facts:

- Patents must be defended by lawsuits – even in manufacturing industry, these are long and expensive, money few small companies can afford.
- Historically, patents have been applicable within a reasonable sector of industry, within which a researcher might be expected to be aware of the "state of the art". With software being so ubiquitous, advances in software are generally applicable across very wide areas of commercial and other endeavour.
- The number of patent jurisdictions, and the variety of languages in which patents are issued combined with the rapid and relentless advance of computer technology all conspire to increase the problems for smaller companies in determining where patent coverage exists. They are attempting to produce product to market, rather than to conduct original research.
- The inability, whether due to legal restrictions,[8] pressure of work, or lack of understanding of information technology of the patent awarding authorities, to properly consider "prior art".

In my opinion, however, the biggest complication is the incredibly loose language being allowed by the patent awarding authorities, especially in method patents. The impact of this is a huge variety of patents that are applicable to far too many situations and, although they can be challenged by the profusion of "prior art", this takes the expensive lawsuits already mentioned.

Security improvements depend, not only on good design and tight implementation, but on the continual flow of innovative product and, more importantly, on the interoperability between products from different manufacturers. We have seen this most unimpressively with the recent (Sep 2004) collapse of the Internet Engineering Task Force's Madrid working group, which was focused on fighting spam. The group were considering"Sender ID" – the proposed merger of Microsoft's CallerID and PoBox's SPF (Sender Policy Framework). The Group was working to develop a standard to authenticate email senders, which would make it more difficult for spammers to hide their identity. Intellectual Property Rights regarding SenderID hampered progression of the idea. Spam is, I think all of you would accept, certainly not the most serious issue security currently faces[9] but is, actually, fairly important. For a single organization to be able to essentially destroy the global Internet industry's response plan for spam, by deliberately introducing licensing conditions (despite the IETF rules requiring "fair and non-discriminatory" licensing) for unpublished patents (i.e. claimed but not awarded) that you have written to ensure that your main competition, as you see it, cannot accept, does not bode well for the future of security.[10]

The ideas behind the Open Source Software movement have been much debated. These debates include the legal[11] and regulatory issues surrounding the use and abuse of open sourced code (and ideas and methods) in subsequent products released under a different licensing regime.

This battle, probably best seen in the SCO / IBM and Novell / SCO court cases, has yet to be truly begun in earnest. How can the vast majority of Open Source advocates (neither IBM, the industry's biggest holder of patents, nor Novell can be considered in the least representative) afford to take even a medium-sized organization to court?

Of particular personal disgust are companies that merely exist to hold patent claims to extort from other organizations. I have no problem with an inventor licensing her invention so that a larger, or more production-focussed, organization can use it (even on a monopoly basis.) The factor that I find offensive is an organization that does nothing with its patent, possibly even refusing to license it despite not using it itself, and subsequently engages in a rash of legal suits. The epitome of this level of anti-social behaviour is the "submarine patent" – where an organization encourages adoption of some standard or protocol against which it holds a degree of intellectual property rights and, once the standard is adopted, announces the patent and starts its inevitable quest for license fees, damages, and legal costs.

I believe that it will be necessary for a single international and fair framework for patents to be established. This will need to provide both for proper protection and reward for genuine inventors, while still permitting the continued development of technology, in both the traditional commercial and the open-rights sectors.

Data and creative works

Patents are the main issue with software – copyright is well understood (even if the US abstraction, filtration, comparison test from the Altai case is less so). With data and creative works, the complexities of copyright and permitted uses are a very significant issue.

The rise of peer-to-peer filesharing, in conjunction with the huge rise in the size of a "normal" hard disk and the prevalence of broadband connections in homes, took the content distribution industry by surprise. The rights owners' industry bodies, particularly the RIAA (Recording Industry Association of America), and the British Phonographic Industry (BPI) and the Motion Picture Association of America, have fought back with civil and, where possible, criminal cases[12] against individual file-sharers and against the systems supporting them. How much this has actually either reduced piracy or increased income for the rights owners is dubious, given that they still trumpet falling sales and blame piracy.[13] However it has achieved considerable legal success, with Napster as the most famous (or notorious, if you are an IP lawyer) case. Luckily, the rise of legal music download sites, particularly Apple's iTunes, has provided a proper alternative, although Apple are currently having their own legal issues with the European Union's cross-border free-trade provisions[14].

The situation is complicated by international legislative differences, as discussed in the previous section. The EU "database right" does not exist in the USA (and may actually be opposed by significant sectors of US industry). Conversely there is no "fair use" right under UK copyright law. As with software, harmonisation of laws to take account of the modern ease of cross-border communication is necessary. In addition is right's owners should pay better attention to developments in technology so that they can take proper advantage and not leave gaps for exploitation whether by criminals or by the general public.

What are the implications for information security:

- At the strategic level, the increasing openness of data structures and the large volume of readily (publicly) searchable data are very significant.[15]
- At the operational level, the sophistication of peer-to-peer networks are reducing the ability to secure what is left of the corporate perimeter.

Scott McNealy, CEO at Sun said, a couple years ago, that, "the network is the computer." I firmly believe that the future is data, not applications nor hardware.[16] Currently most of our technology is concentrated on protecting the platform, with application level security seen as the rising star. Security is going to have to head down the data stream quite quickly.

Firmware, hardware and upgrades

It may be difficult to consider that hardware would be significantly impacted by the non-commercial movement. However, clearly it costs money to build and transport, therefore there will be a commercial aspect to its distribution. There is a very long history of embracing and (not to coin a new phrase) extending intellectual property in the hardware world. The first computer my family owned was an EACA Video Genie[17], a clone of the Tandy TRS-80 (but with an internal tape drive and other improvements.) Certainly, the huge expansion of the distributed computer industry was driven not by the original IBM PC product but by the availability of the much cheaper clones[18].

The availability of clone components, such as the wide variety of Ethernet cards, the AMD microprocessors, and unbranded memory has both driven down prices. The consequent competition has been significantly responsible for the increasing quality of product. However, the complexity of modern equipment, the costs of fabrication plants for microprocessors or ASICs (Application Specific Integrated Circuits) – even with the availability of very large Field Programmable Gate Array matrices – means that complex hardware production is likely to remain with the ultra-committed hobbyist or for any relevant volume, a larger-than-micro business.

More significantly, recently, Richard Stallman has called[19] for action to develop an open-source BIOS. Partly, as he admits, this is because it is now possible, with BIOS in flash-RAM rather than ROM. Also it is due to his completely consistent (if somewhat fundamentalist) philosophy. This will nearly complete the open-source computer – GNU, Linux, and BIOS, with the tin being the only proprietary material left.

One area where this has significance is in the upgrade of older equipment. Most computers are still viable for limited purposes significantly after their design life is over: the machine this article is backed-up on was built out of second-hand junk over eight years ago.[20] The major manufacturers do not continue to support outdated hardware once the volumes (and the margins) begin to fall. If there are significant IPR restrictions on production of compatible equipment, a valuable market sector (at least, to compulsive hoarders like me) will drastically reduce if not actually disappear.

Summary

We are engaged in a fundamental shift in the way the world treats ownership. It is not new. The concept has been in the public realm for some time now. Richard Stallman published "The Right to Read"[21] in 1997 In addition, James Boyles opinion piece "Sold Out" was printed in the *New York Times* over nine years ago.[22] This issue is going to fundamentally affect our lives. It will influence our ability to earn a wage, our ability to communicate with people of whom others disapprove. It even affects the control our governments can have over what is currently "private space."

> **"A fair framework for patents should be established"**

Not every advance in the protection of intellectual property is wrong – we need the efforts and output of the musicians, the creative writers and the inventors. Some of them may choose to exploit their creation for personal gain, others may donate it gratis to the public domain. The issue is how much choice they are allowed to have. There is no real gain to society if, for example, I created music you wished to hear and had it licensed under say "Creative Commons" but the law put severe restrictions on the dissemination of it. If, for example, the law required for every public performance or broadcast of my creation a fee to be paid to an industry quango which distributed the income according to the popularity of fully commercial music.

Copyright, in the UK, currently lasts for between 25 and 70 years.[23] Patents generally apply for 20 years. Both international (WIPO) and local legislatures are regularly presented with proposals either to increase the duration or the extent[24] of IPR. Benefit to the author / creator, as opposed to the large publisher or vendor is often negligible.

The impact of any changes, either way, to our existing rights could have very significant effects on the way society proceeds. It is important that all of us make efforts to properly educate ourselves regarding what is being proposed, make a rational decision on the propriety of each change and, where necessary, use our democratic rights of the vote and protest to make sure that the politicians appreciate what their signatures mean.

References:

1 http://www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//TEXT+PRESS+NR-20050309-1+0+DOC+XML+V0//EN&LEVEL=2&NAV=S

2 I could have said "typical whopping great vendor fib" but the Editor gets worried about law suits.

3 Best demonstrated by the work of the Samba project in their continued work around Microsoft's implementations of IBM's SMB file-sharing protocol.

4 http://www.petting-zoo.net/~deadbeef/archive/2282.html for the Quicken hack by CCC. A Swedish group demonstrated a similar attack against Microsoft Money. Oh, and if you think Authenticode is a solution: http://www.microsoft.com/technet/security/bulletin/MS01-017.mspx

5 http://www.tourolaw.edu/2ndcircuit/july95/93-7957.html

6 http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/gates.html

7 Amazon's "1-click" patent being one of the more notorious, but there are many more, including the previously mentioned RSA patent (this expired in 2000 but, if you look at

http://www.rsasecurity.com/rsalabs/node.asp?id=2326, RSA do not explicitly list it as expired – to be fair, they do here: http://www.rsasecurity.com/rsalabs/node.asp?id=2322), and the LZW patent that affected the GIFF graphics file format.

8 Such as the US rule which insists that only material published in a professional journal can be considered, mere production of a product which uses the same method is not relevant.

9 This would have to be the insistent and effective encroach of organised crime.

10 Mind you, there is an upside to everything: imagine the increase in worldwide productivity if Universal USA Inc had been granted a method patent for "Space Panic" – the first of the "platform games." – See http://en.wikipedia.org/wiki/Platform_game

11 See http://news.ft.com/cms/s/78d9812a-2386-11d9-aee5-00000e2511c8.html

12 http://www.riaa.com/news/newsletter/022805.asp, http://www.msnbc.msn.com/id/6504024/ & http://www.bpi.co.uk/news/legal/index.asp?fName=news_content_file_903.shtml

13 http://www.riaa.com/news/marketingdata/pdf/2003consumerProfile.pdf

14 http://biz.yahoo.com/ap/050225/eu_apple_1.html

15 The use of various government "Freedom of Information" legislation to obtain details of commercial significance or confidentiality is increasing – sometimes for purposes of responsible journalism, often for industrial espionage.

16 Grid computing, especially with the new "Cell" processor chip-set, is likely to significantly accelerate this trend.

17 PMC80 in the USA, System80 in other locations

18 This is being written on an, admittedly rather expensive, IBM laptop, but see Mr Stallman's comments on these in link 19 below.

19 http://www.fsf.org/news/freebios.html

20 And is very happily running on FreeBSD, as it has since it was donated to me. Admittedly, only 4.3 STABLE, but I have had a busy few years!

21 http://www.gnu.org/philosophy/right-to-read.html

22 http://www.law.duke.edu/boylesite/sold_out.htm

23 Except, of course, for "Peter Pan." http://www.gosh.org/about_us/peter-pan/copyright.html Much as Great Ormond Street Hospital is a national treasure fulfilling a vital role, the Government should fund it directly, rather than tinker with fundamental civil liberties. As we have seen with politicians before, once a liberty is bent, it quickly cracks, breaks and is then written out of history.

24 This one is classic – there are few TV commercials worth watching once (I apologise for hieroglyphics): "http://thomas.loc.gov/cgi-bin/bdquery/z?d108:h.r.04586:" In fact, a significant feature of both the design and the operation of the UK electrical power generation and distribution systems is that people do not watch TV commercials. They get up and make a cup of tea instead. For popular programmes, that number of kettles switched on, in a narrow time frame, is a major power demand.

About the author

Matthew Pemble runs the technical investigations and threat management unit for a major international bank. He is a Fellow of the British Computer Society, a Fellow and Director of the Institute for Communications Arbitration and Forensics, and a Chartered Engineer, CISSP, CISM and CFE. A regular writer and presenter on information security and investigations issues, he does not use peer-to-peer software and has only just bought himself an iPod, but he does use open source software regularly at work and at home, and relies on open-source intelligence. He can't write music, certainly can't sing, but does occasionally play the bagpipes.

Looking out into a world of threat

Debi Ashenden is a senior research fellow in information assurance at the Royal Military College of Science, in Shrivenham, UK. She spoke to Brian McKenna about the risk assessment culture information security professionals need to develop.

The May Day protests in 2003. The City under siege from anti-capitalist protesters. Debi Ashenden and Andy Jones, then of Qinetiq Trusted Information Management, were advising a financial services client. "We looked at who in their part of the City of London was a likely target, and whose security was particularly tough", says Ashenden. "The threat to that target could also be a threat to our client. It's that kind of threat agent awareness that IT security professionals need to bring to their jobs".

Debi Ashenden moved from Qinetiq six months ago to take up the post of Senior Research Fellow in the Department of Information Systems, Cranfield University, at the Royal Military College of Science, Shrivenham.

Amid the tanks, guns and buildings that don't officially exist, she has a research remit that runs over the 'soft issues' of information security. She believes that IT security managers need to reinvent themselves as "risk professionals" and take on board the methods that physical security specialists from a services background deploy. She and her former colleague Andy Jones expand on this in their forthcoming book, *Risk Management for Computer Security : protecting your network &*

information assets. It suggests security professionals need to learn how to do threat assessments by looking outwards. "We tend to look inwards at vulnerabilities not at external threat agents", she maintains.

Qinetiq ethos

Ashenden was at Qinetiq from 1998-2004, latterly as Head of Professional Risk Services in the Trusted Information Management department. She joined what was then the Defence Evaluation and Research Agency as a student. "The ethos there was that you could wander around, and if you saw teams doing work that looked interesting then you could just go up and join in. It was that control over your own working environment that appealed".

> **"IT security pros. need to reinvent as risk professionals"**

As DERA morphed into the private company Qinetiq, the consultancy business was slow to begin with, she recalls. "The problem was that when we were DERA we had a culture of not talking to outsiders about what we did. So it was an uphill struggle. And anyone who could do bits of sales and marketing pitched in. When we started, the consultants and the IT security health check team had no profile in the marketplace. That has now changed".

Process junkies

Looking at the broader information security profession, Ashenden believes that it has to slough off its traditionally process-oriented mind-set. "The focus in our book is on the need for the risk professional to play a full part in the organization. Traditionally the typical IT security manager has paid lip service to the people and process part of 'people, process, and technology'. There is more focus now on process because of the new and emerging regulatory environment, but a lot of research is still to be done on the people issues".

"We need to take a sociological perspective to IT security risk assessment. Most infosecurity people have come from a science or engineering background and so they tend to see security as a process. So, for example, security awareness campaigns tend to be done in process terms. And so you roll out a package, capture an electronic record of who's seen it online, and so on. But you never test whether awareness has really been taken on board, whether there really has been a culture change".

"Security needs to be apprehended as part of a change management process. That is what we are trying to do, after all - make a change. People are not machines, and you can't expect them to process stuff in a way you expect".

Crossroads

Ashenden poses the issue of professional evolution sharply. "IT security managers have a choice. They can either retreat, in the new more regulated environment, into technical problems, or they can move to embrace operational risk, taking on board what operational risk people have to teach. With organizations now maturing in how they see security, it tends to get pushed away from the IT professionals. So, there is now space for the information security professional to change the perception that the organization has of them".

She ascribes the reluctance of some IT security managers to this kind of step to "a lack of desire; they often don't have the language. They can't see beyond the technical. There is also a certain amount of fear. It is quite comfortable being a techie and knowing a lot about your specific area".

The prominence of risk and compliance in the current discourse of the business world, both prompted by the Enron debacle, and other corporate scandals, gives infosec professionals a golden opportunity to re-invent themselves, says Ashenden.

"Risk is a convenient way of doing this at this present time because risk and regulation are so tightly bound together now. There is an opportunity to use risk as a vehicle that takes [IT security managers] further in their careers.

"There are also the pressures created by outsourcing and off-shoring. IT security managers now need, at least, to know the legal basics. It has changed the way security professionals are having to operate - doing contract management, relationship management, and so on". "And from the physical security guys you can learn how to do threat assessments. They understate things in terms of threat agents not just vulnerabilities. When I was consulting for Qinetiq, IT security people would say: 'we really like this idea of threat assessment; can you tell us how to do it?' And I have had to say, 'well you have physical security people here who do this kind of thing all the time. Go talk to them!'"

Looking beyond borders

Ashenden's academic background is in English Literature rather than Computer Science. To this she attributes a tendency "to look at security more broadly. Having changed disciplines, I am more willing to talk to others outside security and borrow from other disciplines. It also brings that other dimension of not just thinking from a technical dimension, but understanding context".

> **"It is quite comfortable being a techie"**

And so she specializes in the 'soft issues' around information security, acting as a translator between IT security and business. The need for this she illustrates by recollecting how, on one consultancy assignment she was working in an organization where the team needed to look hard at what the purpose of the organization was. And the answer came back, from someone in her team: "'They are in IT' - but they weren't, they were in finance. There was just no awareness of what the IT was there to do!"

"I'm inspired by people on the edge of security. For example, I worked on the DTI's Foresight programme on cyber-trust and crime prevention. They worked hard to bring a range of people from different disciplines, such as Peter Sommer, from the legal side, and Robin Mansell, also from the LSE, on the sociology side".

The military view

At Qinetiq, she recalls that the best project for her were those that "taught me to see security as a whole. I've also learnt a lot from military approaches. If you look at the military environment,when projects are going for security accreditation the ones that do best are the ones that take a step back and realise that you need to negotiate with the accreditor. Regulation is not black and white".

Ashenden sees danger as well as opportunity in the new regulatory landscape. "The new regulations culture could be constraining the way we think about security, and could encourage a US style box-ticking approach, where UK security has been, historically, more holistic. And so there is a danger that we could overlook greater threats. You could start to miss the context because you don't look beyond what the regulator wants".

Elsevier's Butterworth-Heinemann will be publishing *Risk Management for Computer Security: protecting your network & information assets*, by Debi Ashenden and Andy Jones, in March 2005.

CIOs at the heart of IT all

Stephen Hinde

Chief Information Officers need to manouvre IT so it is at the centre of the business strategy. The realisation of business goals is heavily linked to IT systems.

Aristotle Onassis, once one of the world's richest men, once said the secret of a successful business was to know something no-one else did. That should have tipped off chief information officers.

IT services company CSC has been asking what will drive chief information officers in the 21st Century. It has just concluded an extensive survey of companies to try to find the probable key drivers of corporate information system strategies in the next 10 years. The results should not surprise anyone who has had to run either a business or an IT shop. Bottom line? IT is integral to the organisation, as a strategic element, not just a service provider.

The most important change for CIOs is for them to develop the ability to translate business needs and expectations into realistic technical specifications and delivery schedules. In large part, that means the CIO has first and foremost to run the IT shop according to business principles. In a nutshell, the job is to optimize the allocation of available resources while minimizing the risks in the pursuit and retention of profitable customers.

The cost of obsolete software

The American Business Performance Management Forum has reviewed America's information architecture and found that it is replete with obsolete, redundant and unused software applications. These drain tens of billions of dollars per year, just from the most information intensive companies.

The survey also enquired about how IT relates to business processes and overall business performance. The researchers report shows responses that reflect the CSC findings. Nearly two-thirds of respondents said business software helps their companies capture new business, with fractionally fewer relying on it to gain competitive differentiation. But nearly a half take a dim view of the way IT spending is aligned relative to the strategic priorities and business needs.

Management consultancy Accenture recently surveyed 300 business and IT managers in the UK and Ireland. It found that the gap in priorities between IT and business is narrowing. It seems organizations are learning the lessons from the problematic and disappointing IT projects of the late 1990s and early 2000s.

The survey found that 84% of business managers and 76% of IT managers believe better use of IT has been the key driver in productivity gains over the past three years. But both groups believe IT is under-delivering on investments. Companies that are getting the biggest productivity gains from IT investments focus on the value to the business of IT investment and appoint managers specifically to bridge between the IT department and business units.

Accenture identified three core characteristics of IT departments that deliver productivity gains:

- A strong emphasis of IT governance.
- A project steering committee comprising both IT and business.
- An operational model including a core relationship management role to work between business and IT teams.

A survey by Nucleus Research into the top 10 IT predictions for 2005 found the winner to be consolidating for savings. It says companies are undergoing infrastructure audits to identify and clean out redundant or unnecessary IT assets. The payoffs will be big for systems auditing and analysis tool providers, it predicts.

This finding is similar to that of the Business Performance Management Forum mentioned above. Over 40% of the Forum respondents estimated that unwanted applications drained more than 10% of their IT budgets. Seven in ten said their companies had redundant, deficient or obsolete applications on their networks. Larger companies seemed to have the more serious problems. Only 40% of the respondents said they conducted company-wide software audits on an as-needed basis while just over 10% never did them at all.

Not delivering advantage or anything?

According to reports in the UK's *The Guardian* newspaper, the British Medical Association is worried that new software for the National Health Service (NHS) could open a backdoor for trojan horses to give unauthorized access to patients' records. This threat comes from the "Choose and Book" electronic appointments system. This makes a booking after it gives the hospital access to the patient's General Practitioner's (GP) computer record, which it downloads automatically. The aim is to give the hospital a complete copy of the GP's record as this give the hospital's consulting physician the patient's full primary care record.

Doctors' leaders are concerned that malware could piggyback its way into the NHS Care Record System and breach the traditional confidentiality in doctor-patient relationships. Whether or not the doctors' concerns have a solid foundation, their action helps to undermine the public's perception of confidentiality and security of computer systems.

The Choose and Book e-booking system is a key component of the National Programme for IT (NPfIT) in the NHS. Perhaps because of the stance taken by the British Medical Association, although the software was successfully delivered, it has hardly been used. The UK's National Audit Office (NAO) found that at the end of December 2004 there had been just 63 live bookings against a target of 205,000. The NAO found that there had been an intermittent fault with the system's authentication process, which prevented access to systems and led to a reluctance among GPs to use the system.

> **"Responsibility cannot be outsourced"**

The NAO also reported that a third of the NHS Trusts will not meet the government's target of having all patient bookings done electronically by the end of this year. The government has now announced a £95 million "reward" scheme to provide doctors with an incentive to use the new system.

There is a symbiotic relationship between the achievement of business objectives and IT systems. However, the quality of the systems becomes irrelevant if the users do not use them.

The NHS has experience of an expensive computer system that users ignored. In November 1992 the London Ambulance Service's new computer-aided despatch control system was largely abandoned because the users chose to make it not work. True, the system broke just about every rule for developing a computer system. These included:

- Organizational change as three organizations merged into one.
- Basing the system on a new PC network.
- A poor system specification.
- A management that lacked the technical expertise to specify the project requirements and to manage the project effectively.
- Little user training.
- Poor industrial relations.
- Hostile users who did not want the system to work.
- Tight development timescale, and outsourcing the contract to a small software developer with no previous experience.

Never on a Monday

The UK's Department of Inland Revenue has just rolled out a new human resources system that allows its 68,000 employees to view their payslips and update their personal data on-line. It also lets managers record and book absences due to sickness and holidays. But it can handle just 3,600 concurrent users.

The Inland Revenue has had to ration user access. Ironically, users now keep manual records until they get a chance to access the system and update it. On a Monday only managers are permitted access, which gives them a chance to clear backlogs of approval requests for holiday and absentee records.

The result is a similar level of user dissatisfaction as the NHS faces with its Choose and Book system. The difference is that Revenue is a victim of it own success.

Responsibility cannot be outsourced

With many of these large IT projects, both public and private companies prefer to outsourced the development and often the operation. But this does not change their management obligations and responsibilities. Responsibility cannot be outsourced; it stays with management.

Risk management objectives and regulatory obligations (e.g. UK Financial Services Agency, US Sarbanes-Oxley Act) stay the responsibility of management. And regulators are starting to require that managements demonstrate prudence and control even in intra-group outsourcing.

However, outsourcing does change the mix of essential management skills. In particular, managers on both user and contractor sides need to develop relationship management skills, stronger commercial skills, and lower profile technical skills.

There also needs to be an emphasis on managing processes, especially those that lead to or stem from service quality, incident response, change, and cost reduction.

Executives need to be involved early in the process. This enables them to set the agenda and timetable. They should aim to identify the key success factors early, to establish risk control and information governance models, and set controls and standards. These are all nothing new, and should be business as usual processes. If only.

For the user executives, the big benefit of the outsourcing process is that they can concentrate on outputs and results rather than get bogged down in technical and operational detail. That does not absolve them of the need to know how things work, because they need to be realistic in their expectations of performance and costs that they will spell out in detail in the Service Level Agreement and contract.

CIOs need to understand the business and the ways in which value is created. They need to be able to articulate a clear vision for the IT programme, and to be the educator of the business in terms of technology: what IT is and what IT can contribute to the success of the organization. They need to be the champions of innovation and to drive competitive advantage through innovation; understanding what organizational innovation is and introduce and develop technologies that encourage business innovation. IT is an enabler and a driver. It provides the tools for change and leads business change.

There needs to be a partnership between the business and IT. Neither part can succeed without the other. Neither can one party succeed without the full commitment of the other. There is a symbiotic relationship between the achievement of business objectives and Information Technology Systems, and the successful managers are those who fully grasp this and actively manage the resource of information. That is they recognise that it is their systems, their data and their information. The computer is the tool to enable them to collect, store and manipulate this information, and the IT department provides the application system keys to unlock this tool.

What is required is management action. Over the years I have seen many systems where there has been a lack of commitment; a lack of commitment of user involvement in the development of the system; a lack of commitment from users in not using the system, or not using it properly, or not trusting it and maintaining their own manual system, or not taking the trouble to ensure that the data that they are entering is accurate, complete and timely; and a lack of commitment by management who do not fulfil their managerial and stewardship duties to ensure that the quality of the underlying data from which is derived the information that supports their decision making, and to ensure that adequate controls and security exist and are enforced. All too often, the various parties are involved rather than committed to the systems - the bacon and eggs syndrome - the pig is committed to the meal whereas the chicken is only involved in it.

Success, however, needs to be measured in terms of organizational success rather than the purely implementation side. A successfully implemented computer system is a wasted opportunity if it is in isolation of the organization's requirements; it has to take the organization forward; there must be commitment, not just involvement.

Incident analysis and recovery

Getting the whole picture

Peter Stephenson

We have been discussing the management process for information security incidents. While we have emphasized that these incidents may, often, be prevented by taking a series of proactive steps such as risk management, inevitably those steps will fail and there will be an incident. When that happens, your proactive measures as well as solid preparation should help minimize the severity of the incident. It is axiomatic that our preparatory measures must be planned and executed to minimize the number and severity of such incidents.

This month we will take the position that all preventative measures have failed and we have an incident. What needs to be done to recover from the incident and analyze it so that lessons learned help reduce the probability of such incidents in the future? We begin with a few definitions.

Risk, vulnerabilities, threats, attacks and incidents

If one examines the information security literature, one finds varying meanings for the above terms. In order to ensure that we are talking about the same things in the same ways, however, it is useful to standardize on some important definitions. Additionally, good, formal definitions can help us arrive at a deeper understanding of the problem and its possible solutions. I have been working on the problem of consistent definitions for some time and I'd like to offer a few important ones that we can use in the context of this discussion.

If we think about the notion of an incident the first think that comes to mind is that we've been attacked. That means that we need to understand what we mean by an attack. We also have discussed the notion of information systems risk which also, as it happens, leads us to attacks. So with that in mind we should begin by understanding what we mean by an attack.

An attack does not need to succeed. In fact, most Internet-facing organizations are attacked many times per day, sometimes many times per hour. Most of these attacks bounce off the defences implemented for the purpose of protecting the enterprise. The simple, but formal, definition of an attack is an ordered threat, vulnerability pair. That means, simply, that there is a threat delivered against a vulnerability. Intent is not an issue, and the outcome is unimportant for the purposes of the definition.

A vulnerability, then, is a weakness or flaw, in an element of a system, that has the potential to be exploited with a damaging outcome. This definition does not say that there has been an attack and it doesn't say that a threat exists. At this point the vulnerability is nothing more than a weakness or flaw that could cause a problem if someone delivered a threat against it. The definition also does not say that such a delivery would or would not succeed.

Taking up the definition of a threat, we have an external stimulus that may lead to an incident when the external stimulus is applied to an element. That one requires a bit more discussion. First, an element is nothing more than something in a computing system. It could be an application, a communications stack or even the device itself. An external stimulus is anything that could, under the right circumstances lead to an incident of some sort. This says nothing about the threat agent however. The threat is not the agent. For example, a virus is a threat, but it has no meaning if there is no threat agent to release it into the wild or to direct it against a computing system.

We said in an earlier column that a risk was the probability that a threat against a vulnerability would produce an impact. The impact is not necessarily negative for the purposes of this definition. In fact, we define an impact rather benignly as well.

An impact results when an external stimulus is applied to a state. Again, we say nothing about intent or outcome. We simply say that when an external stimulus is applied to some element, such that the element changes its state, we have an impact. The notion of impact is Boolean. There either is an impact or there is not one. Still, at this stage, we have not said whether all of this is bad. That comes next.

Now we can put all of these pieces together and get to the bad part: an incident. A computer security incident results when a change of state of an element that conforms to a policy causes that element no longer to conform to that policy, and where the state change is caused by the application of a stimulus external to the system. Now we have a problem. We've caused a change of state in an element of a computing system (that means that we have an impact), and that change of state has caused the element no longer to conform to a policy to which it previously conformed.

Doing a little high school math and expanding these notions we find that an incident is nothing more than a threat successfully delivered against a vulnerability in an element of a computing system that causes that element no longer to conform to a policy to which it previously conformed. Most of us know that, at least intuitively, but viewing the issue in this manner helps us see where we can pursue analysis and recovery after the incident occurs.

Questions to ask:

Since we now clearly understand what's happening in a security incident, we now need to apply that knowledge usefully. We can look at the definitions above and ask ten simple questions, the answers to which might be helpful:

1. What was the threat?
2. Who was the threat agent?
3. Why did the threat agent select this target?
4. What was the nature of the vulnerability or vulnerabilities that were exploited?
5. What elements were involved?
6. What were the state changes?
7. What was the impact?
8. What policy or policies did the target element(s) violate after the state change caused by the attack?
9. There are explicit (actual written policies with some means of enforcement) and implicit (ad hoc security configurations) policies. What kinds are involved in the incident and why did they fail?
10. What could have been done to prevent the state change? This is the most important post mortem question of all.

Analysis

Now, let's take these ten questions and examine their importance and application to our analysis.

1. What was the threat? Understanding the nature of the threat helps us to pinpoint how we defend against it. For example, is there a credible threat agent to deliver the threat? For example, if we have a very strong antivirus policy and the technology and procedures to enforce it, does a virus constitute a threat to our system. If our antivirus controls are effective, no threat agent will be able to deliver a virus to our system in the first place.
2. Who was the threat agent? Was the threat agent internal or external? What were the threat agent's motives? Could we have done something to recognize and defuse the agent before he or she delivered the threat?
3. Why did the threat agent select this target? Was there something particularly attractive about the target? Was the threat agent a disgruntled employee? A script kiddy? A data

thief? A look at the FBI's computer crime adversarial matrix can help here. The matrix is described in C*omputer Crime : a Crimefighter's Handbook (95 Edition)* by David, Seger, Vonstorch, and Icove.

4. What was the nature of the vulnerability or vulnerabilities that were exploited? This helps analyze and remediate the vulnerability or vulnerabilities that were exploited.
5. What elements were involved? Where did the vulnerability exist? What can be done to protect that element more completely?
6. What were the state changes? What, exactly, happened? Can you describe the details of the state of the element both before and after the attack? If so, that may help apply countermeasures ranging from patches, to upgrades, to changing to a less vulnerable product.
7. What was the impact? Could the impact have been reduced or redirected? Was the extent of the impact serious or trivial? Could it have been forseen and planned for?
8. What policy or policies did the target element(s) violate after the state change caused by the attack? Was there a security policy that was in place or was there a security hole that allowed the state change? What was the policy? This is allied closely with the next question. Together these two questions can help design countermeasures or safeguards that can strengthen the protection of the element. Sometimes it is not possible to implement a strong policy due to circumstances specific to the element. In that case the notion of preventative measures must give way to detective measures. In other words, if we can't protect an element through the application of policy, we at least must monitor it for misuse.
9. There are explicit (actual written policies with some means of enforcement) and implicit (ad hoc security configurations) policies. What kinds are involved in the incident and why did they fail? This question addresses, specifically, configuration errors. Configuration that is ad hoc (i.e., not in direct support of a formal, written security policy) tend to fail because there is no specific process for keeping them current. An incident may point out these ad hoc policies/configurations and offer opportunities for improvement.
10. What could have been done to prevent the state change? This addresses countermeasures directly.

The nature of a thorough incident analysis is that all of the underlying causes become known. The problem with that is that it results, often, in finger-pointing. This is unproductive and hampers the analysis. In an earlier column, a year or so ago, we discussed formal post incident root cause analysis. At that time I pointed out that formal analysis is good for very complicated incidents in large networks but might be overkill for smaller, less complex ones. For those incidents, or for where resources to investigate are limited, this approach works well. It presupposes, of course, that an adequate investigation has taken place to allow these ten questions to be answered.

Recovery

Recovery is a real issue in most organizations. It usually is the case that recovery supersedes analysis. That, simply, is because most organizations exist because they maintain the production of their product or service. If that production stops, even during an incident investigation, it costs the organization money. Therefore, the first rule of incident response is "get back on line as fast as possible".

Security professionals know this but they don't like it. To them, not being able to conduct a thorough post mortem virtually ensures that the same thing will repeat. That does not need to be the case.

For recovery and analysis to coexist peacefully it is necessary that preparation for an incident occur prior to the incident. That goes back to our earlier discussions of being proactive. One of the most important proactive tasks the organization has is to develop techniques to preserve evidence while recovering rapidly. As it happens, this is now quite practical with today's technology. Here are some examples.

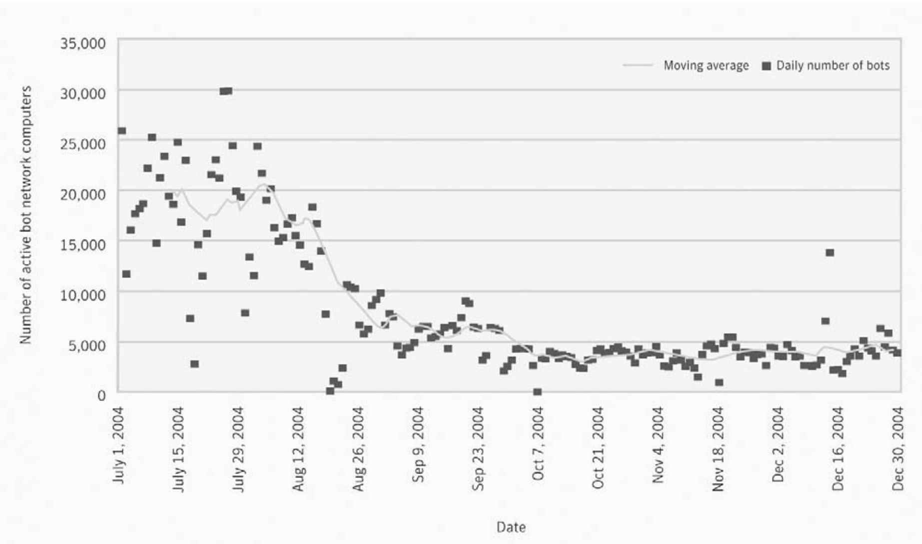
1. Log Retention. Use log hosts and spool all logs from all servers, firewalls and intrusion detection systems off of their host systems onto the log hosts. In a large network many such log hosts may be required. Log to these hosts on an ongoing basis, not on a batch basis, to avoid loss of important data. Back up the log hosts frequently and treat all logs securely, placing them routinely into a chain of custody.
2. Forensic Analysis of Servers and Hosts. This now is easy to do using remote/network-based forensic tools from either of two vendors. enCase Enterprise, by Guidance Software is the current market leader. A less expensive, but very effective alternative product is ProDiscover Response version from Technology Pathways. These two products allow immediate isolation of forensic data from involved computers by providing centralized, remote access to the computers over a network. Using this technique critical evidence may be extracted immediately before it is lost or damaged and, if the computer must stay on line, it can without compromising evidence.

The key issue, of course, is that data not backed up won't be recoverable so if these and other proactive measures are not in place recovery will be difficult to impossible. There are, of course, always situations where the impact of an attack is severe enough that the system under attack fails completely. The intent of proactive measures is to avoid this catastrophic outcome, but it can happen. When that is the case, your preparations may be all that is between the attacker and real, expensive, loss.

Windows XP SP2 release – the cull of the Bots

The number of slave computers controlled by hackers plunged last year after the release of Microsoft XP Service Pack 2, research from Symantec shows.

The number of Bot network computers plummeted from 30,000 per day in July last year to below 5,000 per day by the end of 2004 according to the *Internet Security Threat Report.*



Known bot network computers, July 1 - December 31, 2004.
Source: Symantec Corporation

As a result the number of scans and attacks against TCP port 445 and TCP port 135 dropped. Both ports are used by bot network applications such as Gaobot to spread onto computer systems through unpatched flaws or bad user name and password choices.

The climax of the last's year drop in zombie computers was in August, which marked the debut of the XP update.

Symantec also says that the inclusion of default firewall rules that block TCP port 135 and limit TCP port 445 activity may have curbed the recruitment of machines for bot networks.

As a result hackers are reverting to using spoofed hosts for attacking, said the report. These allow an attacker to overwhelm a victim with fewer compromised computers. But this gets harder to defend against. Symantec warned: "The spoofing of the addresses makes filtering based on the IP address much more complicated."

EVENTS CALENDAR

29 March - 1 April 2005
BLACKHAT EUROPE
Location: Amsterdam, The Netherlands
Website: www.blackhat.com

5 - 6 April 2005
E-CRIME CONGRESS
Location: London, UK
Website: www.e-crime-congress.org

26 - 28 April 2005
INFOSECURITY EUROPE
Location: London, UK
Website: www.infosec.co.uk

5 - 6 May 2005
CLA 2005 World Computer and Internet Law Congress
Location: Washington DC, USA
Website: www.cla.org

12 - 13 May 2005
RSA Japan
Location: Tokyo Prince Hotel, Tokyo, Japan
Website: www.rsasecurity.com/conference

13 - 15 June 2005
CSI NETSEC
Location: Scotsdale, Arizona, USA
Website: www.gocsi.com

26 June - 1 July 2005
17th ANNUAL COMPUTER SECURITY CONFERENCE
Location: Singapore
Website: www.first.org

23 - 28 July 2005
BLACKHAT USA
Location: Las Vegas, USA
Website: www.blackhat.com

17 - 19 November 2005
RSA Europe
Location: Vienna, Austria
Website: www.rsasecurity.com/conference

14 - 16 November 2005
CSI 32nd ANNUAL COMPUTER SECURITY CONFERENCE & EXPO
Location: Washington, USA
Website: www.gocsi.com