# Data leakage

Data leakage is the “ unauthorized or unintentional exposure, disclosure, or loss of sensitive information” (GAO, 2007, p. 2). Many businesses have in their control sensitive data about their organisation, employees and customers. The Information Commissioner (ICO) in a recent press statement (ICO, 2010) is alarmed with the “ unacceptable” number of data leakages within the modern world and will issue fines for major breaches to commence in 2010.

“ In addition to our markets, the safety and security of our information could not be assumed either.” (Verizon Business, 2009 p. 2). In 2008 there appears to be a link between the turn of the recession and an increase in reported data leakages. Research conducted by Verizon Business (2009) showed that the number of reported compromised records was more than the previous four years combined as shown below in Figure 1. 1.

Figure 1. 1 – Number of records compromised per year in breaches investigated by Verizon Business (2009)

Within this study (Verizon Business, 2009) it was found that the industries with the highest number of data leakages were in retail (31%) and financial services (30%).

“ As employees exit, so does corporate data” (Ponemon Institute, 2009, p. 1). A survey conducted (Ponemon Institute, 2009) showed 59% of employees who left a business (including voluntarily and those asked to leave) stole data.

It is difficult to measure the entire impact of a data leakage. “ Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown”. (GAO, 2007, p. 1.) The financial impact on a business per breach according to the Ponemon Institute (2006) is on average $4. 8 million. Breaches can not only be financially costing to a business but also extremely damaging to a company’s reputation, this study (Ponemon Institute, 2006) showed that 60% of customers terminated or considered terminating contracts after a security breach.

According to Verizon Business (2009) in 2008 91% of all compromised records were linked to organized criminal groups. Examples of confidential data that criminal groups may wish to obtain are company’s financial information, customers’ sensitive data and credit card details.

There are many ways in which data leakage can occur, some of which will be discussed in the following chapter of this report.

## 1. 2 Data Leakage in the Media

The media is one of the most influencing ways of communicating issues globally. Data leakage appears to be increasingly more popular in the media as the reported breaches increase. The ICO stated that there were 434 organisations that reported data security breaches in 2009, the previous year had 277 reported (“ Unacceptable” level of data loss, 2009). This evidence supports the theory of there being an increase in breaches during the recession but what must be taken into account is that there is an increase in the “ reported” cases. It may be that more businesses are

becoming aware of data leakages where previously they were oblivious to breaches committed or did not disclose the known leakages.

Reported in the media, a Nationwide employee's laptop was stolen from their home containing confidential customer data (FSA, 2007). 11 million Nationwide customers were said to be at risk of identity crime at the time. The FSA (Financial Services Authority) were alerted by the breach and it was found that the Nationwide did not start an investigation until 3 weeks after the theft took place. The firm were fined £980, 000 by the City watchdog for the security violation.

Another example in the media (Previous Cases of Missing Data, 2009) is the Ministry of Defence data security breaches. The Ministry of Defence admitted to losing or having stolen 121 memory sticks in a four year period. According to this press release (Previous Cases of Missing Data, 2009) Defence Secretary Des Browne said 747 laptops had been stolen of those only 32 have been recovered.

### 1. 3 Data Loss Prevention (DLP)

The protection of sensitive data, to avoid data breaches, should be a vital part of a business' day to day operations. " Yet organisations rarely have adequate visibility or control of their data" (Broom, cited in When financial data goes missing, 2008).

From the research conducted (Verizon Business, 2008) out of all the data leakages that occurred in the year 87% were preventable through simple or intermediate controls. This suggests that many businesses are not putting in adequate controls to prevent leakages.

The Date Protection Act (DPA) is “ a framework to ensure that personal information is handled properly” (ICO, The Basics, no date). One of the principles of the act is, it is the responsibility of the business to “ secure” the sensitive data it withholds. The DPA have the right to prosecute and unless exempt, all businesses have to abide by this act.

The difficulty faced by many businesses is to manage the risk without affecting their productivity and to “ manage risk in a new and challenging environment” (CFO Research Services and Crowe Chizek and Company LLC , 2008, p. 2).

The important factors to consider when implementing a DLP plan is the alignment of process, technology and people as a unit. “ developing a robust security policy and ensuring that all employees fully understand their role and obligations”(Broom, cited in When financial data goes missing, 2008). Broom also stated that users need high-quality training and good communication regarding information security concerns.

## Chapter 2: Types of Threats

Threats to the protection of data can be split into two broad categories: Internal and External threats. Internal threats are from within the business itself and majorly centred on employees’ actions. Attacks from outside of the business are known as external threats. “ Examples include hackers, organized crime groups and government entities” (p. 8, Verizon Business, 2009)

According to Verizon Business (2008 or 2009??) 20% of reported data breaches are caused by insiders whilst 39% of the breaches involved

multiple parties, thus proving the importance of a combination of internal and external controls.

## 2. 2 External Threats

According to Verizon Business, 2008 saw " more targeted, cutting edge, complex, and clever cybercrime attacks than seen in previous years" (p5 2009). The fact that attacks appear to be increasingly more sophisticated is a concern for many organisations to ensure they have adequate control measures in place.

One of the most common external threats to data security is Malware. According to Easttom (p6 Computer Secuirty Fundamentals) Malware is the " Generic term for software that has a malicious purpose." Malware can be used to steal confidential data from a personal computer to a global network.

A virus is " a small program that replicates and hides itself in other programs, usually without your knowledge" (Symantec, 2003) through Computer security fundamentals p6.)

A Trojan Horse " is a useful or apparently useful program containing hidden code that, when invoked, performs some unwanted function." (P48 info sec pipkin). Trojans must spread through user interaction such as opening an e-mail attachment. It looks legitimate and so users are " tricked" into executing the malicious program. The Trojan can then potentially delete files, steal data and spread other malware. They can also be created to generate " back doors" to give hackers access to the system. (http://www. cisco. com/web/about/security/intelligence/virus-worm-diffs. html)

An example of a dangerous Trojan is the Dmsys Trojan. According to (http://www. 2-spyware. com/trojans-remova) and (http://www. uninstallspyware. com/uninstallDmsysTrojan. html) it steals user's confidential information by infecting instant messengers. It uses a keystroke logging technique to steal passwords and private conversations. This information is stored in a log file and then sent to the hacker. Thus allowing the malicious user to have access to potentially, confidential information. There are various tools online that can dispose of this Trojan automatically, but if a user wanted to do it manually they would need to delete the files: dmsysmail. eml and dat. log.

## Manually Deleting Malware

" Each program consists of files. Evenspyware, a virus or a different parasite – all have their own files"( http://www. 2-spyware. com/news/post203. html – ) To remove a " parasite" usually means to delete all its files. According to this website, it is not always this simple, as files being used by active applications can not be deleted and some of the Malware's files may be set to invisible. Following this site's guidelines:

Open Windows Task Manager and select End Process but only works if you know what processes should be running and those that look suspicious.

Once you have stopped the process it is now possible to try and delete the malicious files. Locate the folder you believe the program to be (eg My Computer) and ensure all hidden and protected files are visible (Tools, Folder Options, View, Advanced Settings). There may still be files that are invisible, now type " cmd" into run to access the Command Prompt. Within the

Command Prompt enter dir /A folder_name. All files within this folder will be listed including all hidden files. To delete these files within the cmd enter the command cd folder_name to locate the folder. Then enter del file_name to delete the file. Ensure the Recyle Bin is also emptied.

http://www. 2-spyware. com/news/post203. html – steps on how to manually remove Malware.

## Preventing Malware attacks

“ Since new viruses are introduced daily” (p49 info sec pipkin) an up-to-date valid anti-virus software is essential to avoid data leakages via Malware.

Vulnerability patching

firewalls

A combination of the mentioned attacks can be catastrophic to the security of data “ hacking gets the criminal in the door, but malware gets him the data” (p20 verizon) It is critical that a blend of the above security measures are put into place.

## 2. 1 Internal Threats

“ Whether knowingly or unknowingly, innocently or maliciously, employees engage in behaviours that heighten the risk of data loss.”( Cisco data leakage find page)

According to a study conducted by cisco data leakage 46% of employees admitted to transferring files between work and personal computers and approximately 1 in 4 admitted sharing sensitive information with friends, family, or even strangers.

According to the Deputy Information Commissioner David Smith (http://news. bbc. co. uk/1/hi/uk_politics/8354655. stm) “ Unacceptable amounts of data are being stolen, lost in transit or mislaid by staff.” Dangerous numbers of personal data is still being needlessly stored on unencrypted laptops and USB sticks.

“ if they do not think about security, users can start to cause quite a few problems” p37 computer insecurity book.

bar chart 5 ponemon 2009 – page8 – info kept after leaving

chart 7 ponemon 2009 – page 9 –

According to Ponemon (2009), only 11% of the respondents who took part in this research had permission from their supervisor to keep this information. in figure …. An alarming percentage of the above transfers may have been avoided with appropriate controls, which will be discussed later in this report.

It can often be hard to detect data leakages, such an employee copying confidential data to a USB device. “ more often, the information is left just as it was so that the theft is not quickly discovered” p59 info sec pipkin.

Using a Data Leakage Prevention tool can assist in monitoring and blocking users’ risky actions to avoid leakages. In this report Digital Guardian by Verdasys will be used to demonstrate some examples of how a DLP tool can be used to assist in the “ battle” of information security.

## Chapter 3: Verdasys Digital Guardian Software

### Introduction

“ Digital Guardian is a comprehensive and proven data security solution for protecting and tracking the flow of critical data anywhere in the world.” (Verdasys, 2006) (http://www. daman. it/wp/dg/Digital_Guardian_DS. pdf ) According to Verdasys (2006) Digital Guardian (DG) can help to prevent the loss of data by identifying “ hard to detect” user actions. The tool can block unauthorized access, copying, printing, and other user actions.

The DG platform consists of a central server and control console to communicate with remote agents deployed to desktops, laptops and servers where data needs protection. It is an agent based (Endpoint) Data Loss Prevention (DLP) tool. These agents operate silently and report rules violations, “ continuing to operate even when a device is removed from the network.” (Verdasys, 2006 http://www. daman. it/wp/dg/Digital_Guardian_DS. pdf ). The DG server is accessed via a web-based interface to the Control Console.

Figure … DG Management /Control Console

The above figure is the “ web-based” management console.

This tool can be implemented on both Windows and Linux machines. For this project Windows machines have been used.

### Capabilities

Digital Guardian can monitor or block various “ risky” actions users are taking. Whether it be users’ abuse or accidental operations. There are many actions that the software can perform some of which will be shown in the

following….. Rules can be created within the software and then applied to policies which are deployed to machines chosen. These rules can generate warnings to the user and also email alerts to administrators upon policy breach. Reports can be generated to allow for auditing and drilldown summaries of use of data and users' actions.

Along with being able to completely block specific actions DG can also ask for justification from a user which is a form of " Soft Blocking" (DG, 2006). This type of DLP can also allow for a monitoring only approach, which according to ( http://www. networkcomputing. com/wireless/time-to-take-action-against-data-loss. php) can be more successful than a blocking solution. It can be used assist in computer forensics investigations whether it would be monitoring triggered rules by prohibited actions that breach corporate policy or more sinister illegal activity. According to (http://www. networkcomputing. com/wireless/time-to-take-action-against-data-loss. php) The beginning of the investigative process is to find out what was being sent, where, and by whom. Is it legitimate business reasons? Maliciously? They didn't know any better? " Blocking may keep the data safe, but it won't answer those questions." (http://www. networkcomputing. com/wireless/time-to-take-action-against-data-loss. php)

There are functions within the tool that can block the removal of confidential data via clipboard actions (cut/paste/print screen).

add on features such as mail/file encryption and content inspection by Autonomy??…… (company name)

(Verdasys 2006)

Figure (…) shows the capabilities of the software,

**How the software works**

Digital Guardian installs drivers that tie into the Operating System (O/S) at a very low level within the kernel. When an application wants to save a file, it calls a function within the application that does this, and that the O/S handles the task, right down to the kernel that does the hard work, without application writers having to know the details. DG ties into that kernel, detects these events happening, extract useful details (like the filename and size etc), and then send the details onto the DG server. The advantage of this is that any application saving a file will have to get the O/S to do it, so tying in at that very low level ensures it works for virtually all applications. Any more??

Installation – oh god try and remember!! Installation details of .. appendix. windows server, SQL Server, DG Server, DG Agents, Hardware and Software … pre , key etc. Detailed in the "…. Digital Guardian files".

Limitations —- FIND some

Digital Guardian is mainly used for insider threats and doesn't lessen external threats by intruders or malicious attacks. It also does not address server and network vulnerabilities.

(http://www. software. co. il/data-security/17-data-loss-prevention-shoppers-guide. html)

No functionality to actually block users downloading applications (CHECK THIS) and running them if not already blocked within " Application

Management”. The software has to be installed on the network to be able to block the use of it. ??? check!!

No rule to be able to block all attachments sent via email?? check

Scalability challenge of maintaining classifications of Windows shares/content????

(http://www. software. co. il/data-security/17-data-loss-prevention-shoppers-guide. html)

## Chapter 4: Testing and Implementation –

## Policy Exception USB

Encrypt Email Prompt

Encrypt Mail Rule

Encrypted Email Password

Application Management

Application Management Exceptions

Application Management Exceptions

Block of Applications Prompt

Upload Via Webmail

Upload via Webmail Prompt

Block upload via webmail sites. This rule controls users access. Instead of completely blocking their access to certain sites…. Can access the specified

sites but can not upload to these sites. For example social networking sites like Facebook. Stops the sending of attachments via webmail. … If laptop accessed from outside of network these rules will still function…..

**NEED BETTER SCREEN SHOT THAN THIS??**

**IS THERE A COMPONENT RULE FOR THIS?**

**Control of USB Devices**

**Block non-approved USB devices**

Within DG it is possible to block all uploads to all USB devices, thus preventing all users from removing any data from the network. It is also possible to block uploads to USB devices with the exception of predefined USB devices. For example if a business provides users with an encrypted USB device (such as Kingston….) a rule is created to say block all USB device if stated device is not listed in the component rule associated. The USB device is recognised by its Product ID and Vendor ID. These IDs can be discovered by using a simple tool such as ……..

Block non approved USBs

Above is the control rule called “ Block non approved USBs”. This rule is set to block any File Copy/Move/SaveAs to a removable device that is not listed within the function (component control rule) “ approved usb device”.

Component rule for USB Approved

Within the “ approved usb device” component rule is the Vendor Id and Product Id for the approved USB device(s).

USB Block Prompt

If the USB device inserted does not match the predefined “ approved” removable device then the above prompt is triggered. This prompt is flexible and any message the administrator wishes to set will be displayed. Once “ Close” is selected no data can then be transferred to the device.

This way if the USB device is lost/stolen it is encrypted so would be extremely difficult to view any sensitive contents on the device without knowing the password. This rule could be useful for businesses where their employees have to travel regularly (eg Sales) and so data needs to be easily transportable. Obviously this rule does not stop users from stealing the data but does assist with accidental loss. The software could still be used to monitor who/what/how much data is being transferred to these devices.

**BETTER SCREEN SHOT??**

Content inspection rules…. Look into

TRY AND CRACK/BREAK THESE RULES.

Manually blocking USB within the Registry

It is possible to manually block all USB devices via the registry. The following steps were taken from Microsoft’s Support site (http://support. microsoft. com/kb/823732).

Before manually adapting the registry it is strongly recommended that a backup of the registry is made as any errors made within the registry can cause severe problems.  To enter the registry of the computer from the Start menu click Run and enter “ regedit”.  Find the registry key : HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesUsbStor. On the

right hand side double click " Start" as highlighted in figure……. Ensure Hexadecimal is highlighted and enter 4 within " Value data". This will now block all USB devices being used on this machine. When a device is plugged into the machine the device will not be acknowledged. To re-enable USB devices follow the same steps above but change the " Value data" back to the default value of 3.

## Chapter 5: Analysis of results founded by Digital Guardian.

### Digital Guardian Technology–

ANY IMPROVEMENTS FOR DG

## Chapter 6: Critical review of other products

Having assessed an Endpoint (agent based) DLP tool, secondary research was conducted on a Network DLP tool, Websense Data Security, for comparison.

Figure below is a table of brief pros and cons for different DLP measures available, taken from informationweek. com . Analyse table

Taken from (http://www. informationweek. com/1163/163ss_impactassessment690. jhtml; jsessionid= WA0XH3S4GN0CTQE1GHPSKH4ATMY32JVN)

" WhenDLPvendors are being honest, they'll readily admit they can't stop the serious and skilled insider from getting data out." (http://www. networkcomputing. com/wireless/time-to-take-action-against-data-loss. php)Their real significance is in finding employees who are accidentally leaking data, those who don't know it's against policy or who are taking risky shortcuts to get their jobs done.

Websense Data Security is a network based DLP tool with forward proxy. According to a review by (http://www. software. co. il/data-security/17-data-loss-prevention-shoppers-guide. html) it is typically used for monitoring email traffic and quarantining suspect messages. It requires placing an application-layer proxy next to an Exchange server or server agent.

With a network based DLP such as Websense it avoids having to install an agent onto every machine, and instead involving installing network taps. As data passes through these it is checked, and events collected that way.

According to(http://www. networkcomputing. com/wireless/time-to-take-action-against-data-loss. php) Network-based solutions have the potential to be more vulnerable to an insider threat. An insider can steal data out via thenetwork, using encryption or steganography (where data is embedded within another data format).

Unlike DG a network-based tool would not prevent a user plugging in a USB stick and copying files, it also would not log that this event had even occurred.

TYPE UP MORE COMPARISONS

“ Still, an even somewhat paranoid but unskilled insider can use a cell phone or digital camera to photograph documents on the screen. No form ofDLPcan protect against that.” (http://www. networkcomputing. com/wireless/time-to-take-action-against-data-loss. php) Installing  a DLP tool is not the “ be all and end all” protection against threats and as emphasised earlier in this report a combination of measures needs to be addressed.

## Chapter 7:

Conclusion and Future Work. Highlight any deficiencies etc — Ethical?? Traking employees? ANY IMPROVEMENTS FOR DG . Many different aspects to consider

Link intro with conclusion.

Verizon – other factors p3 .

“ The best security technology in the world won’t produce a good return on investment without the foundation of security processes, policies, and education.” P8 Cisco data leakage.

“ if you have never experienced a security incident, does this mean that you are secure? Or does it just mean that, so far, you have been lucky?” computer insecurity book “ in short no one is immune” computer insecurity book

More..

Glossary

Bibliography

Online Sources

ICO. (2010), Press Release: Data Breaches to Incur up to £500, 000 penalty, [Online]. Available at

[Accessed 31st January 2010].

(2009), Unacceptable Level of Data Loss, [Online]. Available at

[Accessed 1st February 2010].

FSA. (2007), Final Notice to Nationwide Building Society, [Online]. Available at [Accessed 26th January 2010]

(2009), Previous Cases of Missing Data [Online]. Available at [Accessed 12th January 2010]

Broom, A. (2008), When financial data goes missing.[Online]. Available at [Accessed 3rd February 2010]

ICO. (date unknown), The Basics . [Online] Available at [Accessed 2nd February 2010]

## Journals

GAO. (2007), What GAO Found, Report to Congressional Requesters

Verizon Business (2009), Data Breach investigations Report

Ponemon Institute. (2009), As Employees Exit so does Corporate Data, Data Loss Risks During Downsizing

Ponemon Institute. (2006), 2006 Annual Study: Cost of a Data Breach

CFO Research Services, Crowe Chizek and Company LLC. (2008), The Changing Landscape of Risk Management

## Appendices