Information Leakage & Data Loss Prevention

Professor Malik Datardina

Prepared by
Karen Leung

July 5, 2009
**Table of Contents**

Introduction ................................................................................................................................ 3
Definition of Information Leakage ............................................................................................... 3
Origination of Information Leakage ............................................................................................ 3

*Behavioral Risks of Employees* .............................................................................................. 4
Impact of Data Leakage ............................................................................................................. 6
Need of Controls and Policies to Prevent Information Leakage .................................................. 7

*Specific Areas of Concern* ....................................................................................................... 9
Data Loss Prevention Tools .......................................................................................................10
Implications for the CA Profession ............................................................................................12
Conclusion ................................................................................................................................ 12
Works Cited ..............................................................................................................................13
Appendix A - Additional Resources Used ..................................................................................16
Introduction

Information within a company increases significantly each year. This could be to a point where it becomes unmanageable, resulting in data leakages. Although many companies may have implemented some form of security policy or technological barrier (e.g. firewall), many times this is insufficient as data still finds a way out of the organization, as such this is a hot topic management and auditors should be aware of. This report will first identify what information leakages are; how it can occur; the impact it has on the organization; the need of controls and policies; and tools that can help organizations with data leakage.

Definition of Information Leakage

Information leakage (also known as data leakage) is when sensitive data are revealed intentionally or not intentionally to unauthorized parties (CWE-200: Information Leak (Information Disclosure), 2008). The information leaked out can either be private in nature and are deemed confidential, such as credit card numbers or information that could be used by attackers to further exploit the system (Information Leakage, 2005).

Origination of Information Leakage

Information leakage can occur in the common ways corporations envision. Many organizations may invest heavily into firewalls, anti-virus software, encryptions and intrusion detection systems in order to protect lost of data to unauthorized parties such as external hackers (Mallery, 2009). Data leakages can also occur through comments left by a developer in the system script codes or HTML for future debugging or integration, providing unauthorized parties a view of how scripts work or even passwords and usernames used during the development phase (Information Leakage, 2005). Other times, organizations may collaborate with other organizations and information is shared between each other. A risk is posed through this as reliance in the other parties’ system is required (Alawneh & Abbadi, 2008). However, the least expected form of data leakage can occur through insider parties of the organization. It appears data leak occur the most from insiders of the organization. This is supported as one study found that 87% of confidential information leaked out is from insiders (Baek, Kim, & Lee, 2008). Therefore, this is important for both management and auditors to take note of.

Many times employees may use simple portable devices (e.g. USBs, flash drives). These devices may look harmless as they become part of the normal work life and go unnoticed if employees use them to carry corporate data in and out of the organization. The main issue here is the ability to carry and store large amounts of files and data in these devices and import it to another computer easily (Mallery, 2009). These devices also do not require technical
expertise from the user when compared to hackers who need IT knowledge, and almost every computer used today contains a USB port (Mallery, 2009). Although many businesses may recognize the threat posed by USB flash drives, a lot of the times portable “lifestyle” devices (iPods, MP3 players and digital cameras) are ignored (Mallery, 2009).

With the virtual network expanding and the increase in opportunities for employees to work outside of the office, having access to data anywhere provides convenience. As such, sites that provide online data storage (e.g. GMail Drive) are becoming extremely popular, allowing users to upload and store files on an Internet accessible server and accessing it anywhere else (Mallery, 2009). Through this, a risk of data leakage exists, as employees can virtually carry corporate data outside without being noticed. Other virtual methods that exist appear in the forms of personal cell phones, instant messengers, e-mails and blogs (Mallery, 2009). Employees may intentionally use these methods to transmit private information or use them as ways to vent their feelings as part of their normal lifestyles (e.g. diary of the work day through a blog). As these forms of communication are usually not monitored by the organization or logs kept for the information transmitted through these methods, confidential information (e.g. trade secrets) can easily be leaked out (Mallery, 2009).

The use of e-mails to transmit data can be one of the worst leaks as found by a pharmaceutical firm during a data leak audit. Employees may send unencrypted confidential zip files, e-mails marked as confidential (which raises flags) or even unfinished research documents that are not encrypted (Gittlen, 2009). Through this, the firm is exposed to legal, regulatory and business partner risks if data leak occurs. (Gittlen, 2009).

Besides data leak through technological solutions, are other ways leakage can occur. These exist in the form of confidential data left on the white board of the conference room (e.g. business plans or expansion diagrams) where anyone can walk by and take pictures of them or jot them down (Mallery, 2009). Another leak may be through media interviews, unskilled employees can easily leak confidential information (e.g. mergers and acquisitions, new product launch, etc.) without knowing as interviewers are skilled in asking about a topic in different angles (Mallery, 2009).

Behavioral Risks of Employees

As mentioned above, many times privacy leaks occur directly within the organization. Studies have been performed to determine where employee behaviors can result in data leak risks to the organization. As such, management of corporations should be aware of potential behavioral risks from their employees in order to determine where data leaks can result. Through this understanding, effective policies and procedures can then be created to minimize
potential data leaks.

A study performed by Cisco surveyed 1000 employees and another 1000 IT professionals from all over the world, and found 10 most noteworthy behavioral actions employees may engage in which leads to an increase of risks in data leakage. These include: (1) altering security settings on computers to access unauthorized Websites, (2) installation and usage of unauthorized applications, (3) unauthorized access to network or facility of the organization, (4) corporate information shared to non-employees of the organizations, (5) corporate devices shared with non-employees of the organizations, (6) personal and work devices used interchangeably, (7) devices are unprotected (e.g. unattended laptops left unlocked or logged on), (8) passwords and logins stored (e.g. stored in unlocked cabinets, written and left on desks, (9) portable storage devices lost with corporate data and (10) unsupervised roaming or “tailgating” of non-employees brought into the office (Duffy, 2008).

Cisco also found that 63% of the employees use corporate computers for personal use at least once a day (Data Leakage Worldwide: Common Mistakes Employees Make, 2008). Furthermore, 39% of the surveyed IT professionals also indicate that they have dealt with unauthorized employees accessing the company’s network or facility (Data Leakage Worldwide: Common Mistakes Employees Make, 2008).

With businesses becoming more distributed, often times employees working between the office and home may transfer data using unprotected personal communications to home computers or fail to use privacy screens on laptops while working outside the office. These actions lead to risks of data leakages. Cisco found that almost 46% of the employees transfer data between home and the office, while more than 75% do not use privacy screens (Data Leakage Worldwide: Common Mistakes Employees Make, 2008).

With employees’ ability to carry portable devices (e.g. laptops, etc.) outside of the office, another red flag that should be noted is getting employees to safeguard their devices. According to another study Cisco conducted, 9% of the employees have reported a loss of the devices or having them stolen (Data Leakage Worldwide White Paper: The High Cost of Insider Threats, 2008). The impact of these statistics is more astounding as one incident that occurred in 2006 highlights the importance of this issue. A veteran affairs analyst from the VA Department in the U.S. had taken a laptop home from work without clearance (Press, 2009). This laptop had over 26 million data of active troops and veterans’ names, date of births, and social security numbers (Press, 2009). Unfortunately, this laptop and its external hard drive was stolen when the employee’s home was robbed, resulting in identify thefts (Press, 2009). At the end, the VA Department had to pay $20M as a settlement to the veterans who suffered harm. (Press, 2009).
Through these surveys, Cisco also went about determining why employees engaged in such risky behaviors. It appears that employees tend to justify themselves, with reasons such as I need to “bounce ideas off of other people” or “I didn’t see anything wrong with it” in terms of sharing sensitive corporate information (Data Leakage Worldwide: Common Mistakes Employees Make, 2008). In terms of altering security settings, 52% of the employees wanted to visit the website regardless of corporate policy and 35% believed it was none of their company’s business as this is their privacy (Data Leakage Worldwide: Common Mistakes Employees Make, 2008). Through these explanations, it reveals that a lot of times employees are ignorant. They lack awareness of the resultant damage that their organization can experience. Cisco found that 43% of the IT professionals surveyed say employees are not educated enough about security (Data Leakage Worldwide White Paper: The High Cost of Insider Threats, 2008).

Other reasons employees engage in risky behaviors is because they are unhappy with their job (or other vindictive reasons) and deliberately want to do damage and leak data (Data Leakage Worldwide: Common Mistakes Employees Make, 2008). Companies should also consider ex-employees. For example, in the Pennwell Publishing case, an employee took his list of contacts from the Penwell’s Outlook system and left to set up his own business, although the case was ultimately resolved, this also puts the company at risk of loss income (Desai, 2008).

Impact of Data Leakage

The impact of data leakage to an organization can become severe and costly, therefore this issue is extremely relevant for management to consider. Although at first, organizations may not notice any immediate effects, the “small bits and bytes leaving the organization day by day” can result in considerable business costs that are difficult to quantify (Zinkewicz, 2009).

According to a research conducted by US security think tank, Ponemon Institute, through interviewing 56 US companies, the average leak per company was valued at more than AU$6 million (Average Cost of Data Leak $6 Million, 2006). Not only is this an impact on a company’s bottom line, a corporation’s brand value can also be eroded (as customer and shareholders lose faith in the corporation’s controls), taking years to recover (Average Cost of Data Leak $6 Million, 2006).

With companies holding increasing amounts of privacy data now, such as social insurance numbers of employees or credit card information of customers, the leakage of data can allow unauthorized parties to use it for criminal activities like identity theft. As such, in the US, legislations have been enacted. For more than 40 states, companies are now required to notify customers if their information was compromised (Zinkewicz, 2009). For states not required by law, the failure to notify can still result in extreme legal, civil and regulatory costs
(Zinkewicz, 2009). Therefore, the discovery and notification costs can amount to an estimate of $50 per record (or higher), which adds on to the lost customer satisfaction, legal and public relation costs (Zinkewicz, 2009). Furthermore, the corporation would likely be more closely monitored by regulatory bodies and may result in system and process audits for up to five years by another party (Meizlik, 2009).

Furthermore, data leakage can also wreck havoc for company plans and deals. According to a study performed by Cass, commissioned by an online workspace provider, Intralinks, looked at more than 350,000 transactions between 1994 and 2007 that were leaked ahead of time and found that more than 50% did not run to completion or on average, took longer to complete (MacFadyen, 2008). Thus, dealmakers will have to work harder to complete the deals as the leak (to the press) may have changed the context of the negotiations (MacFadyen, 2008).

**Need of Controls and Policies to Prevent Information Leakage**

To prevent information leakage and the high impact it can have on organizations, management should be aware of the existing policies and controls in place (e.g. firewalls, virus protection, etc.), and reviewing and updating them accordingly. As it is extremely important for management to set good effective policies, control weaknesses identified by auditors in relation to data flow should also be taken into consideration. Furthermore, management needs to know exactly what the important data is and manage it properly (Data Leakage Worldwide: Common Mistakes Employees Make, 2008). This can be accomplished by knowing exactly how users interact with the data daily through tools and processes to track data flow (Data Leakage Worldwide: Common Mistakes Employees Make, 2008). Once the data has been identified, management should determine which type of data needs a unique protection within and outside the corporation (Data Leakage Worldwide: Common Mistakes Employees Make, 2008). Organizations should always be on the lookout for new security approaches as tools and capabilities are constantly changing (Data Leakage Worldwide: Common Mistakes Employees Make, 2008).

Besides setting effective policies, it is also important that they actually work. Ways that management can ensure this is by increasing the awareness in employees, communicating them effectively, simplifying enforcement, integrating the need of security with its corporate culture, providing clear leadership and using a good creation process for setting policies (Data Leakage Worldwide: The Effectiveness of Security Policy, 2008). Management should basically guard corporate data as the most important possession, teaching employees that the lost of data is the lost of money to the corporation (Data Leakage Worldwide: Common Mistakes
Employees Make, 2008). Through the communication and awareness of policies, employees (both existing and newly hired) should also understand basic security procedures. Management should ensure these policies communicated addresses: the use of authorized application and access methods, the importance of maintenance using security software like antivirus applications, respect of security settings and awareness of phishing, spamming, malware, etc (Data Leakage Worldwide: Common Mistakes Employees Make, 2008). Furthermore, if employees are allowed to use portable devices (e.g. laptops, USBs, etc.), they should understand that these devices need to be kept with them or locked up at all times and that the usage is not shared with others or for personal activities (Data Leakage Worldwide: Common Mistakes Employees Make, 2008). Information should also not be transferred to personal devices or unauthorized online storage and neither should employees be accessing unauthorized and inappropriate sites for uploads or downloads (Data Leakage Worldwide: Common Mistakes Employees Make, 2008). Systems should always be logged off or locked if employees walk away or leave for the night and passwords created with sound techniques, stored securely and not shared with others (Data Leakage Worldwide: Common Mistakes Employees Make, 2008). When employees work in the public, they should speak softly, use privacy screens or VPN and a business printer only if they are there to retrieve the document (Data Leakage Worldwide: Common Mistakes Employees Make, 2008). Through all this, employees should also be knowledgeable on being aware of suspicious activities and knowing who to report to if a security incident occurs (Data Leakage Worldwide: Common Mistakes Employees Make, 2008). Everyone should be aware of physical access security to company buildings and not allow unauthorized people into the building or left to their own devices without supervision (Data Leakage Worldwide: Common Mistakes Employees Make, 2008).

As mentioned previously, management should simplify enforcement of policies, this means not creating a long list but keeping it to a manageable amount (Data Leakage Worldwide: The Effectiveness of Security Policy, 2008). The language used in the policies should be easy to understand, and the policies should be easy to comply with (Data Leakage Worldwide: The Effectiveness of Security Policy, 2008). Furthermore, it is important to have policies integrated into the business processes to avoid employees bypassing them and should ensure policies work with the employee’s job requirements (to avoid the need of employees to look bypasses to do a better job) (Data Leakage Worldwide: The Effectiveness of Security Policy, 2008). To effectively integrate the need for security into the corporate culture, management can consider tying the policies to the code of conduct; working with legal, HR or other compliance teams to communicate and train employees for security compliance; or
creating a security team to help employees in establishing good relationships (Data Leakage Worldwide: The Effectiveness of Security Policy, 2008). Management should also be setting the tone in security compliance for other employees and advocate the importance of security. Lastly, the creation process should have an understanding on when a policy should change, have consistent definitions and have continuous monitoring for compliance, etc (Data Leakage Worldwide: The Effectiveness of Security Policy, 2008).

Specific Areas of Concern

Companies should always consider obtaining restrictive covenants and ensuring confidentiality obligations are written into the employee contracts. To help prevent leakages, they should be written to specifically prevent database misuse by an employee before and after employment (Desai, 2008). Furthermore, only certain relevant staff should be granted access to it. Organizations can consider testing whether leakages or unauthorized usage occur by occasionally penetrating the database with “false” information (Desai, 2008).

Another important consideration is encryption as it is one of the first principles to help prevent data leakages (Tankard, 2009). This is important as the information obtained by unauthorized persons, whether for espionage, fraud or theft, the data would be meaningless as they are encrypted (Tankard, 2009). Furthermore, in some places like the U.K., the Companies Act of 2006 cause limited companies to have legal obligations to encrypt, making this an important area management should be aware of (Tankard, 2009). In order to determine the required level of encryption, IT professionals and management should ask themselves several critical questions. The first question is, “who has access?” to the data, as it is pointless if everyone has the keys to the encryption, therefore, only authorized people should have access (Tankard, 2009). Moreover, the keys should not be passed on without documented and clear permission given (Tankard, 2009). The second question that should be asked is “when the data has been accessed?” (Tankard, 2009). A log should be kept of all who had accessed the encrypted material, since this would serve as reference in case data was leaked (Tankard, 2009). The third question asks whether “the data is secure in the first place?” (Tankard, 2009).

In order to build a secure foundation using encryption and other secondary controls to help foundations from being compromised, a flaw in the system cannot exist (Tankard, 2009). Lastly, management should be aware of complacency settling in. As technology is constantly improving, computer security should be monitored and updated. Thus, the encryption systems implemented should be dynamic and proactive, especially when hackers who want to get through the system are constantly improving their techniques (Tankard, 2009).

In terms of portable devices, organizations can reduce this risk by setting up policies for
USB port usage based on the type of users (Rolls, 2008). This way, normal business operation would not be hampered by a strict “no-use” policy as many organizations may have workers that require the use of portable devices (Rolls, 2008). An example would be setting policies as “read only” access for some users and completely denying or allowing access for others (Rolls, 2008). To accomplish this, IT administrators can use third-party software that has the ability to lock all avenues data can be leaked and being able to control when certain types of files can be access (Rolls, 2008). One important ability that IT administrators should have is the ability to track and obtain reports of data breaches in terms of the person involved, when, where and what they did (Rolls, 2008). This can help management understand the extent of the breach, where the weaknesses are and how it can be improved.

Earlier, leakages through e-mails were also mentioned as one of the worst issues that can occur. To help combat this, companies should set up e-mail policies that identify information that belongs to the employee and those that belong to the company, and thereby prohibiting removal of employer information (Desai, 2008). Furthermore, for future reference and evidence, deleted e-mails should be easily retrieved (Desai, 2008). Monitoring can also be used; however, many organizations may be concerned with privacy issues and the illusion of employee distrust in the culture. Management can combat this by developing a clear understanding in the organization for the need to monitor and properly identify what sensitive data is (Fleming, 2007). If employees are notified of monitoring and feel that they are working with the monitoring process instead of against it (similar to a person monitoring their own home security), they may become more acceptable towards management monitoring. Also, management may consider obtaining consent in terms of monitoring usage (Desai, 2008).

Lastly, organizations should make sure devices are returned once the employees leave the organization.

Data Loss Prevention Tools

In order to respond to data loss leakages problems, besides policies and procedures management can implement, Data Loss Prevention (DLP) tools is an option management can consider helping track sensitive information and help enforce policies.

DLP tools are defined as “products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use, through deep content analysis” (Mogull, 2009). It should be noted that DLP tools most likely cannot stop “highly motivated threat agents” from within the organization, however, it can help “deter accidents, promote awareness and enforce information security and privacy policies by prompting the insider to exercise good information security and privacy practices” (Murphy, 2008). There are three main components that a DLP
tool works in order to protect data. The first being the “data-at-rest” component, which actively “crawls” the servers, end-points and databases in order to find sensitive information and providing a snapshot of the different types of info in the network (Murphy, 2008). The sensitive information profile and discovery rules are set by management, and once sensitive data are identified, a tag can be placed on it for further monitoring (Murphy, 2008). The second component is called “data-in-motion”, which is the actual monitoring and filtering of the network (Murphy, 2008). This component watches for any “tagged” sensitive information in the network traffic and enforces a policy if violation has occurred (Murphy, 2008). The last component is called “data-in-use” which focuses on the endpoints, specifically workstations, laptops and end user activities (e.g. save to USB, print, save/save as, burn to CD/DVD) (Murphy, 2008). Policies are enforced at the end point if triggered, resulting in “prohibiting copy/paste, delete, e-mail, burning to CD, moving files onto USB stick, and printing” (Murphy, 2008).

DLP tools can help management address the issues identified earlier in this report, and can allow the organization stay in compliance with legislations such as HIPAA, PIPEDA, etc. Furthermore, DLP works in conjunction with the advice of raising security awareness and relevant policies in the corporation and culture as DLP provides real-time response and on the spot correction (Tan, 2009). It should be noted however, that management should not confuse DLP features with DLP solutions. DLP solutions is what mentioned so far, whereas DLP features includes “some of the detection and enforcement capabilities of DLP products, but are not dedicated to the task of protecting content and data”, thus DLP features is more suitable for smaller organizations (Mogull, 2009).

Some management may be concerned with the cost of implementing a DLP, as it can become costly, however, management should compare this with the considerable costs that can result if a breach occurs (Wilson, 2008)

If organizations are interested in DLP solutions, there are several steps management should consider before jumping ahead to choices of vendors. In order to prepare the organizations, needs should be defined. This include: identifying business units (i.e. content owners and content protectors) that will be involved and creating a selection committee; define what specific data the organization wants to protect; how the data should be protected along with the set expectations; and lastly outline the process workflow (Mogull, 2009). Next, the team needs to translate the needs into formal requirements (i.e. specific criteria and technical features), evaluate the different products against their requirements and then perform internal testing to find any last problems from your DLP selection (Murphy, 2008).

There are many vendors in the market that organizations can choose from. Some of the
ones notable are Websense (which offer DLP tools combined with encryption and endpoint security technologies), Reconnex (which offers automated discovery and forensic features), Verdasys (offers software agents to protect data at endpoint), RSA (a division of EMC was the first vendor to enter the market) and Vericept (has a balanced coverage and strong analytical features) which scored well under a report conducted on DLP vendors by Forrester Research Inc. between December 2007 to February 2008 (Westervelt, 2008). Other well known vendors that did not participate in the research are Symantec (the second vendor to enter the DLP market) and McAfee (Westervelt, 2008).

Although DLP tools are excellent, problems for management may arise as they may not necessary know “where their unstructured data is, let alone where their sensitive data is” (Garretson, 2008). Therefore, management will have to “start out with a limited scope to create IT processes that will solve business problems” (Garretson, 2008). Both the business management leaders and technology leaders in the organizations must work together to identify and classify the information and successfully implement the DLP solution. Furthermore, management needs to be aware of what current technologies (e.g. current encryption tools or digital rights management) and policies it has in the organization as these needs to be pinpointed and integrated with the DLP during implementation (Wilson, 2008). Management should also be aware that it can take years for DLP to be fully implemented; therefore results may not be immediate (Wilson, 2008).

**Implications for the CA Profession**

From the overview given in this report regarding data leakages, CAs as auditors or business advisors should be aware of potential weaknesses in the organizations in terms of data leakages. The impact of data leaks should be highlighted and recommendations for improvement in policies and controls or even the use of DLP tools should be given if possible. This will add client value if CAs can point clients toward the right direction in mitigating risks which can damage the organization significantly.

**Conclusion**

Data leakages can be detrimental to an organization if proper procedures, policies and controls are not taken. Management needs to understand what data leaks are, the effect it has, and take proper measures as outlined in this report. Good tools to help monitor and prevent against data leaks are DLP solutions, however careful analysis and preparation is required first.
Works Cited


**Average Cost of Data Leak $6 Million.** (2006). Retrieved May 23, 2009, from iTWire:
http://www.itwire.com/content/view/6718/545/


Appendix A - Additional Resources Used


## ANNOTATED BIBLIOGRAPHY

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zinkewicz, Phil</td>
<td>Dealing with Data Leakage</td>
<td>Rough Notes</td>
<td>Vol. 152, Iss. 4</td>
<td>2009</td>
<td>82-83</td>
<td>May 17, 2009</td>
<td>ABI/INFORM Global database</td>
</tr>
</tbody>
</table>

**Website Link:**

**Annotation**
This article describes the impact of data leakage to an organization, indicating data leakage may seem insignificant at first; however, the “small bits and bytes leaving the organization day by day” can cause considerable business costs that are difficult to quantify. It also indicates that many states in the U.S. have legislation that demands organization to notify individuals if their identity has been breached, however, even if this was not so, severe legal liabilities, reputational damage and loss of consumer trust may result. Organization can mitigate monetary loss through insurance and implement DLP, but the idea that data leakage is an everyday occurrence and more than just an IT problem must be put across management minds. As organization’s data doubles every 2 to 3 years, the way companies handle the information and safeguarding it is extremely important. A DLP tool that companies can use is Fidelis’ Security System XPS.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Murphy, Joanna</td>
<td>Data Loss For Prevention: An Elixir For Privacy Compliance Headache?</td>
<td>EDPACS</td>
<td>38(6)</td>
<td>2008</td>
<td>10-17</td>
<td>May 17, 2009</td>
<td>ABI/INFORM Global database</td>
</tr>
</tbody>
</table>

**Website:**

**Annotation**
This article looks into what DLP tools are and why it is becoming a hot demand in technology. The DLP solution is described as “a combination of hardware and software that aims at the loss or leakage of data assets out of the organization”. Three main components of a DLP tool are described as: Data-at-Rest (“a discovery activity that crawls your server…looking for sensitive data”), Data-in-Motion (“a network content monitoring and filtering tool”) and Data-in-Use (“a component concerned with end-point – laptops, workstations”). The article also describes how DLP address the privacy issues under Principle 5 (Limiting Use and Disclosure), Principle 7 (Safeguards), Principle 8 (Openness) and Principle 9 (Individual's Access to Personal Information) and critical success factors that look into specific security management controls.
Fratto, Mike

What You Know Can Hurt You

InformationWeek

1205

2008

24

May 17, 2009

ABI/INFORM Global database, Website Link:


Annotation

This brief article describes a survey conducted on data leakage. It appears that 52% employees bypass company policy to access unauthorized websites. Furthermore, IT users may give others the use of their computers without IT personnel knowing, and data leakages can occur while employees work outside the office (e.g. on plane flights).

Duffy, Jim

Collaboration causes net problems.

Network World

25(39)

2008

24

May 17, 2009

ABI/INFORM Global database, Website Link:


Annotation

In this article, it describes behavioural risks employees present that can cause data leakage. As businesses provide employees the mobility and the ability to become more collaborative, corporations are more vulnerable to information loss if there is a lack in “modern security technology, awareness and education”. The top 10 behaviour risks found through studies are: employees altering security settings on computers; the use of unauthorized applications; unauthorized network/facility access; sharing of sensitive corporate information; sharing corporate devices; blurring of work and personal devices; unprotected devices; storing logins and passwords; losing portable storage devices; allowing tailgating and unsupervised roaming.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zalud, Bill</td>
<td>Protecting the Most Important Network</td>
<td>Security</td>
<td>45(10)</td>
<td>2008</td>
<td>74</td>
<td>May 17, 2009</td>
<td>ABI/INFORM Global database,</td>
</tr>
<tr>
<td></td>
<td>Website Link:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="http://proquest.umi.com.proxy.lib.uwaterloo.ca/pqdweb?did=1590057671&amp;Fmt=3&amp;clientId=16746&amp;RQT=309&amp;VName=PQD">http://proquest.umi.com.proxy.lib.uwaterloo.ca/pqdweb?did=1590057671&amp;Fmt=3&amp;clientId=16746&amp;RQT=309&amp;VName=PQD</a></td>
</tr>
<tr>
<td>Annotation</td>
<td>In this article, it describes measures and IT controls the City of London Police places in order to secure data and information from leakage. In order to protect their network, they've developed a model IT governance policy to protect information internally and information coming in externally. They also identified and secured all potential points for data leakage, “as well as safeguards against unauthorized electronic transmission of data”. In order to secure transportation of data with USBs, biometric authentication has been used along with another device called Stealth MXP.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Garretson, Cara</td>
<td>Data-leak prevention: Pros and cons</td>
<td>Network World</td>
<td>25(1)</td>
<td>2008</td>
<td>39</td>
<td>May 17, 2009</td>
<td>ABI/INFORM Global database,</td>
</tr>
<tr>
<td></td>
<td>Website Link:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="http://proquest.umi.com.proxy.lib.uwaterloo.ca/pqdweb?did=1415888251&amp;sid=7&amp;Fmt=3&amp;clientId=16746&amp;RQT=309&amp;VName=PQD">http://proquest.umi.com.proxy.lib.uwaterloo.ca/pqdweb?did=1415888251&amp;sid=7&amp;Fmt=3&amp;clientId=16746&amp;RQT=309&amp;VName=PQD</a></td>
</tr>
<tr>
<td>Annotation</td>
<td>This article provides positive and negative aspects of DLP tools. It claims that DLP tools are “helpful with some tasks but far from the solution”. The pro about DLP tools is the ability in allowing entities to monitor the flow of information, yet the con is that “enterprises don’t know where their unstructured data is, let alone where their sensitive data are” which are required by DLP. Therefore, the article suggests that besides DLP tools, ultimately, enterprises need to work “between technology and business leaders” in order to achieve the management of information life cycle.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Author</td>
<td>Title of Article</td>
<td>Periodical/ website</td>
<td>Vol. / No. / Edition</td>
<td>Year published</td>
<td>Pages</td>
<td>Date accessed</td>
<td>Location, database, website, link</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>----------------------</td>
<td>----------------</td>
<td>-------</td>
<td>--------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Schutzer, Dan</td>
<td>Data leakage will continue to plague financial institutions in the coming year</td>
<td>Bank Systems &amp; Technology</td>
<td>44(12)</td>
<td>2007</td>
<td>35</td>
<td>May 17, 2009</td>
<td>ABI/INFORM Global database,</td>
</tr>
<tr>
<td></td>
<td>Annotation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This article describes the factors as to why financial institutions are continually experiencing data leakage problems. The three main factors that contribute to this are: consolidation and globalization, rise of the extended enterprise, increased value of information. Data retention is also a problem as the amount of information being accumulated is explosive. Financial institutions are still “working to establish electronic document/records management policies, procedures and technologies”, however, “processes largely are not automated and not connected end-to-end across businesses&quot;.</td>
</tr>
<tr>
<td>Author</td>
<td>Title of Article</td>
<td>Periodical/ website</td>
<td>Vol. / No. / Edition</td>
<td>Year published</td>
<td>Pages</td>
<td>Date accessed</td>
<td>Location, database, website, link</td>
</tr>
<tr>
<td>Anonymous</td>
<td>Research and Markets Offers Report: World Data Leakage Prevention Market</td>
<td>Wireless News</td>
<td>n/a</td>
<td>2008</td>
<td>n/a</td>
<td>May 17, 2009</td>
<td>ABI/INFORM Global database,</td>
</tr>
<tr>
<td></td>
<td>Website Link: <a href="http://proquest.umi.com.proxy.lib.uwaterloo.ca/pqdweb?did=1565517391&amp;sid=9&amp;Fmt=3&amp;clientId=16746&amp;RQT=309&amp;VName=PQD">http://proquest.umi.com.proxy.lib.uwaterloo.ca/pqdweb?did=1565517391&amp;sid=9&amp;Fmt=3&amp;clientId=16746&amp;RQT=309&amp;VName=PQD</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Annotation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This article gives a brief overview into the DLP and ILP market and why these markets are becoming increasingly important. Major contributors to data leakages are “e-mail, mobile technology, and thumbdrives”, companies need to understand the types of data in their network and ensure their entity complies with internal and external policies. This way, entities can lower the risk of reputation loss and costly penalties from data leakages.</td>
</tr>
<tr>
<td>Author</td>
<td>Title of Article</td>
<td>Periodical/ website</td>
<td>Vol. / No. / Edition</td>
<td>Year published</td>
<td>Pages</td>
<td>Date accessed</td>
<td>Location, database, website, link</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------</td>
<td>---------------------</td>
<td>----------------------</td>
<td>----------------</td>
<td>-------</td>
<td>-----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Tankard, Colin</td>
<td>Is your customer data encrypted?</td>
<td>MicroScope</td>
<td>b/a</td>
<td>2009</td>
<td>19</td>
<td>May 17, 2009</td>
<td>ABI/INFORM Global database,</td>
</tr>
<tr>
<td>Mallery, John</td>
<td>Overlooked Data Leaks</td>
<td>Security Technology Executive</td>
<td>19(3)</td>
<td>2009</td>
<td>78-80, 82</td>
<td>May 17, 2009</td>
<td>ABI/INFORM Global database,</td>
</tr>
</tbody>
</table>

**Website Link:**

**Annotation**
This article describes the need for encryption in case data leakages occur. As data falling into the wrong hands can be detrimental, effective encryption is required as risks are rising. Four critical questions should be looked at when determining the encryption level, they are: Who has access?, When has the data been accessed?, Is data secured in the first place?, When does complacency set in?"

This article talks about how information leakage cannot be 100% protected. Although most companies invest in technological mechanisms to protect their data (e.g. firewalls, encryptions, etc.), information leakage can still occur elsewhere. These places are namely: flash drives, portable media, online data storage, IMs, E-mail, blogs and through non-technological examples (e.g. media interviews, whiteboards, trade shows, and corporate espionage.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Annotation**

This article describes how information leakage occurs and how corporations can prevent internal breaches. It indicates that a rigid “no-use policy” for USB drives can affect business activities, therefore, policies can be set through third party software that allows “read-only” access on devices for certain users and deny access for others. These policies should be flexible yet strong, and any data breaches should be reported and documented for audit trails. Softwares that “can lock all avenues of data leakages and use permissions and policies to control who has access to the files, where and when” are ideal.

Information leakage is a threat in which “a web site reveals sensitive data” that “may aid an attacker in exploiting the system”. Although it may not be a breach in security, an attacker can obtain guidance for future usage. The three main categories consist of: “Comments left in code, verbose error messages and confidential data in plain sight”. It may also occur through insufficient protection for data that are confidential or attacks that are not within the scope of the website protection.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
</table>

**Website Link:**
http://proquest.umi.com.proxy.lib.uwaterloo.ca/pqdweb?did=1484085461&sid=7&Fmt=2&clientId=16746&RQT=309&VName=PQD

**Annotation**
This paper attempts to calculate the confidentiality of a system by quantifying the amount of information leakage. It measures leakage by “a notion of approximate process equivalence” to an adversary. There are three classes of adversaries looked at and each have different expressive power. However to estimate the maximum leakage is impractical and to find the most powerful adversary is hyper-exponential.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messmer, Ellen</td>
<td>Data leaks are a people problem.</td>
<td>Network World</td>
<td>25(36)</td>
<td>2008</td>
<td>22, 40</td>
<td>May 23, 2009</td>
<td>ABI/INFORM Global database,</td>
</tr>
</tbody>
</table>

**Website Link:**

**Annotation**
This article indicates that DLP tools are excellent for monitoring “unauthorized transmission of sensitive content” and is “a powerful technology sometimes put to surprising use”. However, without a strong policy in place, DLP tools would not work as enforcement will become difficult if violations occur. With a policy that management accepts, it sets the factors as to what constitutes a violation and how enforcement should be taken. But overall, DLP products allow the entity to “determine where the data is and who’s using it”.

23
This article describes how results from a study indicate that “information leaks to the press have a significant impact on both the terms and success rate of deals”. Dealmakers will have to work harder as competition will become aware of the project. It is also found that more than half of the deals do not arrive to completion after the leak.

This article mentions that the most dangerous threat of information stolen can be by ex-employees. Employees can use the database without authorization and obtain client information for their own purposes (e.g. set up competition). This can not only occur with USBs, but through messages sent. Companies need to set up e-mail policies with restrictive covenants and proper access controls to protect themselves. As organizations can spend a lot of resources on their database, they should investigate whether “they do in fact own the intellectual property rights…how they deal with them, and how they might protect them from unauthorised use”.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gittlen, Sandra</td>
<td>Inside a Data Leak Audit</td>
<td>Network World</td>
<td>26(18)</td>
<td>2009</td>
<td>30, 32, 34</td>
<td>May 23, 2009</td>
<td>ABI/INFORM Global database</td>
</tr>
</tbody>
</table>

**Website Link:**

**Annotation**
In this article, it discusses how a pharmaceutical firm with annual audits and other IT security in place, still found many loop holes in their system, placing them at legal, regulatory, and business partner risks. Some of the worst leaks uncovered in the company were: 1) An unencrypted confidential zip file sent through email, 2) email attachments marked as confidential sent 3) Unencrypted unfinished research document sent. The auditors suggested a two-pronged approach to revisit the “business processes and technology fortification”, for example, have automated encryption, user/business partner education, rank information sensitivity, regular audits performed on the network and “do business with companies that know how to exchange information securely”.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>Average Cost of Data Leak $6 million</td>
<td>iTWire</td>
<td>n/a</td>
<td>2006</td>
<td>n/a</td>
<td>May 23, 2009</td>
<td>Google</td>
</tr>
</tbody>
</table>

**Website Link:** http://www.itwire.com/content/view/6718/545/

**Annotation**
This press release reported the estimated average dollar cost on a company from data leakage. The impact is estimated at AU$6 million, which are from costs of informing shareholders, staff, customers and the lost of brand value. These leaks can originate from both internal and external sources.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>Data Leakage Worldwide: Common Mistakes Employees Make</td>
<td>Cisco</td>
<td>n/a</td>
<td>2008</td>
<td>1-10</td>
<td>May 23, 2009</td>
<td>Google</td>
</tr>
</tbody>
</table>


**Annotation**

This is a report released by Cisco on a research study conducted “to understand the challenge that increasingly distributed and mobile businesses face in protecting sensitive information”. The study found that employees all over the world engage in risky behaviours which can be a threat to the company. It also explains why employees engage in these risky behaviours. These risky behaviours include: unauthorized application use, misuse of corporate computer, unauthorized physical and network access, remote worker security, and misuse of passwords. Therefore, businesses must evaluate risks and incorporate in their corporate culture the importance of security.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Giannoulis, Peter</td>
<td>Data loss prevention (DLP) tools: The new way to prevent identity theft</td>
<td>SearchSecurity.com</td>
<td>n/a</td>
<td>2008</td>
<td>n/a</td>
<td>May 23, 2008</td>
<td>Google</td>
</tr>
</tbody>
</table>

**Website Link:** [http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1301484,00.html](http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1301484,00.html)

**Annotation**

The article describes the key differentiating features of DLP technology that helps protect data for entities. The main features include: protect information from accidental disclosure, protecting information from malicious intent (internal and external) and meeting regulatory compliance requirements (SOX, GLBA, HIPAA). All personnel from every levels of management should meet in order to classify data correctly. In order to decide the best DLP technology, one of the qualities to look at is its ability to block and monitor by system and user.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tan, Suzie</td>
<td>Setting strategies for data loss prevention</td>
<td>Malaysian Business</td>
<td>6</td>
<td>2009</td>
<td>n/a</td>
<td>May 28, 2009</td>
<td>ProQuest Asian Business Reference database</td>
</tr>
</tbody>
</table>

**Website Link:**

**Annotation**
This article discusses why more businesses are using data loss prevention (DLP) in order to mitigate risks in computing. As DLP combines technology, people and processes, it can prevent loss in various points of the information cycle, and allow users to know the data loss policy and follow it. DLP has automated efforts that provide real-time response and on-the-spot correction, which gives insights on corporation’s data, creating effectiveness in managing and controlling information risk.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>McLaughlin, Kevin; Ohlhorst, Frank J.</td>
<td>Fixing Leaky Pipes – Data leak prevention is a hot topic, but jumping in will require new skills.</td>
<td>CRN</td>
<td>6</td>
<td>2007</td>
<td>26</td>
<td>May 28, 2009</td>
<td>ABI/Inform Global database</td>
</tr>
</tbody>
</table>

**Website Link:**

**Annotation**
This article discusses the impact of acquiring and implementing DLP amidst its growing acknowledgment. DLP certainly contains obstacles as they can be extremely pricey and requires policy changes that may affect entities’ business processes. It is not a simple box to turn on, but “a complete project management flow”. Therefore, new skill sets are required such as information management skills, managing and monitoring skills for key alerts identified by DLP.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fleming, Sam</td>
<td>Implicit Trust Can Lead to Data Loss</td>
<td><em>Information System Security</em></td>
<td>16(2)</td>
<td>2007</td>
<td>109-113</td>
<td>May 28, 2009</td>
<td>ABI/Inform Global Database</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Website Link:</td>
</tr>
<tr>
<td></td>
<td><strong>Annotation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This article analyzes the dilemma organizations face between monitoring employee activities for data security and the conflict with employee privacy and organization culture. It points out that in order for employees to accept, the entity should have a clear understanding of why a need for monitoring is required. The organization should first understand the risk, create effective policies, enforce the policy and monitor compliance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Website Link:</td>
</tr>
<tr>
<td></td>
<td><strong>Annotation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This article talks about the abilities DLP tools can flag that may concern and scare some companies. As DLP tools’ objective is to provide the organization the main picture and where sensitive data may leak out, some organizations may find it spotlighting certain internal practices that can result in violation of regulatory laws. Furthermore, DLP can allow monitoring of business partner’s treatment of shared sensitive data, thus, organizations must be willing to “put in your own castle walls with your business partners” first.</td>
</tr>
</tbody>
</table>
Hook, Brian  
Data leakage prevention: Reducing risk  
SC Magazine  
n/a  
2009  
n/a  
May 28, 2009  
SC Magazine  


Annotation  
This article focuses on how DLP tools can be effective and reduces the risk of data loss versus solving data security. As organizations look for ways to safeguard sensitive information, the market for DLP are driven upwards. In order for the DLP tool chosen to be effective however, four main factors should exist: its ability to identify sensitive data, policies is defined and managed, data movement are monitored and enforced, and all cases of data leakage are documented, reported and investigated. DLP helps prevent misuse and loss of sensitive data by tracking and enforcing secure access to information.

Author  
Title of Article  
Periodical/ website  
Vol. / No. / Edition  
Year published  
Pages  
Date accessed  
Location, data base, website, link

n/a  
Data Leakage Worldwide White Paper: The High Cost of Insider Threats  
Cisco  
n/a  
2008  
1-6  
May 29, 2009  
Google  


Annotation  
Although external threats are real and serious, this paper discusses the high cost of insider threats. Insider threats can be created through negligent employees who lack awareness and diligence, disgruntled employees or those who see financial gains through illicit actions. The insider threat is amplified if there is limited IT awareness of true employee actions. Therefore all levels of the organization should work together to protect sensitive data assets, and be willing to embrace different cultures, business practices while focusing on the accountability and education within its approach.
**Data Leakage Worldwide: The Effectiveness of Security Policy**

*Cisco*

2008

May 29, 2009

Google


**Annotation**

This paper provides reasons as to why security policies are ineffective within an organization through the findings within its survey. The main reasons are: a failure to communicate (policies to employees), email limitations on policy updates, lack of compliance and limited IT-faced policies. In order for organizations to create effective policies, it should: increase awareness, communicate policies effectively, simplify enforcement, integrate security with the corporate culture, provide clear leadership, and use a good security policy creation process.

**The Data Discovery Challenge**

*SC Magazine*

2008

May 29, 2009

SC Magazine


**Annotation**

In order to pin-point the critical data within the organization, this article suggests that traditional security solutions targeted at external threats are no longer the solution, data-focused technology is. To mitigate risk, understanding where the data is extremely critical. The best practices to discover (sensitive) data is for organizations to first discover sensitive data, assess data activity risk, and ensure data compliance(to regulation). Some tools to discover data are: Data Classification Tools, Data Leak Prevention Tools, and Fileshare crawlers.
Data Loss Prevention tools are used “to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders”. As organizations face risks of data leakages and breaches, the need arises for DLP. DLP solutions work by classifying “data in motion, at rest, and in use”, classify the data by control level, and monitors channels for content coming into the organization or leaving the organization.

This article describes a type of control an organization can use to protect data that is valuable from being compromised. Encryption is identified as the most important subcategory for email security; however the challenge is to get users to use it.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campagna, Rich</td>
<td>How New Access Control Technologies Can Address Insider Threats</td>
<td>SC Magazine</td>
<td>n/a</td>
<td>2009</td>
<td>n/a</td>
<td>May 29, 2009</td>
<td>SC Magazine</td>
</tr>
</tbody>
</table>


**Annotation**
This article addresses access controls which can be used against insider threats to information leaks and other misuse. Insider threats can misuse corporation’s information assets and access it through legitimate ways. The resulting loss to the company can be phenomenon. Many financial and personal information breaches are the result of dishonest, vengeful or careless insiders. In order to prevent breaches from occurring, access controls can be used. However, clear policies should be in place as network complexity has increased to assign roles and identifies for the controls. Then the existing network security products should be incorporated and efficiently managed by management.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wilson, Tim</td>
<td>What You Really Need To Know About Data Leak Prevention</td>
<td>DarkReading</td>
<td>n/a</td>
<td>2008</td>
<td>n/a</td>
<td>May 29, 2009</td>
<td>DarkReading</td>
</tr>
</tbody>
</table>

**Website Link:** [http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=211201210](http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=211201210)

**Annotation**
This article discusses the various aspects of why a corporation wants to use a DLP and the implementation process. As the risk sensitive data leaking out is becoming a concern for organization, DLP can offer a solution. Companies may justify the cost with the loss that may result in a serious data breach. In order to implement DLP, a company should first test through a few DLP products, locate where its sensitive data and risks are, define policies and then implement it. To fully implement DLP technology depends on the size of the project. It is also possible to integrate DLP with other technologies in place.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wright, Benjamin</td>
<td>The Cost of Not Securing Personally Identifiable Data</td>
<td>ISACA.org</td>
<td>4</td>
<td>2004</td>
<td>n/a</td>
<td>May 29, 2009</td>
<td>ISACA</td>
</tr>
</tbody>
</table>


**Annotation**

This article discusses the incentive to secure data in a corporation and the consequences of failing to do so. As a large amount of data break-ins occur and hackers find other ways to steal information, safeguarding personal information has become extremely important. The cost to inform people of data loss not only results in monetary costs, but reputation loss and bad publicity. Laws in California have been passed where notifications must be sent if personal data has been compromised and also where financial institutions cannot share personal data with others, these practices have already started to spread across borders.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baek, Eunju; Kim, Yeog; Sung, Jinwon, and Lee, Sangjin</td>
<td>The design of framework for detecting an insider's leak of confidential information</td>
<td>Proceedings of the 1st international Conference on Forensic Applications and Techniques in Telecommunications, information, and Multimedia and Workshop</td>
<td>n/a</td>
<td>2008</td>
<td>1-4</td>
<td>May 29, 2009</td>
<td>ACM Digital Library</td>
</tr>
</tbody>
</table>

**Website Link:**

**Annotation**
This paper provides a framework in order to identify and stop a leak of confidential information by leak type using forensic sight. These leak types can be categorized under removable storage media and communication media. As it is found that 87% of a leak of confidential information is from insiders due to negligent or weak control, the framework focuses on controlling leaks from the inside. The framework focuses on “observation, detection, extraction of evidence and store the evidence”. However, legal issues may exist in terms of privacy problems of employees.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Irwin, Keith; Yu, Ting; and Winsborough, William H.</td>
<td>Avoiding information leakage in security-policy-aware planning</td>
<td>Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society</td>
<td>n/a</td>
<td>2008</td>
<td>85-94</td>
<td>May 29, 2009</td>
<td>ACM Digital Library</td>
</tr>
</tbody>
</table>

**Website Link:**

**Annotation**
In this paper, the issue of how planning systems used by organizations for complex tasks can leak out sensitive information. One approach given by the paper is to prevent information leakage by separating a user from the things they are to perform with the actions that are to be kept secret. This is usually highly not feasible; therefore the second approach is to cancel and rescheduling "higher secrecy actions", although effective, negative impacts may result.
### Author: Borders, Kevin; Zhao, Xin; and Prakash, Atul

**Title of Article**: Securing sensitive content in a view-only file system

**Periodical/website**: Proceedings of the ACM Workshop on Digital Rights Management

**Vol. / No. / Edition**: n/a

**Year published**: 2006

**Pages**: 27-36

**Date accessed**: May 29, 2009

**Location, data base, website, link**: ACM Digital Library


**Annotation**

This paper discusses a new method that could be used to protect sensitive data from unauthorized exposure. This is through the use of a View-Only-File System (VOFS) where a higher level of security can be provided than current systems. Authorization is required before a user can access data, once this process is complete, VOFS “disables non-essential device output” until the user is finished viewing the sensitive data. This way, the user or any other software cannot steal, print, or upload sensitive data. The description of the implementation, design and evaluation plans of VOFS is also provided.

### Author: Lopresti, D. and Spitz, A. L

**Title of Article**: Quantifying Information Leakage in Document Redaction

**Periodical/website**: Proceedings of the 1st ACM Workshop on Hardcopy Document Processing

**Vol. / No. / Edition**: n/a

**Year published**: 2004

**Pages**: 63-69

**Date accessed**: May 29, 2009

**Location, data base, website, link**: ACM Digital Library


**Annotation**

This paper discusses how through the process of redaction, sensitive information may be leaked out. Adversary can use several techniques to extract information, these include image processing, font metrics, usage of artifacts, and natural language processing. A prototype semi-automated system is designed to provide feedback as to whether a document can suffer from this type of leak.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alawneh, Muntaha and Abbadi, Imad M.</td>
<td>Preventing information leakage between collaborating organisations</td>
<td>Proceedings of the 10th international Conference on Electronic Commerce</td>
<td>342</td>
<td>2008</td>
<td>1-10</td>
<td>May 29, 2009</td>
<td>ACM Digital Library</td>
</tr>
</tbody>
</table>

**Website Link:**

**Annotation**
Many organizations collaborate amongst each other, which increases the risk of data leakage as information is shared between organizations. The foundation would include two elements: 1) having mutual trust between the organizations 2) having a secure system. For a secure system, this paper provides a suggested system to protect the sensitive data, which include two stages: 1) Protect content in destination organization by using a global domain and a trusted software agent 2) Protect content that is restricted for access for a certain group of users/department via a dynamic domain.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meizlik, David</td>
<td>The True Cost of a Data Leak</td>
<td>Financial Services Technology</td>
<td>8</td>
<td>2009</td>
<td>n/a</td>
<td>May 29, 2009</td>
<td>Google</td>
</tr>
</tbody>
</table>

**Website Link:**

**Annotation**
This article discusses the cost that can result due to a data leak. The cost can be significantly greater than the amount organizations could have invested in prevention in the first place. Continuous costs can result from a data leak, therefore a prevention could be using DLP technologies which can “act as a cornerstone of a company’s information security strategy” to help mitigate the risks of data breaches. In the end, DLP can costs only half a percentage of the cost of a leak to an entity, which is extremely cost-effective.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>CWE-200: Information Leak (Information Disclosure)</td>
<td>Common Weakness Enumeration</td>
<td>n/a</td>
<td>2008</td>
<td>n/a</td>
<td>May 31, 2009</td>
<td>Google</td>
</tr>
</tbody>
</table>

**Website Link:** [http://cwe.mitre.org/data/definitions/200.html](http://cwe.mitre.org/data/definitions/200.html)

**Annotation**
Information leak is defined as a disclosure of information, whether intentional or not, to an unauthorized person by allowing them to have access to that information. This information can be sensitive due to its functionality or it can provide data about a product or environment which can be used by the unauthorized person in an attack, when they normally could not have done so.