Mechanisms to Prevent lose Data

Dr. Majid Bakhtiari, Arafat Mohammed Rashad Al-dhaqm

Abstract— today the organizations have suffered from the loss data, which consider one of the threats that threaten the digital world. The human errors formed one of the reasons which cause the loss data. Therefore, the researchers have address this kind of problems and still try to get the best mechanisms to detect, prevent or mitigate it, such as physical, technical and social mechanisms. However, the loss data still growth day by day. In this paper, we will discuss the background of the loss data and the strengths and limitations of the exit mechanism as well as our suggestions to detect, prevent or mitigate loss data. We suggested two suggestions to solve this problem, the first one is merging the physical and technical techniques such as connect the portable devices with special trace systems that connected with GPS, to detect it in case of theft. Second suggestion, disappear the sensitive data (sensitive attributes) of the end users and appointments one responsible only for that data.
.

Index Terms --- Loss Data, Physical Mechanism, Technical Mechanism, Social Mechanism;

1 INTRODUCTION

Today, it seems to be universally accepted that data security is the most valuable things in organizations, it's the law. Losing sensitive data by way of natural disasters or physical theft can make a big lost for the critical and sensitive data in the entire organization. The loss data consider the most important asset for any corporation of the digital world, therefore, it define like a blood of the digital body world. Millions files transfer in cyberspace from country to country as a one unit each moment, such as emails message, downloads files, chatting, sending and receiving financial files and soon.

In this paper, we will discuss the background of loss data, reasons, the mechanisms that mitigate the loss data, strengthen and weakness of these mechanisms and the authors' suggestions.

The loss data consider is one of the threats that threaten the confidentiality of the organization, for example lost the financial data, personal information, and leak critical information to the competitors. The organizations try to prevent and mitigate this phenomenon by implement and apply many laws, policies, procedures and mechanisms to mitigate it. Many reasons which cause loss data for example, power outage, hardware (hard disk failure, CPU failure), fires, and system crashed earthquake, and floods, lightning and human error. Human errors (intended or unintended errors) are one of the biggest factors which cause loss data and difficult to detect it, such as authorized delete, update and overwriting data [1].

Organization of the Paper

The rest of this paper is organized as follow: in section 2 the background of data loss, section 3 Mechanisms that Detect, Prevent or Mitigate lost data, section 4 discussions and limitations and section 5 conclusions.

2.0 Background of Loss Data.

The problem of data loss has been came in many forms like expose a confidential data of one customer, and steal the sensitive files for any company such as source code files for any product and sale it to the competitor . Loss data may happen intended or unintended, the main factors for loss data to other side and violate the company policies and regularly requirement in this situation are insiders employees and consultants and others who steal a sensitive data about customers files, finances records, intellectual property, or other important information and sale it to third party who will pay more [1]. More than 22 sensitive and critical data loss in year of five corporations. The employees, customers, financial and IT security data have been missing owing to stolen, damage, and leaked. The personal computer, laptops, mobile equipments, emails, applications, databases and chatting message consider the main gate which the user can access through it [2]. In June 2007, in the ministry of justice in United Kingdom, owing to there are no physical measures on the computers within a security facility, also there are no any encryption mechanisms to encrypted the data, three laptops were stolen and they include data about 14,000 persons, who did not pay the fine. The data comprising personal information like names dates of birth, addresses, offences and, national-insurance numbers [2]. In February 2008, one laptop was stolen from Russells Hall

Dr. Majid Bakhtiari, **Senior** Lecturer *Faculty* of Computer Science & Information System UNIVERSITY TECHNOLOGY MALAYSIA **Skudai, 81310 Johore MALAYSIA**. E-mail: **bakhtiari.majid@gmail.com , bakhtiari@utm.my.**
Arafat Mohammed Rashad Aldhaqm is currently pursuing masters degree program in computer science (Information Security) in University Technology Malaysia. E-mail: arafat_aldoqm@yahoo.com

Hospital, and including important data about 5,123 patients. Unfortunately, there are no more protection on that laptop unless password protection [3]. In December 2007, personal information was stolen from West Yorkshire of 45,000 people. The information comprising names dates of birth and national Insurance numbers [4].

In January 2008, in Birmingham from Royal Navy recruiter about 600,000 records were stolen from laptops which include information about Training Administration and Financial Management System [5]. In October 2008, important personal data about 100,000 British military personnel was stolen from portable hard drive which including data about their passports, drivers' licences, address and names. In June 2007, in the ministry of justice in UK the portable 500G hard-drive disk containing personal details of 5,000 prison governors and guards was stolen. The disk includes names, dates of birth, national insurance, prison service employee numbers and addresses. The disc was sent to Mitcheldean, Gloucs, for testing in Washington, Wearside, on July 20 last year, subsequently moved to Telford, Shrops [6].

In December 2007, four compact disks were lost in the post. The compact disks were sent by recorded delivery but never delivered. The investigator of Court management will not evidence whether the data was encrypted or not [7].

In September 2008, during the way to the organization's office in Birmingham, the disk has stolen and includes personal data about 11,423 teachers, and unfortunately, there is no any security mechanism on it, only the password and user ID[14].

The insider employees have many ways to expose and steal sensitive data, so they formed more threaten than the outsider because they know and have authorized access to these data. Therefore, the organization must protect data which move through the networking and the data which reside in corporations like databases, as well as protect data in the endpoint like data on USB devices [1]. Therefore, to avoid data loss, the companies must evaluate their specific vulnerabilities for each loss vector and respond appropriately. According to studying which perform on two sources to evaluate magnitude of data loss in the United State: First source, Request data from insurance company that protect computer hardware. Second source, survey data from a company that specializes in data recovery. Figure-1-, shows the statistics which explain that the hardware failure forms 40% of data loss, and 30% human error accounts, which include the deletion data and damage to the hardware, for example damage occurred by abortion laptop. Software corruption forms 13%. Computer viruses comprising boot sector and file infect viruses' forms 6%. Theft of hardware, especially prevalent with laptops, accounts for 9% of data loss incidents. Finally, hardware destruction, which includes damage, caused by floods, lightning and fire, accounts for 3 percent of all data loss [8].

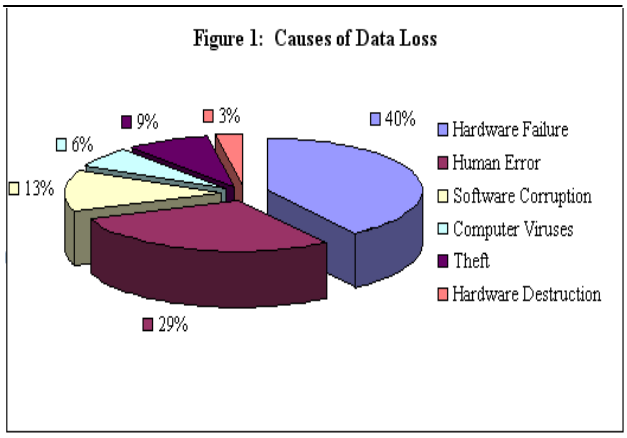

Figure.1.

3.0 Mechanisms that Detect, Prevent or mitigate lost data.

There are many different security mechanisms that detect, prevent or mitigate the loss data. In this section we will concentrate on the physical mechanisms, technical mechanisms and society mechanisms, which help to detect, prevent or mitigate loss data.

3.1 Physical Mechanisms

As we see above the main cause of loss data is not only the hacking or cybercrimes. However, recently reports which are coming from Irish Telecom Company referred that the physical loss and theft laptops formed another threat to loss data. Therefore, there are three laptops were stolen and including personal data about 7,000 customers and employees and their sensitive data like accounts and other sensitive data [9].

The physical loss of the devices like laptop, computers, mobiles and portable media formed 30% of data breaches. Therefore, and for the above reasons that cause loss of data, must have procedures and measures to prevent or mitigate these kinds of thefts. There are some physical measures that prevent steal laptops and computers such as: physical laptop locks that prevent data loss, through prevent the laptops move from it place [10].

The perimeters fences, gates, lighting, CCTV, detection alarms, trained guards, infrareds and beams, intruder detection systems, hard locks, and glass protection can prevent and mitigate the physical stolen to the computers and laptops deceives[11].

3.2 Technical Mechanisms.

The technical mechanisms formed the second layer for protection and prevention lost data. Data encryption, authentication, authorizations are consider the best example about these kinds of mechanisms. However, the data encryption may be considered the most effective mechanism to protect confidential information of the organizations [12].

[13] There are many ways to protect the important data from loss or unauthorized access, such as, first: backup database regularly and early, can protect data from loss. Second: Use Encrypting file system. The EFS utilize the mechanism of asymmetric and symmetric encryption, for security and performance. Third: used disk encryption, to encrypt whole disk that protect whole content of disk. Disk encryption can be used to encrypt portable drives like flash drives, USB drives. Fifth: public key infrastructure, used to protect data that you share it with someone else. Sixth: Hide data with Steganography, this way allow you to hide data inside objects. Seventh: Secure wireless transmissions: the data that send through wireless is less secure that data sent through network wired, owing to the interception. Therefore you should send or store data only on wireless networks that use encryption, preferably Wi-Fi Protected Access (WPA), which is stronger than Wired Equivalent Protocol (WEP).

3.3 Social Mechanisms.

The organization should identify the most sensitive business data and put a set of security procedure and guidelines such as security policies, training the staff and security awareness, training the staff and implement technologies to mitigate user errors, policy, violations, and internet attacks. It also recommends monitoring controls and procedures to ensure compliance and increasing the frequency of audits [2].

4.0 Discussions and limitations.

Although there are many mechanisms that the organizations and governments try to used it to detect, prevent or mitigate the loss data, however, the steals data still occurred and all the mechanisms that they have been used have a weakness and could not prevent 100%. For example the CCTV can detect the physical thefts but could not detect who is steal the data, other weakness of CCTV, owing to the power supply for CCTV is electric, therefore, the professional attackers can cat the power, and then the function of CCTV will be not there.

The weakness point of the physical laptop locks is the attacker can cut that cable by cutting tools and steal it easily. The technical and social mechanisms consider the better solutions for the mitigate and prevent loss data, however, also have still weakness such as who can detect the authorized people who leakage and loss data to others, as well as the professional hackers may can get the password or can decrypt data.

In our point of view, we have suggest to merge the physical and technical techniques such as connect the equipments like laptops, and mobiles, portable hard disks and so on, with special systems that connected with GPS . These special systems have all information about all equipments in any corporations, and when the incident happens the systems can trace the stolen equipment in anywhere. Other suggestion in terms of sensitive data and correlation it with authorized entities. It is better to disappear the sensitive or critical information to end users, and give them applications with general information and the give the sensitive information to one person only, and in this situation, can mitigate the leakage of the information through the authorized persons, for example, hide the details amounts and appear the total amount only, and in this case the end users and also the DBA, cannot determine this amount go to where, and who will get this amount, only one person have this responsibility and finally can distributed this amount to other persons in other database or in special tables who is responsible on it, therefore, if there are any leakage of data , the organization can determine the responsible as far as possible.

5.0 Conclusion

Loss data consider one of the threats which threaten the digital world. A lot of reports and complaints have sent every day to the investigation offices to looking about criminal loss data. There are many mechanisms to detect, mitigate or prevents steals data such as physical, technical and social mechanicals. However, the loss data still growth day by day. In this paper we suggested two methods to detect prevent or mitigate loss data. We suggested merging the physical and technical mechanisms such as connect the portable devices which kept the data, with special trace systems that connected with GPS, to detect it in case of theft. Second suggestion, disappear the sensitive data of the end users and appointments one responsible for that data.

6.0 References:

[1] B R A D L E Y .R . H U N T E R. 2007. Data Loss Prevention Best Practices, Managing Sensitive Data in the Enterprise.

[2] ZDnet, Ministry of Justice report nine data breaches, 18/8/2008. Retrieved from http://news.zdnet.co.uk/security/0,1000000189,39462444,00.htm

[3] Express and Star, 5,000 patient records stolen,14/2/2008. Retrieved from BBC, Nine NHS Trusts lose patient data, 23/12/007. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/7158019.stm

[4] Telegraph, Housing benefit details latest to be lost, 3/12/2007.Retrieved from http://www.telegraph.co.uk/news/uknews/ 1571192/Housing-benefit-details-latest-to-be-lost.html

[5] Herald Tribune, U.K. reports new data loss for 100,000 military staff, 10/10/2008. Retrieved from http://www.iht.com/articles/2008/10/10/europe/britain.php

[6] Herald Tribune, U.K. reports new data loss for 100,000 military staff, 10/10/2008. Retrieved from http://www.iht.com/articles/2008/10/10/europe/britain.php

[7] ZDnet, Ministry of Justice loses four CDs of personal data, 23/1/2008. Retrieved from http://news.zdnet.co.uk/security/0,1000000189,392 92348,00.htm

[8] David M. Smith, PhD. 2003 Volume 6 Issue 3. The Cost of Lost Dat. The importance of investing in that ounce of prevention" of personal data, 23/1/2008. Retrieved. http://gbr.pepperdine.edu/2010/08/the-cost-of-lost-data.

[9] http://clicksafe.kensington.com/laptop-security-blog/bid/78733/Serious-data-loss-highlights need-for-physical-data-loss-prevention.

[10] Serious data loss highlights need for physical data loss prevention. http://clicksafe.kensington.com/laptop-security-blog/bid/78733/Serious-data-loss-highlights-need-for-physical-data-loss-prevention

[11]. Elio Zannoni. 2003. Preventing computer theft http://www.securitysa.com/article.aspx?pklarticleid=2664.

[12]http://www.spamlaws.com/data-encryption-benefits.html.

[13] Deb Shinder. 2006. 10 things you can do to protect your data. http://www.techrepublic.com/article/10-things-you-can-do-to-protect-your-data/6061927.

[14] Vnunet.com, Data loss exposes t eachers' records, 26/9/2008. Retrieved from http://www.vnunet.com/vnunet/news/2227046/gtc-loss-scandal.

.