Reducing Data Loss and Saving Money by Acquiring Data Loss Prevention Software

Master of Art in Information Technology

By
Patarika Tipwong, IT
Patarika_t@hotmail.com

Thesis Advisor
Jacob Furst
jfurst@cdm.depaul.edu

School of Computing and Digital Media

DePaul University, Chicago, Illinois

Fall Quarter 2011

Acknowledgements

This thesis could not have been written without Professor Jacob Furst who not only served as my thesis advisor but also encouraged and challenged me to complete my Master of Art in Information Technology course. I would like to thank him for providing comments and feedback and his contribution to my study at DePaul University.

Table of Contents

Abstract

Choosing and implementing the right security software tools can protect a company's assets. In particular, data breaches might not happen if a company is aware of its information flow and has the proper tool to protect it. This thesis paper will explain why and how acquiring data loss prevention (DLP) software will help a company to reduce data loss, mitigate the loss impact and save money. Facts and examples are provided to support and illustrate the statement above.

1. INTRODUCTION

Challenge
An organization is challenged with maintaining a reliable reputation and regulatory environment. Shareholders and customers trust in a company's ability to protect intellectual property and customer data. According to Symantec (2010), "Intellectual property is hard to find and even harder to protect". Top level management must assure that the company meets its goals and objectives. The ability to implement security software is needed in order to minimize risks, protect against data breaches, and prevent other events that affect financial health, public relations, and brand reputation.

Opportunity
There is an opportunity to raise awareness about how to protect a company's assets including sensitive data. By choosing appropriate security software and selecting a security tool like DLP software, a company can help prevent information security breaches of Personally Identifiable Information (PII), Intellectual Property (IP), and other valuable data.

Benefits
Using and implementing the right software with the right business can reduce data loss and save money. With the tools in DLP, a company can gain benefits such as:

- Increase shareholders' and customers' confidence by providing the ability to protect the intellectual property of the company.
- Retain effective and efficient tools to protect against data breaches.
- Easily identify and analyze problems.
- Prevent misuse of data.
- Gain protection of Personally Identifiable Information.
- Decrease the cost of loss of the company's asset.

1.1 Purpose

The purpose of this thesis is to emphasize how to reduce data loss and save money by acquiring DLP. The thesis will be divided into two parts.

The first part of this thesis begins with a review of breaches. This includes an explanation for each type of data breach like insider threats, corruption or deletion of data. The importance of prevention will be provided in this part. It will then lead to the topic of how to reduce loss and save money by acquiring DLP.

The second part of thesis starts with special tools in DLP such as network DLP, storage DLP, and end user DLP. Also it explains why DLP is different from other software. This is followed by data processes that the company can protect such as data in use, data in motion, and data at rest. It then turns the focus to the discussion of the benefit of DLP compared with other security software. Also, results and recommendations of the topic will be at the end of this thesis.

2. LITERATURE REVIEW

A student, an employee, a patient or a businessman's data could be in the hands of strangers. These strangers have an obligation to keep personal information. However, through weak security on computer networks, theft and loss of laptops, much of your information can be exposed through data breaches. Here are some facts about data breaches in the past.

2.1 Fact about data breaches

"Home Depot, the world's largest retailer of home improvement products, is on the list (see next page) for allowing 10,000 employee records to be compromised".

In 2007, in Massachusetts, one of Home Depot's employee's laptop was stolen in the car park at his residence. Stored in the stolen laptop were some of the private data related to companies, firms, students, government agencies, and hospital information. However, according to Boston Journal by Jonathan 2007, personal information was not the thief's target but it was employees' records stored in the machine. As a result, 10,000 records of employees were affected by this data breach. In addition, Home Depot did not reveal the city in which the data breach happened and it was not giving out its victim's information as well. From the customers' feedback after this data breach, most people were concerned about data security when employees carry or store data on external devices while they were traveling, bringing them home or leaving such devices in insecure places.

"Dai Nippon Printing – 8.6 million records of people targeted in a direct-mail campaign were stolen by a former employee".

On March 12, 2007, an ex-contractor of Dai Nippon Printing Company in Tokyo stole 8.6 million records of customers' personal information including names, addresses and credit card numbers in order to do direct marketing. According to Wakao (2007), "employee stole client data between May 2001 and March 2006 by copying information on to floppy disks and other recording media". The news revealed that at least 43 customers' details were disclosed; (there may have been many more that did not have enough evidence for proof of disclosure). In fact, it was devastating to customers all over the world. After this breach occurred, Dai Nippon printing company lost its reputation and its shares went down almost 75 percent. From feedback, people were worried about how the company dealt with former employees when they were fired or left the company. They should not have had the ability to access information that they used to work on.

"Merrill Lynch, one of the world's largest financial institutions, is on the list (See next page) for exposing 33,000 employee records".

In August 2007, one of the world's largest financial institutions, Merrill Lynch, had a storage device stolen. This device had personal information, Social Security numbers, and compensation details stored in it. It was estimated that 33,000 of its employees' details, including that of current and former employees, were compromised by this loss. However, there is no evidence of data used or accessed. According to feedback from the public, there were a lot of questions raised around where and how the company keeps data in use and data at rest.

2.2 Trend

The number of breaches in companies has dramatically increased in the past few years. There are various reasons why people are committing more crimes in data stealing, i.e. lack of technology to prevent it, environment, human errors and people leaving the company with data. According to data loss database, Figure 1 below shows the number of data loss incidents each year from 2002-2011. Possible reason why incidents in year 2009-2011 declined is because the use of new security software increased. Figure 2 below indicates the kinds of breaches in 2010; DLP has the ability to protect most of these events except lost/stolen media or tape.

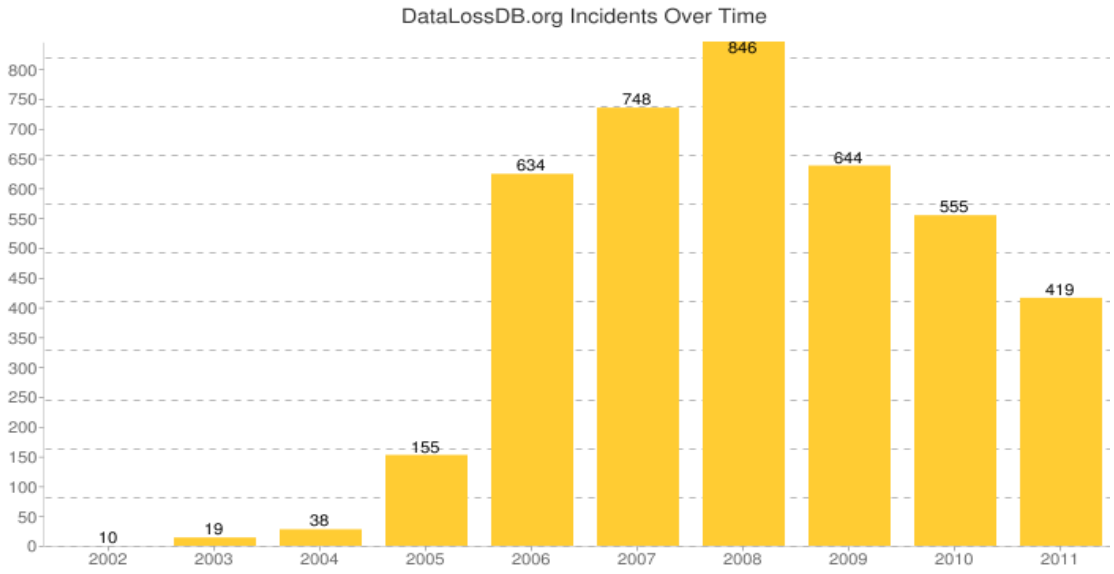


Figure: 1 Data loss from years 2002-2011.

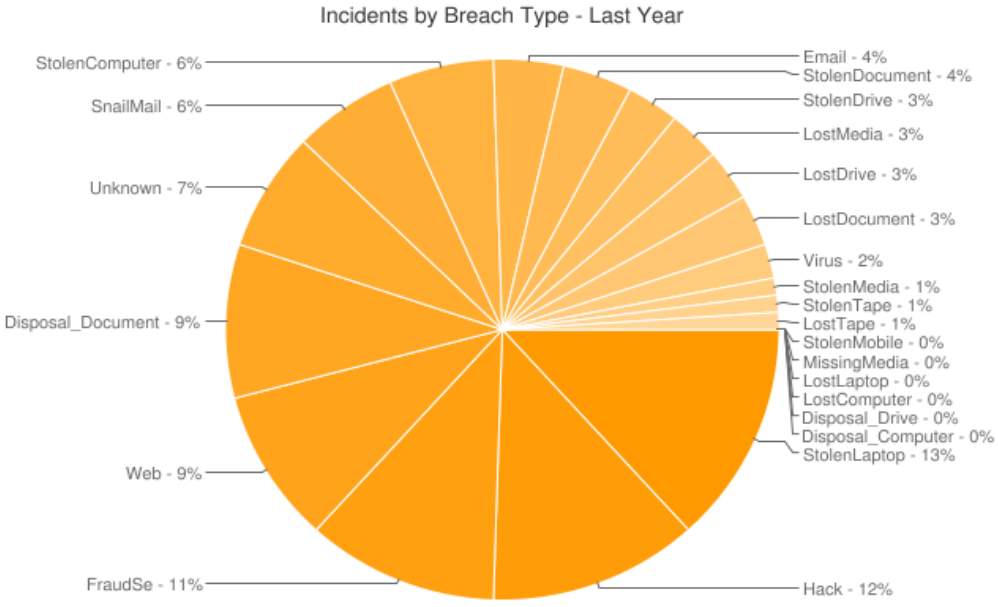


Figure: 2 Types of breaches last year (2010)

It is not only small companies that were under attack but also big companies as well.
According to the 14 most massive data breaches (Data Breaches 2007), the big companies were:

1. Citigroup loses data of 3.9 million Customers.
2. Card System Solution 40 million Visa and Master card records hacked.
3. US Dept of Veteran Affairs 26.5 million records were stolen.
4. AOL posts 20 million user searches.
5. TJX unauthorized intrusion exposed over 100 million records.
6. Dai Nippon Printing Company 8.6 million records were stolen.
7. Fidelity National Information Services (FIS) 8.5 million records were stolen.
8. TD Ameritrade Holding Corp 6.3 million data files were stolen.
9. HM Revenue and Customs 25 million child benefit records were missing.
10. Hannaford Brothers Supermarkets 40 million credit card records were stolen.
11. GS Caltex data of 11 million customers leaked.
12. Check Free Corp 5 million customer records were compromised.
13. Heartland Payment Systems 134 million records were compromised
14. US Military' Veterans 76 million records were compromised.

As can be seen, a data breach is one of the high risk areas in any company. This risk cannot be managed by only advancing technology; one of the most important factors is the awareness of people holding information. It is crucial for a company to raise awareness for their people in this area. This can be done by educating people to use a proper security tool and training them. In fact, there are many types of threats that could harm any company in both reputation and revenues. Mostly, the form of threats that often happens in the current era is listed as a data breach, which may be caused by insider threats, malware attacks, and corruption or deletion of data.

2.3 Insider threat

It is easier to explain the meaning of the word 'insider threats' first before going on to the rest of the explanation. According to Tech Terms (2007), "An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, or agency". The insider threat is someone who can access the computer systems or networks. They could misuse the information in order to harm the company. In addition, the way to commit this type of threat is very simple and easy because this cannot be detected by a firewall, network system, or any block since attackers are inside the company. Most likely, insiders could be an ex-employee, a contractor, a consultant, or someone who wants to harm or defame the company because of their own personal or financial reasons. They can execute many forms of threats such as installing viruses, worms or malwares, stealing secret information, or altering data for their own personal use (ibid). According to Reilly (2009), "Employees can commit cybercrimes much faster and easier than un-trusted outsiders". The reason why employees attempt this kind of threat is because they think that valuable information could be turned into a huge amount of money (ibid). In fact, it was shown that about 84 percents of incidents occurred when insiders sent confidential information outside the company (Ansanelli, 2005). Whether done with or without intention, it is harmful.

2.4 Malware attack

According to Tech Terms (2007), "malware refers to software programs designed to damage or do other unwanted action on a computer system". In this paper, I will focus on malware for data loss only. In fact, there are many types of malware such as viruses, worms, Trojan horses, and spyware (ibid). Malware attacks can be caused by anyone. This type of threat could happen when people download any software from an (un-trusted) site without scanning for viruses or try to update virus versions without a valid license. If attackers are successful in executing malicious code to the program, they would have the access to the computers they are attacking.

3. PREVENTION

Prevention could be the best way to minimize losses in the company. As a result of many breaches occurring recently, it is the responsibility of the company to take all the necessary actions to mitigate risk. One of the actions that can prevent the data loss or misuse is to educate employees in the organization about their job scope, role, standard procedure, and so on. This can help guide people about what they can and should do versus what they are not allowed to. However, this alone may not be enough to prevent the organization from the data loss or misuse. Technology can be brought in to support and prevent the actions taken by human either intentionally or unintentionally. Therefore, there is security software that can control information flow within the company. This software's function is different from other software. With a special tool, the software itself can do many things to protect almost every type of threats. This software is **Data Loss Prevention (DLP) Software.**
This research paper offers a good opportunity for people and companies to obtain more knowledge about data breach history referring to real case studies, experts, and past experiences of the company and learn how DLP software helps a company make more profit and reduce data loss.

3.1 DLP reduces data loss

3.1.1 Data loss prevention software

Data loss prevention (DLP) is a computer security software application that helps a company discover, manage, identify, monitor, and protect its data in use (end point), its data in motion (network), and its data at rest (storage) (Symantec, 2007).

3.1.2 Differentiation of data loss prevention software

Data loss prevention software (DLP) is one of the best security tools on the market right now. It provides many features to safeguard information for the company. DLP is different from other security software applications. For instance, the other software does not have automating block and solve issues for users right after an event occurs, sometimes they do not block affected issues in real time to stop potential data breaches because they just notify, and finally they do not provide solutions to help a company solve complex problems regarding data loss.

3.1.3 Important information for DLP

Important information for DLP can be classified into three types, which are personal information, public information, and intellectual property. In fact, this classification is the most essential to DLP because personal information or intellectuals property are things that are attractive to attackers in order to take advantage of these assets. Software has to know what kind of information is considered important so that it can use appropriate tools to protect it.

3.1.4 Data types

- Personal information
  Social security number, credit card details, health information, and family status.
- Public information
  Financial information such as stock, share, and profit.
  Human Resource information
- Intellectual property
  Patents, trademark, brand value, design, plan, strategies, control strategies, rules and regulations.

4. TOOLS AND TYPES OF DLP

There are three types of DLP, which are Network DLP, End point DLP, and Storage DLP (John and George, 2011).

4.1 Network DLP

A network DLP is a DLP system that monitors network traffic and compares traffic to a rule set for each company. The special tool in network DLP is the ability to view everyone who is running on a Virtual Private Network (VPN) or corporate network. This type of DLP can capture an unauthorized person's attempt to access the company network.

4.2 End point DLP

End point DLP is an agent that installs to end points in laptops and other mobile devices. The special tool in end point DLP is the ability to detect when an employee leaves the office for a business trip or on a long vacation. The company assures that the end point user is safe. This type of DLP guarantees that their mobile machines are not violated.

4.3 Storage DLP

Storage DLP has the ability to discover content for any purpose. Its tools can emphasize what users are using including the content of the data. This type of DLP is beneficial because it will keep secured data in an appropriate place and if someone tries to use it, the software itself will provide notification to a top manager or any person who controls the secret information. An example of storage data in DLP is credit card number, SSN, and identification types that are governed by law and regulation

5. DLP FUNCTION

DLP helps an organization in many ways for its data in use, data in motion and data at rest.

5.1 Data in use

Data in use is a small agent install in the computer (laptop or desktop) which determines work in progress of end point users. Data in use could be specified as downloading a document, printing a document, copying a document, sending a document, or clicking a document. DLP helps to verify if these actions are not appropriate to perform tasks.

5.1.1 DLP's technique to protect data in use

In fact, DLP can do many forms of protection but according to Gijo (2009), the largest danger to the company is people frequently accessing and using email to send and receive information.

> "With literally every employee in a typical organization sending and receiving more than 100 messages every day, it's an obvious vessel for sensitive and confidential information to go where it shouldn't" (ibid).

Therefore, this thesis focuses mainly on how DLP can prevent email transfer through the company. Emails come and go from many sources all over the world and there is a gap while information is sending to receiver. Someone could step in as a middle man in order to take, modify, and execute code to the original message. This situation creates risk to the company. However, DLP prevents errors on how the data was transferred from one place to another place. DLP software application has many steps to check for both incoming and outgoing email (see figure 3).

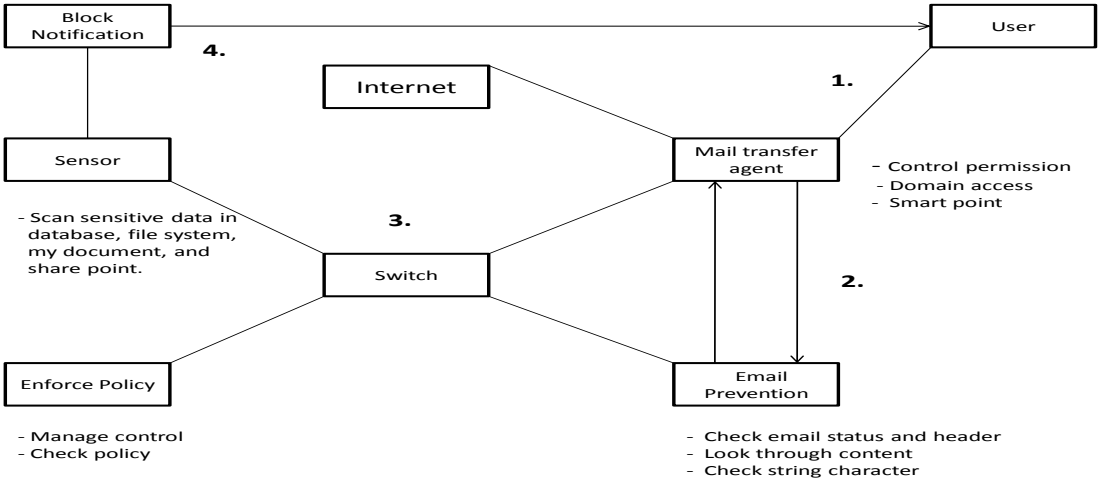


Figure: 3 illustrates steps to check email

- First, when users send or receive email, it will go to a Mail Transfer agent server. The Mail transfer server controls permission, domain access, and acts as a smart point.
- Second, the Mail Transfer Agent server will transfer every email to an Email Prevention. If the email is an email with no modification, a correct header and no execute code added; the email will be sent back to the Mail transfer agent server and processed to the Internet.
  If the email is not a good email, having malicious code or sensitive information leaks, it will be sent to a main Switch**.** At this point, the MTA acts as a smart point comparing and counting strings and characters. If sensitive information leaks, the MTA will know because more information has been added to the original email.
- In fact, according to Nate and Benjamin (2009), "DLP were set up to look for Social Security and credit card numbers, certain piece of source code, and five words in a row from a short story, which would be used to prevent any part of a special report from leaving the network"
- Third, the main Switch will pass this email to an Enforce server and Sensor server. The Enforce server will check the company's policy so see if it is compliant with IT business policy such as IT governance, law suit, and regulation. The sensor server will scan for sensitive information from the database, file system, my documents and share point.
- Lastly, if the email falls into some certain criteria, the server will block the email and send a message to warn the users as the email contains some of the sensitive data. DLP will detect unauthorized users and block unknown senders and receivers by using sensor scan (see Figure: 4 and 5).

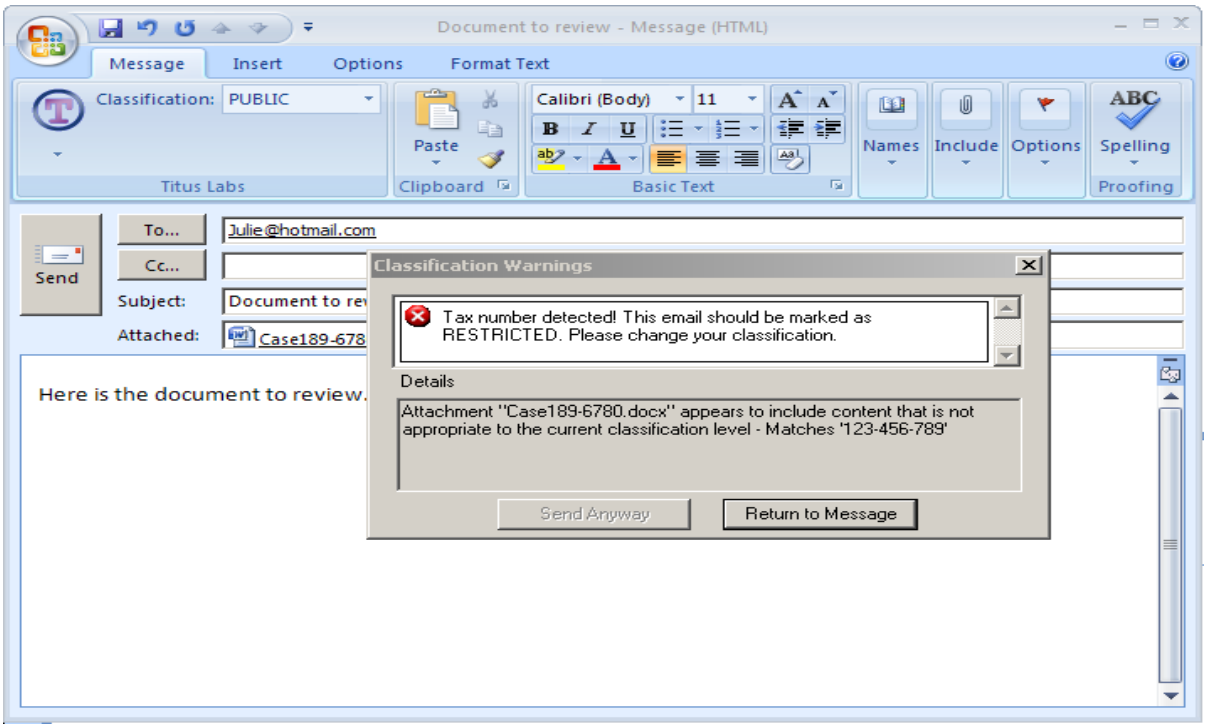


Figure: 4 shows the result of data in use that DLP detects financial information (tax number) when a user is about to send email out. It is from an Outlook program that has already installed share point, pre defined, or built in regular expressions according to policy from Titus labs test.

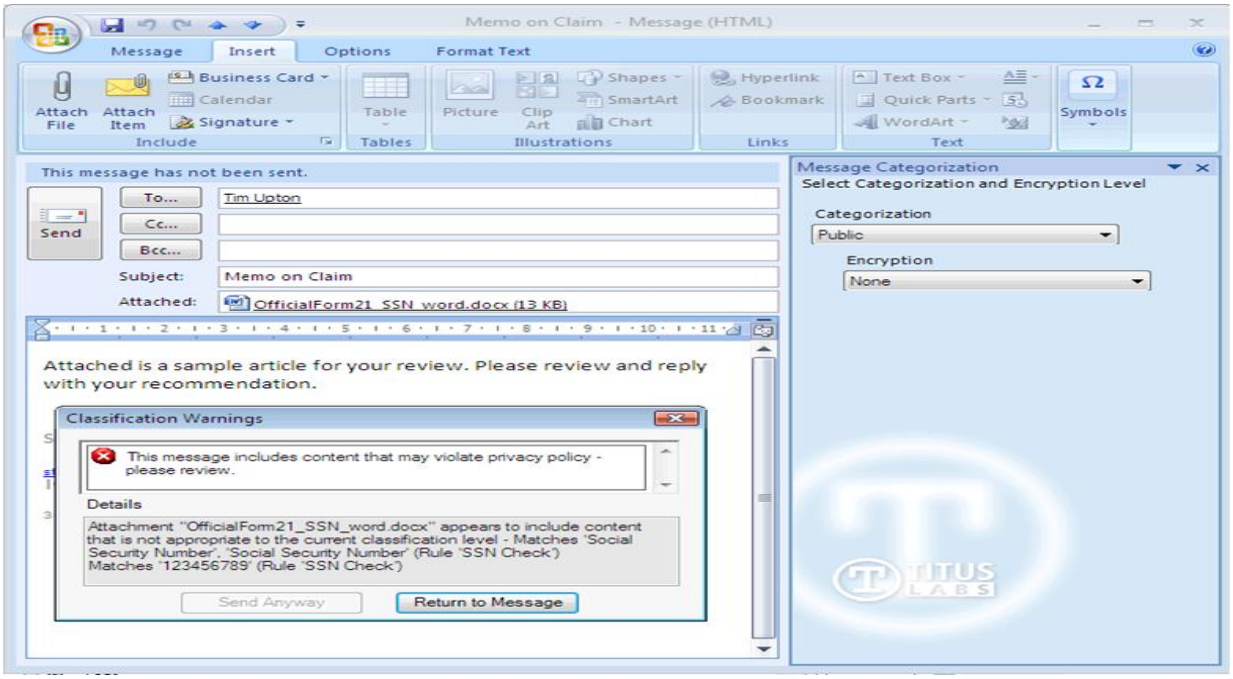


Figure: 5 shows the result of data in use that DLP matches with personal information. A screenshot is from Titus labs test.

5.2 Data in motion

Data in motion in DLP can be viewed as monitoring network traffic or blocking traffic when people send email. Data in motion is the process where DLP indicates how data is being used and transferred on the company network. It includes blocking alerts when the company sends and receives targeted information.

5.2.1 DLP's technique to protect data in motion

- DLP software can show if the users are on or off the corporate network.
- DLP software acts as tracking tool to trace where the information comes from.
- DLP software illustrates users' enterprise visibility (See figure: 6).

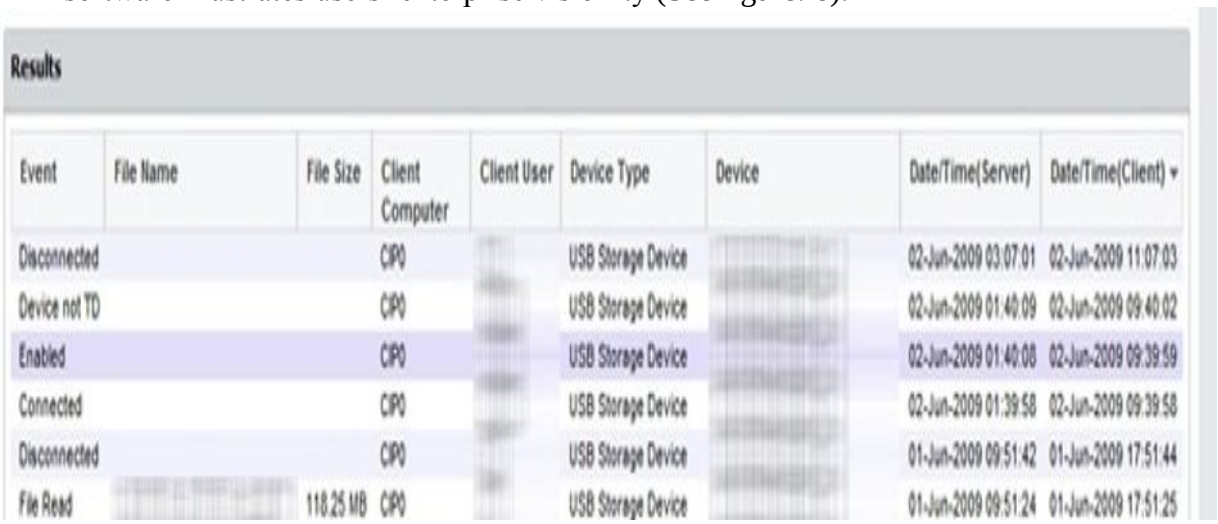
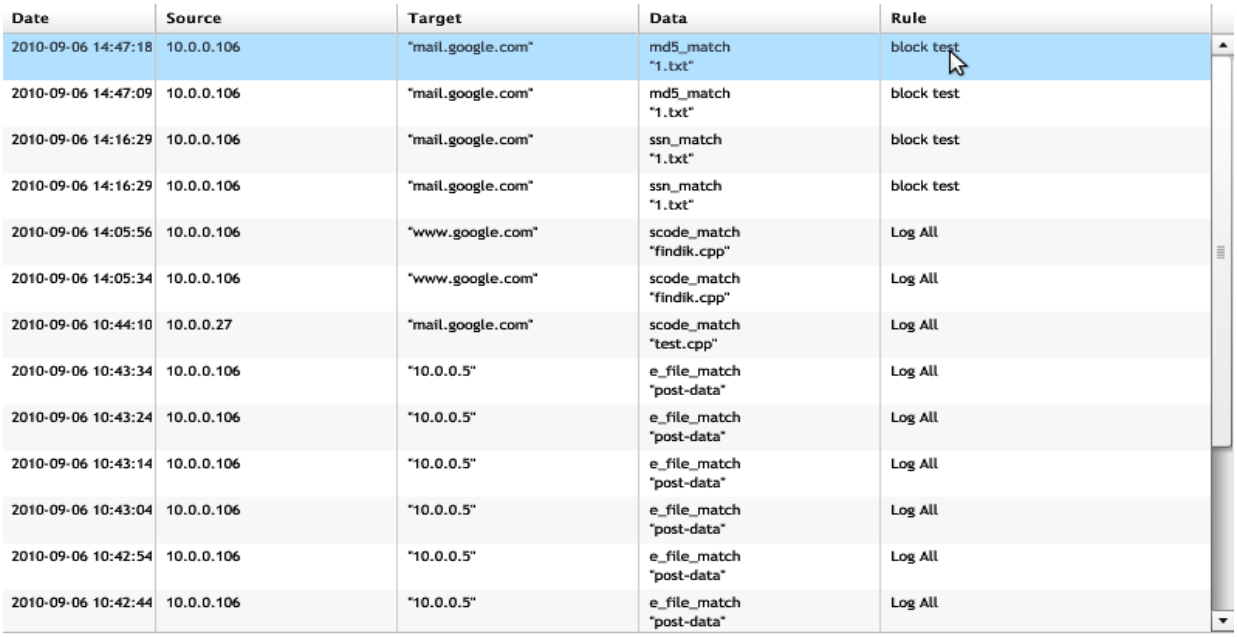


Figure: 6 shows the result of data in motion that DLP could capture from share point protector summary table.

- DLP software monitors network traffic and protects against unauthorized access.
- DLP software enforces security policy to secure data in both sending and receiving.
- Sensor server will block incoming and outgoing information. Pop up message will show up if the users are sending or receiving sensitive information (See figure 7).



Date	Source	Target	Data	Rule
2010-09-06 14:47:18	10.0.0.106	"mail.google.com"	md5_match "1.txt"	block test
2010-09-06 14:47:09	10.0.0.106	"mail.google.com"	md5_match "1.txt"	block test
2010-09-06 14:16:29	10.0.0.106	"mail.google.com"	ssn_match "1.txt"	block test
2010-09-06 14:16:29	10.0.0.106	"mail.google.com"	ssn_match "1.txt"	block test
2010-09-06 14:05:56	10.0.0.106	"www.google.com"	scode_match "findik.cpp"	Log All
2010-09-06 14:05:34	10.0.0.106	"www.google.com"	scode_match "findik.cpp"	Log All
2010-09-06 10:44:10	10.0.0.27	"mail.google.com"	scode_match "test.cpp"	Log All
2010-09-06 10:43:34	10.0.0.106	"10.0.0.5"	e_file_match "post-data"	Log All
2010-09-06 10:43:24	10.0.0.106	"10.0.0.5"	e_file_match "post-data"	Log All
2010-09-06 10:43:14	10.0.0.106	"10.0.0.5"	e_file_match "post-data"	Log All
2010-09-06 10:43:04	10.0.0.106	"10.0.0.5"	e_file_match "post-data"	Log All
2010-09-06 10:42:54	10.0.0.106	"10.0.0.5"	e_file_match "post-data"	Log All
2010-09-06 10:42:44	10.0.0.106	"10.0.0.5"	e_file_match "post-data"	Log All

Figure: 7 shows the result of a sensor server that DLP blocks sensitive information. It is a test screenshot form Titus labs test according to policy.

- DLP software can track each piece of data leaving the company by the main switch which could protect against a data leak at the very first step of sending and receiving information to and from the company.

5.3 Data at rest

Data at rest is a place where data is stored like a database, CPU, server, or USB device. DLP has a special tool for scanning these types of devices in order to sort out the information.

5.3.1 DLP‘s technique to protect data at rest

- DLP software specifies how long the data should be kept in the database or on back up media
- DLP also has the ability to identify when the data should be terminated.
- DLP software can schedule a specific time to dispose of irrelevant data.
- DLP recognizes user’s history from database to protect against unknown users.
- DLP software can trace the data on the database and its back up media (See figure 8).

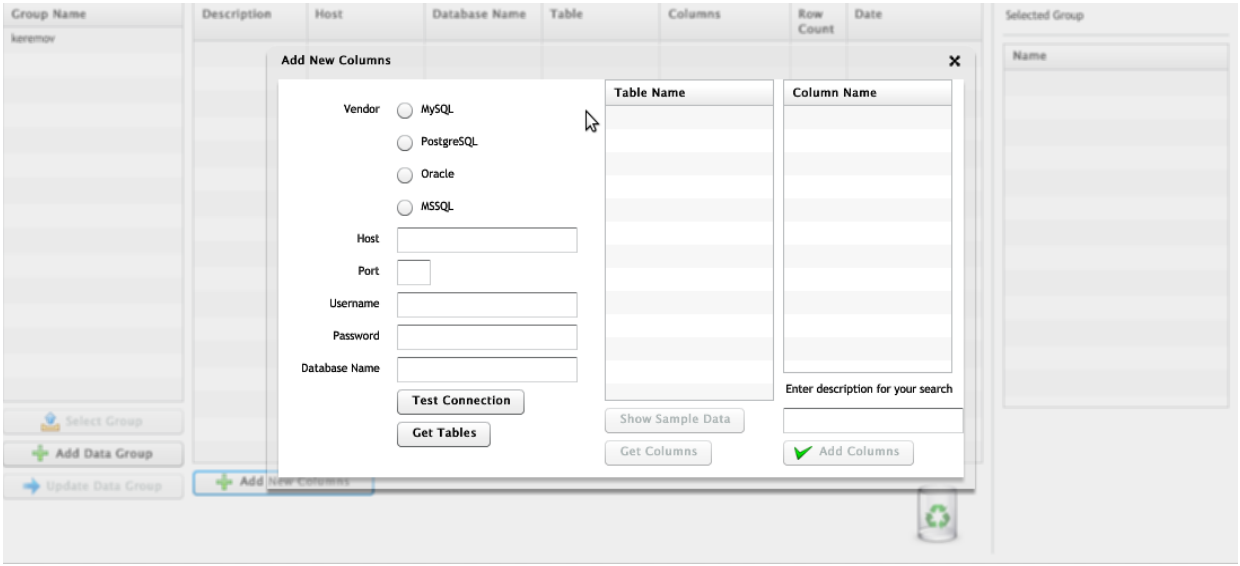


Figure: 8 shows the result of how and what DLP traces information on its database from Titus labs test as they implemented share point on a regular program.

- DLP can analyze scanning result.
- DLP can find confidential data in the company's server.

5.4 DLP work module

The way DLP works is based on the policy that is set by a company. DLP software has been set differently based on the type of businesses and the requirements around them. According to Hansmann (2010), "Not all DLP solutions provide the same functionality". Every tool in DLP performs according to policies and rules including traffic monitoring, looking for possible violations, and capturing sensitive data. DLP will do only work that matches the policy description. If DLP found the matching description, it will automatically do whatever the rules are. It will also record in DB and notify administrator if there is something wrong. This is the core function in DLP because other security software does not have this kind of special tool. However, the question arises as how to deal with information that does not match.

5.5 Setting policy in DLP

As it was stated earlier, DLP will work only if the task was stated in the policy description. Therefore, setting the DLP policy is considered the most important step. In fact, even the IT department does not know what information needs to be protected unless it was set in the governed policy, law, or regulations. Business issues are not IT tasks. IT does not know the importance of financial information so communication is key.

The financial department, human resource department, marketing department, and IT department need to collaborate together and come up with the ideas of what information must be protected in each department in order to make the most benefit to the business. Data often cannot be defined in exact dollar amounts, so classification of data helps to make it easier to manage. In this thesis paper, the classification of data is already indicated in the beginning of the thesis. This will help each department focus on its role. For example, a human resource department will emphasize personal information and the financial department will point out public information of the company (See figure 9). Moreover, experts need to be involved because they can tell and analyze which information is a priority to the company. The board of directors and share holders could be included in the meeting as well.

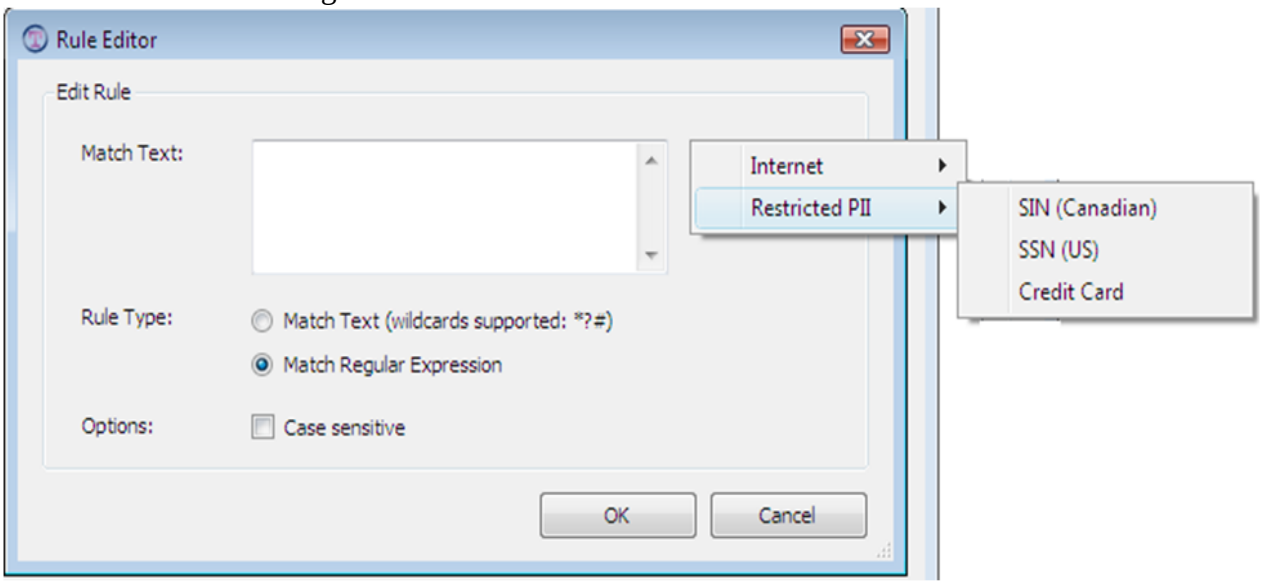


Figure: 9 shows personal information from human resource department in DLP policy.

5.5.1 Example of DLP policy

In fact, a company can set many different policies regarding to its business type. However, a common policy can be seen below;

- PCI policy (see figure 10)

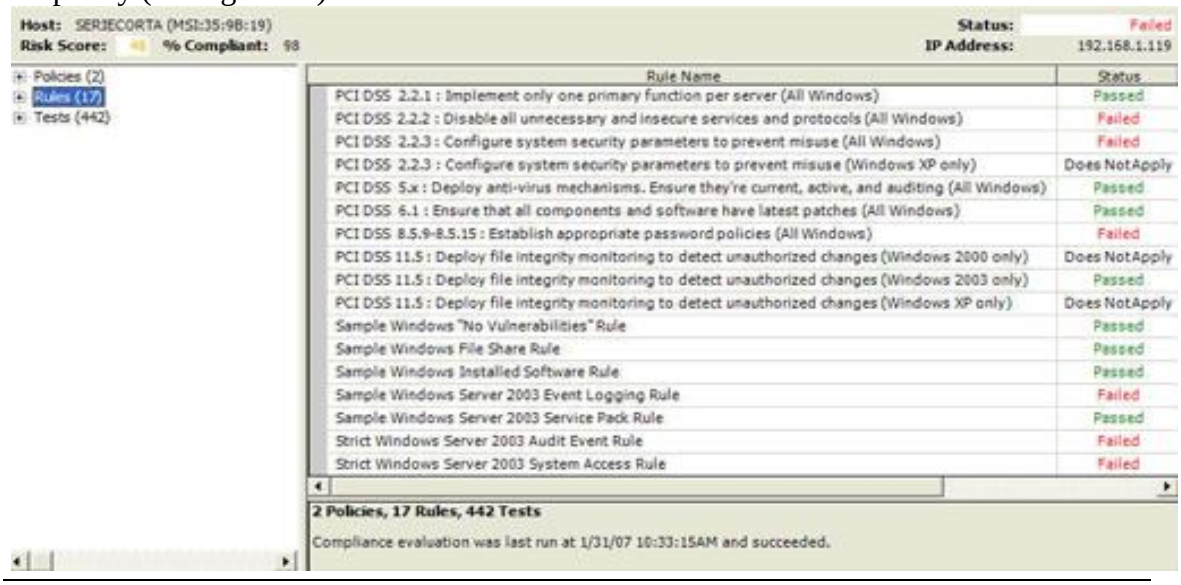


Figure: 10 indicates example of PCI policy.

- Policy to track SSN, credit card number, and important code of products (see figure 11).

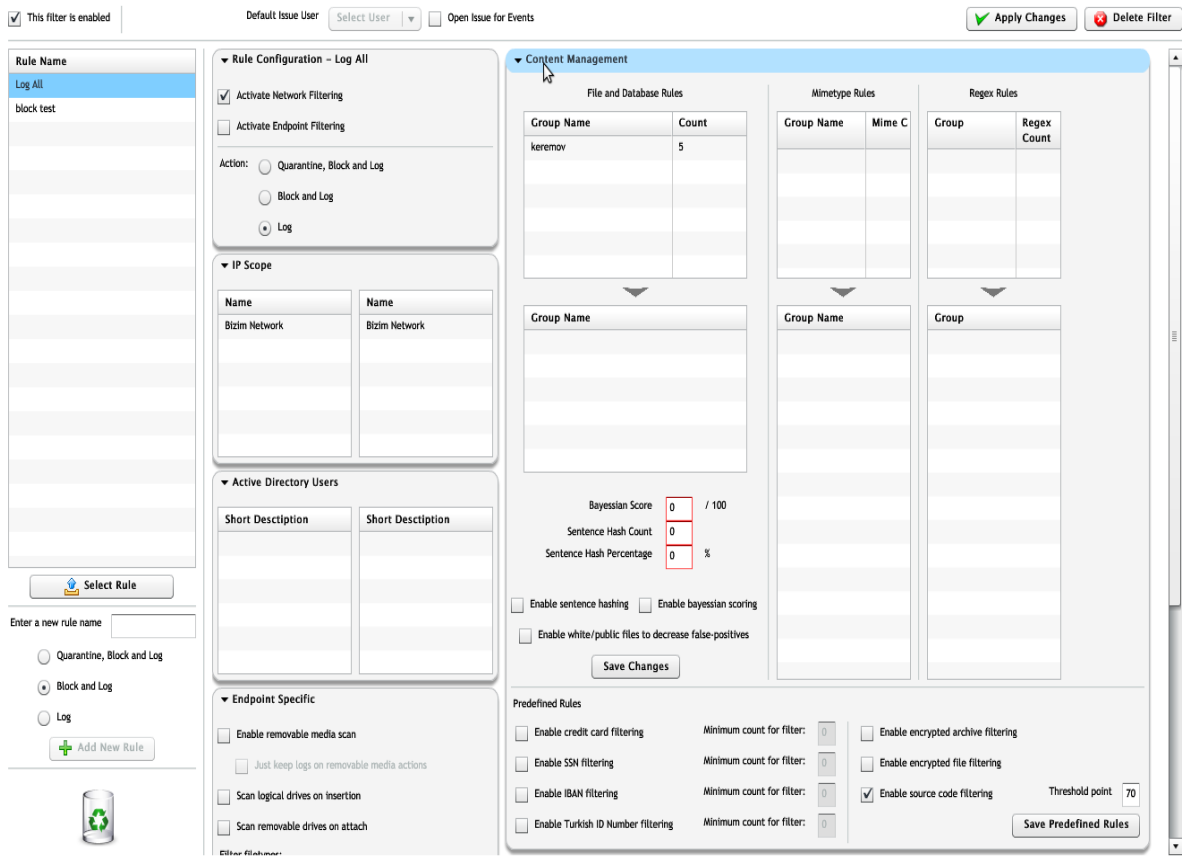


Figure: 11 is a sample screen to set a pre defined rule to track important information.

- Policy to scan physical devices (See figure: 12).

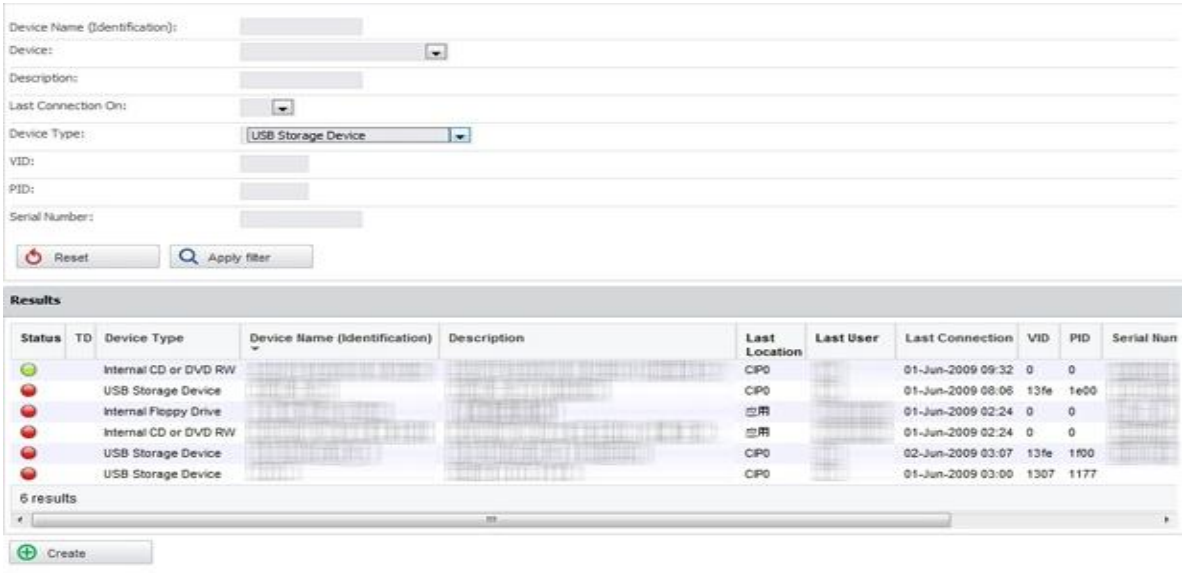


Figure: 12 is a sample screen from Titus labs test to show scanning result.

In addition, there are other possible policies in DLP.

- Capture confidential information of the company; intellectual property.
- Block tax number for each employee.
- Indicate source code.
- View port and users.

6. DLP SAVES MONEY

Recently, the loss of confidential data has become a big issue for many high profile companies. A few of these companies had to spend millions of dollars to compensate the customers for the loss of their data. For instance, when a bank is involved in this type of data loss there are more than just financial aspects. The reason is because if the customers' confidential information is leaked, the bank must re-issue cards, notify customers about their loss, and issue monetary compensations or deal with litigation problem. Most certainly a large amount of money would have to be spent in order to deal with and correct these issues. Therefore, DLP plays an essential role in protecting and mitigating this situation. DLP is not only able to save data and any intellectual properties it would also save the cost of dealing with any issues as a result of such loss. In the real world, there is a lot of security software. It depends on what risk each business needs to protect. The security software ensures that each characteristic will protect sensitive information in compliance with regulation. The security software could also effectively and efficiently help people finish work faster. Some examples of security software are:

- Antivirus software includes Norton, AVG, McAfee, Avast, and many more.
- Network security software could be Netstumbler, inSSIDer, and Hot Spot Defense Kit.
- Scanning software is Nmap, Wireshark, and VMware.
- Monitoring software consists of Refog Keylogger and Spector 360.
- Data controlling software comprises of Recuva, Eraser, and CCleaner
- Encryption software

Authentication, authorization, access control, data validation, and audit log are security software requirements. Although, DLP software covers many areas in this security field, it may not dig deeper into each function. Thus, it could be concluded that by acquiring DLP software, a company does not need to buy a lot of software to protect its business. The company could save cost in many ways such as no hiring cost for monitoring tasks, and reducing human errors that in fact could create more value to the company.

6.1 Benefits of acquiring DLP

Confidential information that will be sent within the company could be hacked, modified, and deleted for personal purpose. It is impossible for each company to buy all security software to protect their customers from every type of vulnerability. Therefore, choosing the right security software that can work well with the company is one of the most challenging tasks. However, DLP includes all security requirements and it could help the company as follow:

- More secure than other security software
- Protect IP
- Reduce audit cost
- Flexible uses of business data, for instance, do not need people to monitor the data at all times and do not need to set the data retention every month or year.
- Maintain competitive advantage
- Easy compliance with regulations
- Protect reputation
- Reduce penalty
- System can still be configured to support business needs

7. COMPARING WITH OTHER SECURITY SOFTWARE

In the internet security world, a lot of security software is available on the market. It can be divided into many categories such as antivirus software, network security software, scanning software, monitoring software, data controlling, and online transaction software. This kind of software has various vendors as well. However, this software is separated by the function it performs. For example, antivirus software cannot encrypt the data, however, it works very well on monitoring source code. As a result, a company needs to use many kinds of software to protect the data. Since security software has a specific function, DLP software has more advantages because with software itself, it can do many types of work. The company does not need to buy a lot of software in order to monitor each function.

7.1 DLP vs. IPS

As the new technology has been developed, hackers tend to attack networks in order to get access to a particular application. A web application is one of the targets (Barracuda Network, 2010). Therefore, there is a system that was created for helping the company for this kind of threat, which is *Intrusion Prevention System (IPS)*. IPS is a system that provides solution and protection to network security. IPS can monitor a network and prevent unethical activities by hackers. It is able to block and prevent some events for web application in a timely manner. Also, it can allow or deny packets after fault events are found. IPS works well under the network layer. Even though it could not secure against all 7 layers, IPS detects network level attacks such as stealth port scan, (Common Gateway Interface) CGI attacks, and protocol attacks (ibid). Lastly, IPS works efficiently by monitoring incoming network traffic and compares against a database of signatures describing all previously known exploits.

According to a brief explanation about IPS, it could not perform every type of protection because its system has limited function. As a result, the company needs to buy other security software or system to fully protect its data. Figure 13 below will describe unique security function and advantages between DLP and IPS.

Security	**IPS Firewall**	**DLP**
Secure network partitioning	No	Yes
Integrated Load Balancer	No	Limited (Symantec does)
Accelerated application delivery	No	Yes
TCP connection pooling	No	Yes
SSL offloading	No	Yes
Built in authentication engine	No	Yes
Validate encrypted sessions	No	Yes (MTA Sensor)
Multiple applications single sign on	No	Yes
Injection attack protection (XSS, SQL)	Limited	Yes
Normalize encoded traffic	No	Yes
Inspect HTTPS traffic	No	Yes (vary from different policy)
Session tampering/ hijacking/ riding protection	No	Yes
Forceful browsing prevention	No	Yes
Data theft protection, cloaking	No	Yes
Brute-force protection	No	Yes
Trojan/Warms/Virus/malware upload protection	Yes (Back Door Detection)	Yes (Block and report users'act)
Rate control protection	No	Yes
Request, response rewrite	No	Yes
Application access logging and user audit trails	No	Yes (depends on policy rule)
Regular attack updates (new signatures) are available	Yes (With support contract)	Yes
Product can detect attacks designed to overload a resource (DoS attacks-Syn Floods)	Yes	Yes
Product can detect unknown attacks and attacks that cannot be characterized (buffer overflows, DNS cache poisoning, future send mail exploits)	Yes (Stateful Signatures)	Yes (Block and report users'act)
Real time protection	Yes	Yes
Application's filtering features	Yes	Yes
Report Spammers	Yes	Yes (Record history)
Stops known and unknown threats	Yes	Yes (Record history)
comply with government regulations and consumer privacy laws	Yes	Yes (HIPPA, PII, PCI…)

7.2 Fact about successful company acquiring DLP software

Aberdeen has conducted a research about Data Loss Prevention in August 12, 2010. The research revealed that the best companies and industries deploy DLP to protect data leaks. This research can be trusted because "Aberdeen polled hundreds of IT decision makers to gauge the level of data management at industry-leading organizations" (Roumiana, 2010). The result shows that companies using email archiving solution and other programs related with content features are aware of data loss. In addition, with a special feature in DLP, companies could check process to ensure their data is protected and compliant with various rules and regulations. "The research shows that successful implementation of DLP can provide an immediate opportunity for IT security to act as a vitally important enabler for supporting the strategic objectives of the business" (ibid).

According to Aberdeen Vice President Derek Brink (2010),

"Companies leveraging content-aware technologies improve not only the organization's ability to share its sensitive data, but also to protect it" (ibid).

7.2.1 New York Life Company

DLP, the software itself does not belong to any organization. However, most big companies buy DLP software from Symantec because it is considered a leader of security software products. According to Kelly (2008), New York Life Company is one of the companies that uses DLP software from Symantec. New York Life Company acquired DLP for 'Education for Immediate Risk Reduction'. The result from New York Life Company showed that DLP

- "Proactively notified and informed employees of DLP deployment
- Deployed automated sender notification after initial deployment phases
- 80% reduction in incidents 10 days after deploying notification
- Reduced workload on remediation team
- Fixed broken business processes"

Steve Attius, Senior VP & Chief Security Officer at New York Life, believes that DLP is "The only security initiative that has proven successful at changing employee behavior" (Kelly, 2008).

Another organization that acquired DLP from Symantec is Bank of America. Bank of America combines DLP with state and federal regulations. It is not only gaining 280+ million customers' trust, but also protects IP (Intellectual Property) (Kelly, 2008). DLP helps Bank of America in monitoring and discovery of data in use, data in motion, and data at rest. According to Symantec, Bank of America achieved "over 90% reduction in risk in 12 months" (ibid).

7.2.2 MITS Networks Inc.

'MITS Networks Inc' is a company that provides solution for high technology client companies using DLP based on Trend Micro DLP software. MITS Networks Inc is located in Taipei, Taiwan. The company expertise in DLP tools and the objective of MITS Networks is to protect Intellectual Property (IP) of small industries or businesses. According to Mr. Theo Liu, the CEO of MITS Networks Inc, when he first studied DLP technology, there were many types of security software on the market but no one was able to overcome the importance of data loss like DLP. Once Liu claimed that "Using Trend Micro Data Loss Prevention, I can help my clients understand the behavior of their employees, identify policy violations, and prevent the theft of critical data assets" (Liu, 2006). Within two years, the company has proven success because it became a well known company in the high technology segment. MITS Networks' key benefits of DLP provider can be divided into three sections, which are

- Automated monitoring, blocking, and reporting
- Intelligent scanning of archives
- Delivering the solution to a growing customer base

In the end of the case, Liu concluded that DLP is the best solution to serve his clients' needs and gain attention to security in all types of businesses such as banks, government organizations, and companies with Web portals. Last but not least, the demand of DLP in Taipei keeps increasing in the IT market.

7.3 DLP is valuable to the company

DLP tools make people easily understand where the data and information is located and flowing. It is easier to find the information in the database. Also the database scans what you want to keep track of or delete (data retention). Indirect use and indirect access will not be accounted in the company's system.

7.4 Measuring company success/benefit of using DLP

It is difficult to prove whether a company is 100% successful at utilizing DLP to protect its intellectual properties. At the very least, decreasing insider threats could help provide the answer. If the employees are involved with illegal activities, the company could detect that before breaches happen. According to Hansmann (2010), "by telling employees that a monitoring technology was deployed reduced incidents by more than 10%. Once department heads were confronted with violations, employee errors were reduced by more than 80%". The benefit to each company is varying. Some could prioritize customer service as the most important and some could raise profits as the most concerned. The company should focus on what they want to achieve, acquire the tools or software, and then re-evaluate what those tools bring to the company.

7.5 Considerations before buying DLP software

Each security software tools has different strengths and weaknesses. Not every tool in DLP works well with various types of business. Therefore, before buying DLP software, the first point to consider is to determine which problem in the system cause the most damage or loss. Study about how software runs is recommended in order to get into the root of the problem. Also, educating employees in the company is a must since they all are the one who use and interact with the software.

8. RECOMMENDATION FOR DLP INSTALLATION

Policy – Do not copy policy from other companies. Even though it could be similar such as tracking Social Security Number (SSN), monitoring email header, or scheduling data retention, the policy depends on each type of business.

Notification Alert - One of the unique tools in DLP is to promptly notify users that they are attempting to senda sensitive file. DLP will block that information right away. However, after notification has been sent to users, the company needs to inspect deeper for the reason why those users did it. This is an easiest way to protect company data at the very first step before breaches happen.

Software price – DLP software is quite expensive. However the benefits do outweigh the cost. It is worth to invest in order to protect business information. It could save audit cost and the company does not need to hire third parties to look after its information which is risky because they are outsiders.

Installation – DLP software needs experts or engineers to set up at the first time. They should have knowledge about network, security, and both IT technical (software and hardware) skills.

DLP Agents – There are many agents that sell DLP software. In fact, the biggest one is Symantec (Security software leader), Websence, and Check Point. Therefore, before buying the software, the company should choose the right vendor that can be able to provide accountability of their products. This means that they are able to provide insurance or maintenance after purchase. Moreover, each vendor varies and could be categorized by specialized function.

Education – DLP is just computer software that makes life easier. However, it still needs people to process it. Therefore, the company should train and educate its employees about how DLP works.

9. CONCLUSION

As facts and cases were stated in this analysis, it could be concluded that DLP can reduce data loss and save cost in many ways. DLP protects the company from a wide range of data loss and misuse by detecting and responding to all violations that could cause extensive financial loss and damage to the reputation of the company. DLP monitors email, Instance Message (IM), Web, mobile mail, File Transfer Protocol (FTP), file repositories, and endpoint activity. Once it takes actions such as blocking, warning, quarantining, or alerting a supervisor, it helps a company protect and control sensitive data wherever it is stored or used. Since DLP offers multi-functionality, it is better for a company to utilize it than to try and acquire other software in order achieves similar result. In addition, the policy in DLP could be set differently according to business function. However, from this thesis, it could be implied that DLP is gaining the attention of other security-sensitive companies such as banks, government, and companies with web portals.

References

Ansanelli, A. (2005). *Employees the biggest threat to network security*. [Web Site]. Retrieved 6/13/2011 from the World Wide Web: http://www.networkworld.com/columnists/2005/022105faceoff-insiders.html

Barracuda Networks (2010). *Web application firewall VS. IPS*. [Web Site]. Retrieved 8/30/2011 from the World Wide Web: http://www.barracudanetworks.com/ns/downloads/White_Papers/Barracuda_Web_App_Firewall_WP_vs_IPS.pdf

Fact about data breach (2007). *15 Most Massive Data Breaches History*. [Web Site]. Retrieved 7/23/2011 from the World Wide Web: http://www.focus.com/fyi/15-most-massive-data-breaches-history/

Gijo, M. (2009). *Data Loss Prevention Roadmap.* [Web Site]. Retrieved 4/13/2011 from the World Wide Web: http://www.ca.com/files/whitepapers/data-loss-prevention-requirements-wp_203570.pdf

Hansmann, B. (2010). *How to Choose a Data Loss Prevention Tool*. [Web Site]. Retrieved 3/1/2011 from the World Wide Web: http://www.eweek.com/c/a/Security/How-to-Choose-a-Data-Loss-Prevention-Tool-256052/

John D. and George D. (2011). *"Making Data Loss Prevention Effective by Overcoming Uncertainty"* [Web Site]. Retrieved 5/12/2011 from the World Wide Web: ISACA webinar 2011

Jonathan F. (2007), Boston Business Journal. *15 Most Massive Data Breaches History*. [Web Site]. Retrieved 7/23/2011 from the World Wide Web: http://www.focus.com/fyi/15-most-massive-data-breaches-history/

Kelly, B. (2008). *DLP Risk Assessment Methodology & Implementation Best Practices.* [Web Site]. Retrieved 8/1/2011 from the World Wide Web: http://www.conferencepage.com/DLP08/downloads/vontu.pdf

Liu, T. (2006). *'Trend Micro: Securing your web world (Success Story)'*. [Web Site]. Retrieved 8/1/2011 from the World Wide Web: http://apac.trendmicro.com/imperia/md/content/us/pdf/products/enterprise/leakproof/ss03mitslp100104tw_0115.pdf

Nate E. and Benjamin B. (2009). "*Best Data Loss Prevention Tool".* [Web Site]. Retrieved 3/1/2011 from the World Wide Web: http://www.networkworld.com/reviews/2009/072709-data-loss-prevention-test.html

Reilly A. Tom (2009). *Employee Monitoring Good for the Employee*. [Web Site]. Retrieved 6/13/2011 from the World Wide Web: http://www.csoonline.com/article/476078/employee-monitoring-good-for-the-employee

Roumiana, D. (2010). *Aberdeen: Best Companies Using Data-Leak Prevention Solution.* [Web Site]. Retrieved 7/22/2011 from the World Wide Web: http://www.messagingarchitects.com/resources/security-compliance-news/email-security/aberdeen-best-companies-using-data-leak-prevention-solutions19924489.html

Symantec Corp. (2011). *Data Loss Prevention Software.* [Web Site]. Retrieved 4/20/2011 from the World Wide Web: http://www.symantec.com/business/products/family.jsp?familyid=data-loss-prevention

TechTerms (2008). *Malware Definition*. [Web Site]. Retrieved 6/13/2011 from the World Wide Web: http://www.techterms.com/definition/malware

TechTerms (2008). *Insider threats*. [Web Site]. Retrieved 6/13/2011 from the World Wide Web: http://www.techterms.com/definition/insider threat

Titus (2011). *Screenshots of share point system for Data Loss Prevention.* [Web Site]. Retrieved 5/12/2011 from the World Wide Web:http://sharepointmetadataandclassification.typepad.com/blog/2010/03/index.html

Wakao, A. (2007). *Dai Nippon Printing reports client data theft*. [Web Site]. Retrieved 7/22/2011 from the World Wide Web: http://www.reuters.com/article/2007/03/12/idUST2997420070312

Walsh, L. (2008). *2007 Data Breaches Not As Bad As We Think*. [Web Site]. Retrieved 6/13/2011 from the World Wide Web: http://www.baselinemag.com/c/a/Projects-Security/2007-Data-Breaches-Not-As-Bad-As-We-Think/