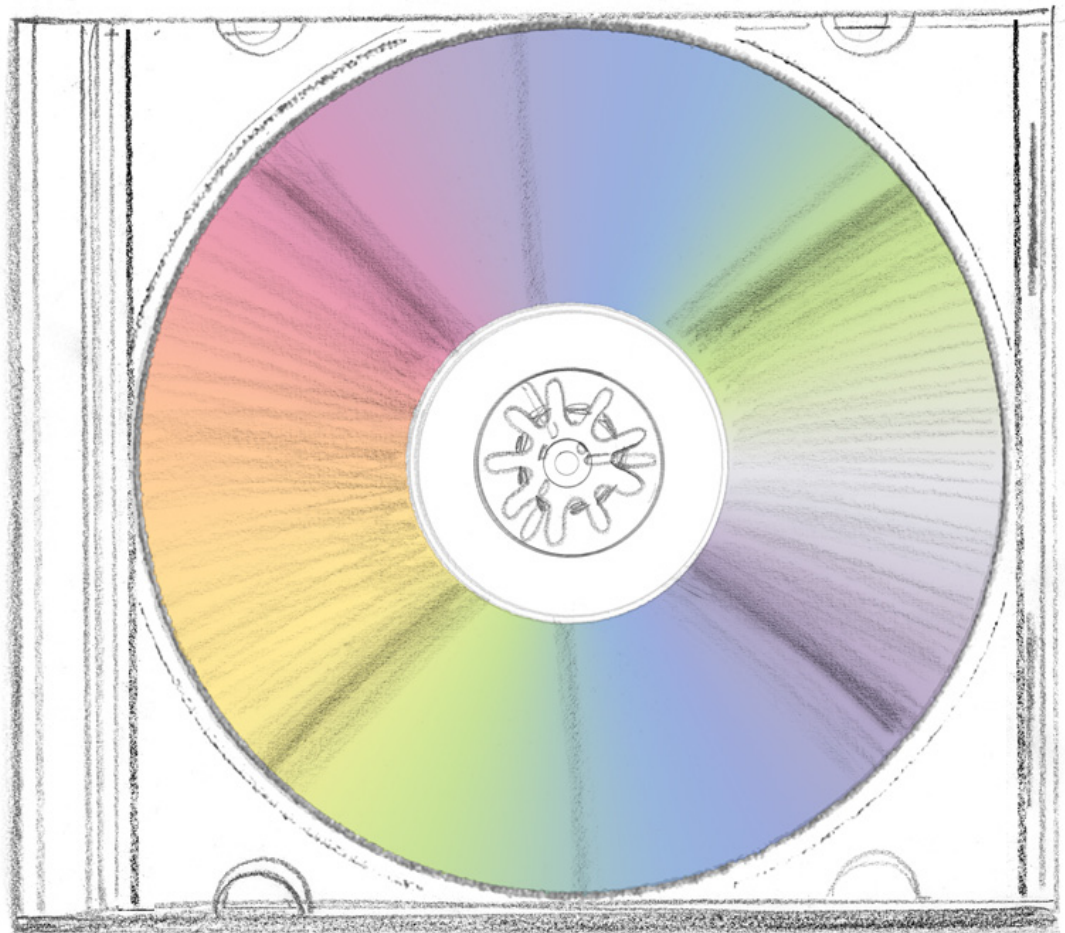


Data leakage and data compromise

Causes and preventative steps

Pearse Ryan and Andrew Harbison



Contents

| | Page |
|------------------------------------|-------------|
| Overview | 2 |
| Increase in data incidents? | 4 |
| Data preservation and data leakage | 6 |
| Types of data incident | 8 |
| Conclusion | 14 |

Overview

If you follow the news, it will appear that there has recently been an upsurge in cases of data leaks from both private and public organisations. The list of incidents in the public domain is lengthy and ever-growing. Recent months have seen the loss of 25 million welfare recipient's records from the UK Department of Internal Revenue, 600,000 records from the UK Ministry of Defence and 1.6 million records from the Monster.com recruiting web-site. Closer to home, Bank of Ireland admitted the loss of four laptops containing the personal details of thousands of clients.¹ Here have even been reports recently of UK ministerial aides having their PDA's stolen, possibly, we are led to believe, by Chinese Intelligence Agents.²

This article will discuss the topic of data leakage and data compromise, asking the question, how can they be prevented and, if not possible, then, how can their consequences be managed or mitigated? This article is the first in a series, with subsequent companion articles discussing data destruction/data retrieval, computer counter-forensic measures/electronic evidence, and Irish statutory computer fraud offences. While these articles will be written from the Irish perspective it is hoped that they will be of general interest.

Before we continue, we need to consider the difference between data leakage and data compromise. The term 'data leakage' we define as referring to instances where private or confidential information is copied or moved from its authorised location, either with or without third party intervention.³ The term 'data compromise' we define as referring to instances where data leakage results in information falling into the hands of unauthorised parties. Thus, whilst all data compromises involve data leakage, the converse is not necessarily true. The term 'data incident' we define as referring to instances of both data leakage and data compromise.⁴

The problem with the majority of incidents discussed in this article was not that the data in question was leaked per-se, but rather that it was not clear where the data had been lost to and who might have ended up in possession of it. In the Internal Revenue case it was not clear in whose possession, if anyone's, the missing data CDs had ended up. In the Monster case, it quickly became apparent that the data had been compromised to hackers, because the stolen data

¹ See statement dated 22/04/08 of Data Protection Commissioner into investigation into theft of personal data on BOI laptops – <http://www.dataprotection.ie/viewdoc.asp?>

² http://www.schneier.com/blog/archives/2008/07/the_case_of_the.html

³ By "moving" data we mean the copying of data from X to Y, involving the deletion or original copy located at x. By "copying" data we mean the retention at X of the original copy.

⁴ The applicable data protection legislation in Ireland is the Data Protection Acts 1988 and 2003 (the "DPA").

was used as the basis of a phishing-type internet scam aimed at defrauding the individuals whose data was stolen.⁵

⁵ http://www.theregister.co.uk/2007/08/21monster_trojan_steals_millions_of_records/

Increase in data incidents?

In reality, contrary to what one might believe from the media, it is unlikely that there has been any major upsurge in actual numbers of data incidents. In all likelihood data incidents have been occurring since mankind first committed words to clay tablets. Instead, what we are observing is a massive increase in the amount of data being lost, allied to an interested if not hyper-interested media, reflecting we hope growing public awareness of the issue of protection of personal and non-personal data.

This increase in apparent data incidents is the result of two main factors:

- firstly, people are becoming more aware of the issue of data leakage by organisations to which it is entrusted, while the organisations themselves are coming under greater legislative and cultural pressure to admit to such incidents. Hence, data incidents are receiving far more publicity than they have in the past. This in turn is because, with the advent of the internet and the corresponding explosion in cyber crime, leaked information has the potential to travel much further, and do much more damage than ever before;⁶
- secondly, as the capacity of portable data storage devices increases exponentially, the sheer amount of data being stored in a generally highly portable medium means the potential for a catastrophic data compromise is all the greater.⁷

In the past, where records were stored on paper, there was only so much information that could be conveniently carried, and thereby stolen or lost at any one time. The recent rapid development of portable data storage means that vast quantities of data can be carried in a jacket pocket, and more on the hard drive of a laptop computer or other portable device. To put this in context, **Tolstoy's War and Peace or Tolkien's Lord of the Rings, can each be stored using less than 4 Megabytes of memory**, without compression. All of Shakespeare can be stored in less than 10 megabytes. It has reached the point that if you walk into any bookshop, the hard drive on one cash register is likely to have more data storage capacity than all the shelves in the store put together.⁸

⁶ The Irish DPA impose certain obligations on data controllers and data processors with respect to the maintenance of security of data, e.g. by requiring that the data controller must ensure the security measures adopted provide a level of security appropriate to: (a) the nature of the information concerned; and (b) the harm that may result from a security breach. This is particularly important given that data controllers and data processors owe a duty of care to data subjects under the DPA.

⁷ See article – “Tiny Storage Devices pose biggest data security risk”,

⁸ We sometimes forget just how recently USB flash drives were developed. The first commercial USB pen drive was released by IBM in December 2000. It had a capacity of 8Megabytes. At time of writing, an 8

Consequently, it is possible (as has happened in the last year) for a junior member of staff to mishandle and lose vast amounts of confidential data, simply because it is stored on a small, easily lost 'gadget'.⁹

Careless handling of data storage media and devices is a very common cause of data incidents. It is made worse by the fact that in many organisations there is often a great number and variety of media and storage devices in use, making data loss all the more likely.

Gigabyte USB pen drive, with a thousand times the capacity of this original device, can be purchased for around €20, and pen drives with 64GB and 128GB capacities are readily available commercially. Computer hard drives with 1.5 terabyte (1,500 gigabytes, or 1.5 million megabytes) capacity may be readily purchased. To put this in context, the entire written collection of the US Library of Congress could be stored on around 14 of such drives. It is predicted that by 2012 it will be possible to store the entire Library on a single hard disk drive.

⁹ The obvious example is the loss of 25 million child benefit records by Her Majesty's Revenue and Customs in November 2007.

Data preservation and data leakage

Data destruction, where data stored on computer systems is overwritten or where the media storing the data is damaged or destroyed, is a common problem for organisations. By far the most common causes of data destruction are hardware and software faults, or mistakes made by people in the normal operation of their computers; accidents in other words. Circumstances where data is leaked or compromised, rather than destroyed, are much rarer, comprising perhaps less than 10% of total events.¹⁰

In general this is because data leakage usually requires some kind of human intervention, whereas data destruction is most commonly a result of hardware or software failure and requires no human involvement. Most people only use their computers for a few hours a day, whereas a computer fault can occur at any time the computer is switched on. Furthermore, intuitively one might expect incompetence in any field will be more likely to result in simple destruction than more complicated outcomes, and it appears that this is as much the case with computer systems as it is in any other form of human endeavour. Hence a mistake with a computer system is far more likely to ruin data than anything else.

Consequently, when data is destroyed inside organisations, through hardware or software failures, or through human error, there are usually measures in place to ensure that it is not lost permanently. Organisations now typically keep multiple copies of key data on multiple systems, often in different locations.

Unfortunately, this profusion of duplicate data greatly increases the amount of data that might potentially leak and, therefore, the likelihood that a data incident will occur. For example, perhaps the most devastating data leak a company can suffer is the loss of its backup tapes. Most organisations now take disaster recovery backups of their computer systems at regular intervals - generally daily or weekly. These backups necessarily store all data of value to the organisation.

If a thief targets a single laptop or USB drive, they may recover something useful, or they may not. If they steal the backup tapes they steal everything. The only problem is likely to be that there is so much data stored on a set of backups, it is likely to take some time to find something useful. It is we believe fair to say that many organisations are careless with their backup tapes, although this trend is reducing as, firstly, data security becomes a greater issue and, secondly, with

¹⁰ Kroll Ontrack <http://www.protect-data.com/information/statistics.html>

the increase in out-sourcing, bringing with it more rigorous application of standards and procedures.¹¹

Similar issues arise from the fact that modern data storage systems are designed to be reasonably durable, so that data will be protected from routine wear and tear on the systems that store them. Networks are designed with redundant arrays, servers, backup tapes and other devices to ensure that data is preserved. Even when these don't work, companies can engage IT forensics and data recovery specialists to try to retrieve the lost data. Much time and thought has been given to how to bring lost data back and methods have been developed that are often highly effective. Data preservation is again the priority.

Unfortunately, in data incidents, this emphasis on data preservation may be very much to an organisation's disadvantage. When data is lost outside the organisation, on stolen laptops, lost CDs and pen drives, accidentally or otherwise, it may well be preferable from the viewpoint of maintaining data security that the missing data not be preserved, so it cannot be retrieved and used by people who might come into possession of it. Some products are now available that allow for laptops to be remotely erased in event of loss, but our experience of a great many companies and organisations suggest that this technology is not commonly used.¹²

¹¹ In one example, an IT manager had adapted the habit of taking the Friday back-up tapes home for the weekend, a habit not continued into an outsourcing of IT operations.

¹² An example is www.computrace.com. As to why organisations have not embraced this remote kill technology, it seems generally to relate to a fear of accidental or malicious triggering as well as an increased onus on laptop and remote backup.

Types of data incident

There are as many ways for data to leak as there are methods of storing it. In our experience there are four broad ways that data can be leaked or compromised by organisations. Firstly, data can be inadvertently leaked, over e-mail or through an organisation website, or even over the telephone. Secondly, data can be lost, accidentally with the computer or media on which it is stored. Thirdly, data can fall into unauthorised hands, when computers or media are disposed of at the end of their operational lives. Fourthly, and most damagingly, data can be stolen deliberately by insiders or outsiders to the organisation. We look below at each of these four data incident routes and consider how they might most effectively be closed off or, at least, narrowed.

- **inadvertent release of information:** “loose lips sink ships” they used to say, and it remains as true as ever. Although today the inadvertent slip that places critical or damaging information in the public domain is as likely to occur on the web-site or an e-mail account as it is in a conversation.

Despite organisations’ best efforts over the last few years, users continue to use e-mail to distribute sensitive information. E-mail is culturally seen as a communications medium where informality is acceptable. **One of the most low lying fruit for the intrepid IT forensic specialist is to examine a suspect’s e-mail account, because if they are likely to have made a mistake and committed an indiscretion, it is most likely to be found in there.** Messages sent through web-mails, services like Hotmail, Yahoo Mail or Google Mail, are often the most indiscreet. Users often assume that their office e-mail may be monitored (in truth they rarely are), or at least that their employers may have access to them, and so reserve their greatest indiscretions for what they think is a private, untraceable medium (something which, again, they are often wrong about).

Some organisations have dealt with this problem by blocking access to web-mail from their sites. This has a number of advantages. It certainly cuts user access to the mode of communication most likely to cause a data leak. It will also result in considerable saving in network ‘bandwidth’ not taken up by employees perusing their web-mail. The disadvantage is that it guarantees that any indiscretion or defamatory statement will be made using the organisation’s own domain name, often in an e-mail containing the organisation’s logos and disclaimers. This increases the chance of any injured party pinning at least some of the blame on the organisation rather than the individual, leaving the organisation more likely to be found legally liable for the offending communication.¹³

¹³ Potential legal issues run the gambit of the common law, from criminal law matters to civil law contract and defamation matters, all depending on the nature of the communication.

Although e-mail leaks are common they at least have the advantage that they are usually limited in scope. You will get the occasional disaster where someone hits the 'reply all' button instead of "reply" and sends a private e-mail to a large group of people. Most e-mail users will also have seen instances where a user has 'cc'ed a list of e-mail recipients rather than using 'bcc'. This of course provides a list of e-mail recipients to everyone receiving the e-mail. This may not always be a problem, but there are certain circumstances when it is. However, such incidents are in the minority.

The best solution to this problem is training. Staff must be made aware of the kinds of disasters that can be initiated by carelessly sent e-mails. There are plenty of good examples on the web. **All too often staff act as if there is an 'unsubscribe' button, when of course, there never is.** Another solution far too little used is proper data management. Staff cannot leak data they do not have, and it is always good practice to ensure that staff members are restricted to the data they actually need. Of course, determining what kinds of data staff need is not always straightforward and nor is the monitoring of access and use thereafter (not to mention the cost involved), but many of the more severe data leakage disasters of recent years would have been averted if proper data management procedures were in place.

One limiting factor on the damage such incidents can do is that, with a few well publicised exceptions,¹⁴ **e-mail indiscretions have a limited audience. Web-indiscretions are potentially far more damaging.**

Historically the most common, and damaging cause of data leakage on web-sites have been through bad programming, which has allowed visitors into areas of web-sites they should not have access to¹⁵ or exposed data transfers to and from their web-server leaving them vulnerable to being intercepted by eavesdroppers.

The premature release of sensitive information, such as financial reports, is a problem that has embarrassed many organisations. Typically this has occurred when IT personnel have set up the sensitive information on their web-sites well in advance of the formal release time, only to have search engines or inquisitive web-site visitors discover the hidden material and release it prematurely. This can be embarrassing at the very least, and may place the organisation concerned in regulatory or legal peril.¹⁶

- **accidental loss of information:** perhaps the best publicised data leakage disasters in recent years have involved the loss or theft of computer equipment. We include the theft of laptop computers in the accidental loss category, because in the vast majority of cases the laptops are stolen for their own intrinsic value, rather than the value of the data stored upon them. It is well known in criminal circles that laptop computers are both easy to steal and easy to fence afterwards. They are, by their very nature, portable. The 2007 CSI Annual Computer Crime and Security Survey,

¹⁴<http://www.guardian.co.uk/technology/2000/dec/15/internetnewsbusiness.timesonline.co.uk/tol/business/columnists/article1336281.ece>

¹⁵ <http://www.msnbc.msn.com/id/4186130/>
<http://thedailywtf.com/Articles/Oklahoma-Leaks-Tens-of-Thousands-of-Social-Security-Numbers,-Other-Sensitive-Data.aspx>

¹⁶ For Example: http://www.rba.gov.au/MediaReleases/2000/mr_00_06.html and <http://kerry.senate.gov/cfm/record.cfm?id=298714>

carried out in the US, reports that 50% of responding companies suffered a laptop theft in the previous 12 months.¹⁷

The fact that you are only one of many affected is not much consolation if your name, personal and financial details are on the stolen laptop, after all, as we've noted already, you cannot be sure where the data is going to end up. One of the disadvantages of increased publicity about data loss is that a growing number of thieves are now becoming aware of the value of data on the computers they steal. Laptops are not the only problem. USB pen drives are increasingly ubiquitous. It is not uncommon for individuals to own a handful of such devices. Branded USB devices are often given away free at conferences and other events. The problem is that these devices can hold vastly more data than the floppy disks of old, and because they are cheap people tend not to notice when they go missing.¹⁸

As a countermeasure, encryption of devices is an effective protection against data loss. Most types of data storage devices can now be purchased with on-board encryption, for relatively little extra cost. Unless the data thief can gain access to the encryption keys that will release the data on the device (no trivial exercise, even for trained IT forensics specialists) any data on the device is likely to remain irretrievable. Encryption is not foolproof however. Most encryption systems store their keys in password protected 'keystores' on the device itself, so that breaching encryption becomes a matter of defeating the password rather than the encryption keys. Passwords are unlikely to be anywhere near as complex as the keys so this makes the task a good deal easier.

A more serious problem has been uncovered in the last few months. Many encryption systems keep their keys in computer memory while the computer is switched on. In theory, if the computer is switched off, the memory is cleared and the keys are lost. Scientists in the US have recently found that this may not necessarily be the case. If the computer in question is kept reasonably cool (heat can cause the data retained in memory to deteriorate) the keys may be retained in the switched-off memory until the computer is rebooted. If the computer can be started in such a way that the memory is not reset, the encryption keys might be recoverable.¹⁹

Notwithstanding these problems, encryption is more than sufficient to deter casual data theft, and properly implemented it is proof against sophisticated attempts at stealing confidential information. Implementing encryption, at least on portable devices, is now expected of organisations holding personal data, and loss of data containing client information in the absence of encryption can now be interpreted as a serious breach of fiduciary duty. An example is the substantial fine handed to Nationwide Building Society in 2007, by the UK Financial Services Authority over the loss of a laptop containing customer data.²⁰ It is at least an issue organisations' legal advisors need to start raising with their clients.

¹⁷ CSI. 12th Annual Computer Crime and Security Survey. 2007

¹⁸ In fact a major factor in the recent loss by PA Consulting of a USB Pen Drive containing the names and addresses of 87,000 individuals may be the fact that the device had a 32GB capacity. At the present time this is an unusually large capacity drive, and the device would have been considerably more valuable than a normal pen drive, so its loss would have been more likely to be noticed.
news.bbc.co.uk/1/hi/uk_politics/7575989.stm

¹⁹ Halderman J.A., Shoen S.C. et al. "Lest We Forget: Cold Boot Attacks on Encryption Keys" Proceedings of the 2008 USENIX Security Symposium Princeton University
<http://citp.princeton.edu/pub/coldboot.pdf>

²⁰ <http://news.bbc.co.uk/2/hi/business/6360715.stm>

- **careless disposal of information:** another problem facing organisations is what to do with computers and other storage media when the time comes to dispose of them.²¹ Simply deleting a file or formatting a hard drive does not remove the data stored on it (a fact that underpins the entire IT Forensics industry). Computers are designed to store data quickly and reliably. This means, conversely, that they are not as effective at removing this data when required. **For most modern computer and data storage devices this means that deletion of information is not the same as erasure and that deleted material can often be straightforwardly recovered.**

The consequence of this fact is that organisations need to be careful about how they deal with old computers. Many send their redundant machines to waste disposal companies, not knowing whether or not the company will choose to recycle the hard drive (usually the most valuable sub-component of any old computer) or dump it in a landfill. Old hard drives regularly turn up for sale on eBay and other auction sites, or are sold on-line by scrappage companies. In the past these were mainly sold as spare components for out of date computers. Today many hackers will buy such drives looking for data, knowing that they can re-auction the drives later after they are finished with them.²²

Even organisation's charitable actions can come back to haunt them. Many companies hand their old computers over to charity for use in the Third World or by other deserving causes. Unfortunately, many do not thoroughly erase the contents of these computer's drives before they are handed over. Handing a computer over in such circumstances is akin to handing a filing cabinet over without first emptying it out. The principal difference being that even a four year old computer is likely to hold as much data as hundreds of filing cabinets.

There are many cheap and reliable programs that can be used to erase hard drives prior to disposal. Many organisations wipe to the standards set out in the US National Industrial Security Program,²³ which requires the overwriting of each data byte on the disk three times with random data. This is because the data hard on hard drives is stored magnetically, and one overwrite may not be sufficient to completely remove the magnetic pattern of data previously stored on the disk.

In truth, for most normal applications a single wipe is sufficient to securely erase a computer's hard drive. While it is possible that data may be recovered from a disk that has been wiped just once, doing so requires a considerable amount of expertise and sophisticated (meaning expensive) equipment. Extraordinary disk wiping measures can probably be safely reserved for hard drives containing highly sensitive information. **A more aggressive, effective (and, indeed, satisfying) method of rendering the data on a hard drive beyond recovery is to hit the drive a number of times with a hammer.** Hard drives are fragile, and the shock should be sufficient to shatter the data storage platters and ruin the mechanism, preventing even a rebuild of the device. Replacement hard drives are not expensive, (we have noted already they can be bought on eBay) so destroying the original does not necessarily preclude any retired computer from being sold or given to charity.

²¹ For instance, http://news.bbc.co.uk/2/hi/uk_news/scotland/south_of_scotland/5339204.stm

²² <http://www.techweb.com/wire/security/showArticle.jhtml?articleID=177105302>

²³ Often known as the "Department of Defence 5220.22-M standard" after a key program document on the handling of classified information.

USB devices are simpler. They do not store data in magnetic patterns, but in electrical potentials within their chips. Once the data is overwritten once, it is fully erased. Most disk erasing applications will sanitise USB pens as well as hard drives.

- **deliberate theft of information:** theft of computer based information is a serious and increasingly common problem for organisations. Anecdotal evidence seems to suggest that the majority of data theft is carried out by organisations' own employees, with most events occurring when individuals leave the organisations in question. While little formal research has been published in this area, much of that which has been carried out appears to support this view.^{24 25}

In Ireland, theft of information by individuals leaving their employers seems to have become epidemic. The principal method of data theft appears to be by means of portable USB devices, such as pen drives, or larger capacity USB portable drives. As discussed already, such devices can now hold large quantities of data, which can be copied quickly and reasonably invisibly at any time. A less common method of data theft is over e-mail. We find that this is less common than in the past, as potential data thieves will typically expect that this method is more likely to leave a trace. In fact theft of data using USB pens is also relatively easy to detect.

Preventing theft by departing employees is difficult. The problem is that they may need to have access to sensitive or confidential information in order to perform their jobs, and they often copy the material they intend to take with them before they give notice of their resignation.

As with most other forms of data loss, proper data management policies and procedures will minimise the risk, ensuring that a potential data thief will only have access to the minimum practical amount of data. Another approach, becoming increasingly common, is to restrict the use of USB devices on computer networks. A number of computer applications are now available that allow IT administrators to centrally manage the USB ports on all computers on a network.

If USB pen drives must be used on a network, it is important that such devices be restricted to only those actually owned and issued by the organisation. This means that if any attempt is made to use them to remove data from the network, they can at least be retrieved and examined without resorting to complex and expensive litigation (often necessary when leavers use their own USB drives to copy data). This restriction might well be expanded to any device attached to an organisations network.

We have heard anecdotal accounts of the deliberate targeting of corporate laptops as part of attempts at intelligence gathering or industrial espionage. It is our experience that such methods are rarely, in fact, practical. In simple terms it is typically more straightforward, effective and covert, to plant a 'trojan horse' or other 'backdoor' program on a victim's computer than it is to steal it. Stealing a computer automatically sets off the alarm bells, planting a trojan does not. In any case, as discussed already, perhaps the most useful item for a potential data thief to steal would be an organisations tape backups, not least because it might take some time for the theft to be detected, if it is detected at all.

²⁴ McAfee and Datamonitor's Data Loss Survey, 2007 (*requires registration*)

²⁵ The 2007 Annual CSI FBI Security Survey dissents, but has glaring inconsistencies, for example 50% of respondents reported laptop or mobile device theft over the period of the survey, but only 25% reported unauthorised access to information, and even fewer, 17%, reported theft of customer or employee data – leaving us to wonder what was stored on the devices which were stolen.

Hacking remains a problem, although less than it used to be. **Hackers have found that it is more profitable to carry out widespread frauds such as 'phishing' attacks, based more on confidence trickery than technical expertise, rather than go to the trouble of hacking individual targets, however large.** The days of the highly skilled hacker slowly infiltrating his way through system after system to reach the heart of a network are long gone.

In recent years when companies have been compromised it has often through the use of Trojan horse programs. Some of these have been placed in the conventional way, by duping an employee into running a program sent to them through e-mail, or internally, by subverting a member of staff (usually in IT). Modern hackers are mostly interested in financial information - names, addresses, credit card and bank account numbers, but not exclusively. In the Monster hack, mentioned above, no financial information was stolen. Instead the hackers used the stolen personal data to write highly convincing phishing e-mails which allowed them to defraud many of the site's users.

Old fashioned hackers could be deterred by technical means alone, which is why as species they are very much endangered. Modern hackers do not attack computers so much as the computer users. **It is a well known hacker's rule that the 'wetware' (the human element) is the least secure component of any computer system.** Technical 'silver bullets' are therefore of limited value in securing modern networks.

Staff training, combined with the proper secure configuration of computers and networks and implementation of comprehensive ICT use policies, can keep hackers out. Perhaps the biggest problem for IT managers in delivering this is the generally low awareness of potential threats among senior executives. For instance, after the Monster hack the company put out a statement suggesting that customers should not be concerned because no financial details had been stolen, even as the first were being defrauded using the information that had been stolen.

Conclusion

Data incidents are a major concern for the integrity of organisation data, whether commercial or administrative/public sector data. IT professionals are well aware of the risks in the area. This awareness has made its way into the general business community and, more lately, into the public consciousness. After all, the data lost or leaked is likely to be yours or mine and typically it is us, the general public, who are the target of the party seeking to use (generally personal) information.

Data leakage is statistically more likely than data compromise. Data leakage is an administrative and business risk issue as old as the maintenance of organised forms of data retrieval. One can imagine the ancient Greek merchant searching for that month end financial statement which was just here a moment ago. Data compromise is an equally old problem, but if technological advances have done one thing they have greatly increased the options available to the thief.

There is as they say nothing new under heaven and earth. The authors are not so bold as to suggest a solution to the problem of data leakage and data compromise. There can be no single solution to issues of human nature. What we do suggest, however, is that business and organisations take appropriate internal precautions, including policing or enforcement, to:

- reduce the possibility of data leakage;
- reduce the possibility of data compromise; and
- mitigate against the adverse effect of each on the business or administration.

Contact

Pearse Ryan is a partner in the Technology and Life Sciences Group at Arthur Cox, Dublin. www.arthurcox.com. **Andrew Harbison** is Director in the Forensic and Investigation Services Group at Grant Thornton, Dublin. www.computer-forensics.ie.

This article was originally published in Computers and Law (www.scl.org).

Contact

Andrew Harbison

Director – IT Forensic Lead, Forensic and Investigation Services

D +353 (0)1 6805 766

M +353 (0)86 0407 211

E andrew.harbison@grantthornton.ie

24-26 City Quay, Dublin 2

Offices also in Limerick and Kildare

This briefing is provided for general information purposes only and is not a comprehensive or complete statement of the issues to which it relates. It should not be used as a substitute for advice on individual cases. Before acting or refraining from acting in particular circumstances, specialists advice should be obtained. No liability can be accepted by Grant Thornton for any loss occasioned to any person acting or refraining from acting as a result of any material in this briefing. Grant Thornton, Irish member of Grant Thornton International, is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business. www.grantthornton.ie. © 2009 Grant Thornton. All rights reserved.



Grant Thornton

Member of Grant Thornton International
Authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.
© 2009 Grant Thornton. All rights reserved.