IJAR&D
Vol. 2, No. 2, July-December, 2016, pp. 16-22

An Empirical Study on Data Breach, Cost Involvement to Encounter this Significant Cyber Security Threats

Arkaprava Chakrabarty

Faculty, Management Studies
Institute of Leadership Entrepreneurship and Development (ILEAD), Kolkata

Abstract

The present paper examines the effects of data breach in various Banking, Financial and Industrial Sectors as well as individuals where it has a massive impact. Data breach is an essential security issue by which any concern's sensitive, protected or confidential data are pilfered, transmitted and gathered by unauthorized individual or group of individuals. This paper attempts to find out the various types of data breach which may affect the economy of any country as a whole. The paper is also trying to analyze the report of some certified international institutions about the cost of data breach study, the level of concentration of some countries to counter the data breach or some unprecedented incidents. Using various graphical representations on cost to prevent data breach or security threats by different concerns, this study also endeavoured to show the assessment of risk by using the technique of Breach Level Index to observe the magnitude of data breach risk for a particular company, institution and organisation. It also tries to evaluate the need of computing the risk and also suggests the remedial measures for the purpose of prevention.

Key Words: *Industry Reaction, Data Breach Summit Asia 2015, Ponemon institute's Report Analysis, Breach Risk Assessment, Breach level Index, Prevention Tips.*

Introduction

In the present days the books of accounts of any concern whether it is domestic or international is maintained electronically. The softwares which are used for the purpose of recording are programmed as per i) the Traditional Techniques, ii) the Accounting Standards of the respective country, or as per iii) the International Financial Reporting Standard (IFRS), the modern way of treatment. Financial reports based on IFRS are worldwide acceptable now.

Manual recording of transactions has become obsolete now for obvious reasons. Electronic maintenance makes it easy, speedy, accurate and convenient to users. Updated information of Government duties, tax rates, interest rates etc is available online. Synchronization of the accounting system with internet based data /rules as per changes made by appropriate authority time to time, is a must in modern times. Hence, the necessity for securing the records by various anti malware or antivirus is felt.

Objective of the Paper

In the recent days various cyber security threats are spreading their dangerous arms everywhere. They can easily destroy the system's network of the particular concern at any time if the security package of the organization is not made powerful. The objective of the paper is to classify the various cyber security threats which may affect the system, boot process, programme etc. The paper concentrates on a particular security threat called "Data Breach" by which all the personal data of an organization can be stolen by some unscrupulous sources without any knowledge and consent of the aggrieved party or administrator. The paper presents:

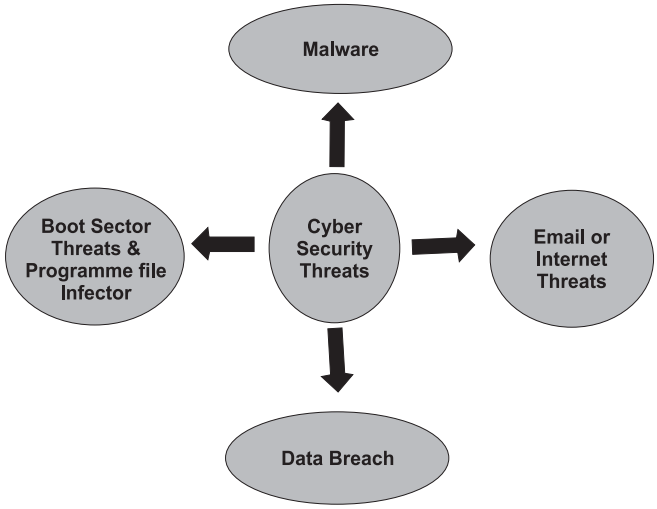
i. The process of the data breach and huge expenses incurred for its prevention.

ii. A procedure to evaluate the level or degree of data breach. and

iii. The various precautionary measures which are needed to protect the system or network from this particular cyber security threat.

About Cyber Security

Today cyber threats or computer viruses are a serious issue as well as the other software's or applications of the computer. The first computer virus isolated in 1982 named Elk Cloner. It infected the Apple DOS 3.3 operating system, displaying a short poem when an infected computer booted up for the 50th time. After that the world witnessed the panic of Michelangelo virus in 1990 and the devastating effect of SoBig-F virus in 2000 and the incidents have been continuing by the cybercriminals. These viruses, internet worms, malware, spyware can damage the computer system with disturbing elements and can destroy the important files from the hard disk. The degree of damages to the computer depends on the capacity of the viruses. These are:



Source: Self Created

Various Types of Cyber Security Threats

1. Malwares

Malware is a general term for malicious software. Malware includes viruses, worms, Trojans, Adware and Spyware. Many people use the terms malware and virus alternatively.

- Spyware is any programme that monitors the online activities or installs programmes without the consent of the aggrieved party or captures personal information. These may collect, display targeted advertisement.
- Trojans are malicious programmes which are generally created from pirated software applications and serial number generations which create fake and illegal license codes for some sites and games as per requirements. It pretends to be legitimate software, but actually carry out hidden, harmful functions.

2. Email and Internet Threats

These are the threats that can affect the computer while it is connected with the Internet. Sensitive financial or personal information are transmitted illegally through fraudulent email or instant messages. Some of the most common attacks include:

- DNS Hijacking: The Domain Name System (DNS) is the phone book of the Internet. This threat can capture the system capacity to translate the websites into IP address number.
- Bonk: An attack on the Microsoft TCP/IP stack that can crash the victim computer.
- Denial-of Service Attack (DoS): It is an activity by a hacker to stop the service of network by the user.
- Phishing Emails: It refers to the process of deceiving recipients into sharing sensitive information with an unknown and unauthorized person.
- Patches: Patches are software add-ons designed to fix software bugs, including security vulnerabilities in operating systems or applications.

3. Boot Sector Threats and Programme file Infector

- Win Nuke – An exploit that can use NetBIOS to crash older Windows computers.

4. Data Breach

The various threats can result a Data Breach of systems. A Data Breach is the release of secured and confidential information to an unreliable path or environment. It is an essential security issue by which any concern's sensitive, protected or confidential data are pilfered, transmitted and gathered by unauthorized individual or group of individuals. Data breach may involve the information of financial institutions viz. banks, personal health information (PHI), Personal identifiable information (PII), Companies confidential information etc.

Process of Data Breach

Even though it's all about unethical activity, we should be aware of the general techniques used by the hackers and the cyber criminals at the time of Data Breaches. A typical data breach occurs in three phases:

1. **Study on Weaknesses**: Before the attack of data breach of any concern, the cyber criminals concentrate on the weaknesses of the concerns like target employees, his or her social networking profile, the system of the concern and its network. The findings of these types of study depend on the degree of security protocol of the targeted organization.
2. **Execution of Plan or Attack:** Having scoped out his target's weaknesses, the cyber criminal makes initial contact through either a network-based attack or through a social attack.
   a. In a **network** attack, the cybercriminal uses the weaknesses in the target's infrastructure to get into its network. These weaknesses may include, inter alia SQL injection, vulnerability exploitation, and/or session hijacking.
   b. In a **social** attack, hackers generally send a malicious crafted mail to one of the employees. The process may run after opening the files of the mail or after providing the personal data of the employee or the organization in reply to the original mail. This type of mail is called phishing mail.
3. **Transmitting Information:** After entering into the network of the administrator unethically, the hacker transmits, or encrypts the data or information back to him. This data may be used for either blackmail or negative propaganda. It may also result in the cybercriminal having enough data for a more damaging attack on the infrastructure as well.

Breach Level Index

The present paper examines the degree or level of index with the help of some parameters. These parameters classifieds in the following contents.

1. **Breach Record or total number of records breached in a certain period of time in a concern whether it is profit seeking or nonprofit seeking.**

Score :	**0 .....**	**1 .....**	**2 .....**	**3 .....**	**4 .....**	**5 .....**
Data No.:	**0**	**10**	**100**	**1000**	**10000**	**100000**

2. **Types of data which are generally breached.**

i. Nuisance (email address, affiliation etc). **(Score 0)**

ii. Account access (username, password of social media) **(Score 0.3)**

iii. Financial access (bank account credentials, credit card details) **(Score 0.5)**

iv. Identity theft (SSN, ID number, name, medical records, date of birth) **(Score 0.6)**

v. Existential data (national security or business id) **(Score 0.7)**

3. **Sources of data breach or reasons of breaching the records.**

i. Lost device **(Score 0)**

ii. Stolen device **(Score 0)**

iii. Malicious Insider **(Score 0.5)**

iv. Malicious Outsider **(Score 0.6)**

v. State Sponsored **(Score 0.7)**

4. **Scope of breaching data**

i. No action was taken at the right time. **(Score 0)**

ii. Publicly disclosed concern's confidential data. **(Score 0.7)**

iii. Data are disclosed to the outsider for financial gain. **(Score 1.0)**

5. **Organization's Location**

All the surveys are made in India

6. **Organization Industry**

i. Education

ii. Financial

iii. Government

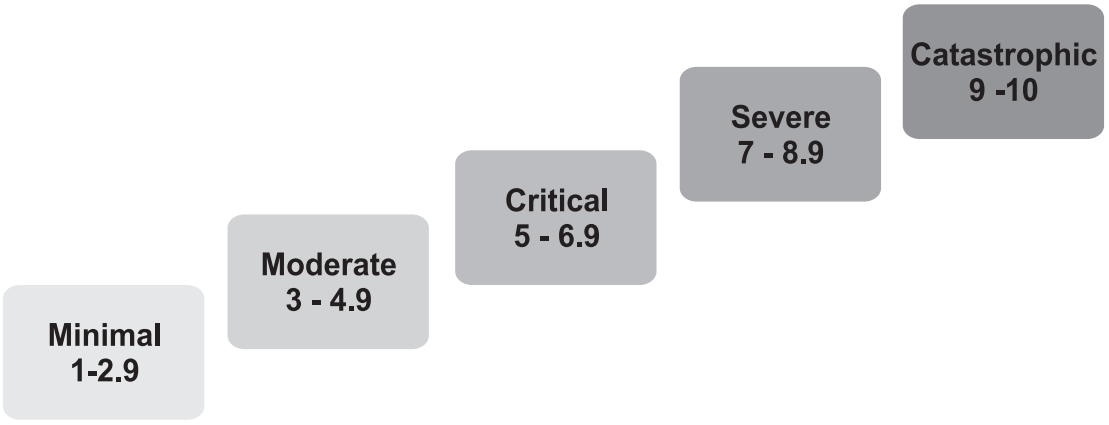
iv. Healthcare

v. Retail

vi. Technology

vii. Other

Five Types of Risk Score



Source: Self Created

From the above shown diagram of risk score we can elaborate the degree or level of risk score. The first parameter reflects the number of records of a particular concern which are breached. As the number of records breached increases, the score will increase. But here the measurement for the level 1-2 is 10 times for each score, whereas the same from 2-3 is 100 times and from 3-4 is 1000 times.

The second parameter shows us the types of data which are generally breached. Here due to nuisance the risk is minimum, whereas for Existential data like national security or business id. The government concern specially should take special care of it.

The third parameter represents Sources of data breach where lost data carries minimum score and state sponsored carries highest score.

Under the Scope of breaching data, the next parameter we can easily calculate the causes of spreading the breach. By adding these scores we can compute the total score of risk and find out whether the risk or breach is harmful for the concern or not. And also the urgency of the remedial can be easily determined from this particular score.

Statistics of Indian Data Breach from 2013 to 2015

Rank	Organization Breached	Date Breached	Records Breached	Location	Industry	Source of Breach	Type of Breach	Risk Score
1	Bharat Sanchar Nigam Limited (BSNL)	4/7/2015	30,000,000	India	Government	Hacktivist	Existential Data	9.5
2	TRAI (Telecom Regulatory Authority of India)	24/04/2014	2,000,000	India	Non Government	Malicious Outsider	Account Access	7.9
3	Principal Controller of Defence Accounts	10/4/2014	50,000	India	Government	State Sponsored	Identity Theft	7.0
4	Aadhaar	28/03/2013	300,000	India	Government	Accidental Loss	Identity Theft	6.8
5	Government of Maharashtra	11/4/2013	300,000	India	Government	Accidental Loss	Existential Data	6.2
6	City and Industrial	19/09/2014	85,000	India	Government	Accidental	Financial	6.1

	Development Corporation's (CIDCO)					Loss	Access	
7	Department of the Brihanmumbai Municipal Corporation	15/06/2013	9,500	India	Government	Unknown	Existential Data	5.4
8	Indian websites	29/01/2014	2,118	India	Non Government	State Sponsored	Nuisance	5.0
9	Satta Matka Results Guessing	20/10/2014	389	India	Non Government	Malicious Outsider	Account Access	4.5
10	OlaCabs	30/08/2015	400	India	Non Government	Accidental Loss	Identity Theft	3.9
11	Axis Bank	31/05/2013	37	India	Financial	Malicious Outsider	Financial Access	3.6
12	Infosys	12/6/2015	23	India	Financial	Malicious Outsider	Financial Access	3.4
13	Madhya Pradesh police	29/11/2015	Unknown	India	Government	State Sponsored	Existential Data	2.4
14	Rural Administrations Centre	3/8/2015	Unknown	India	Government	Malicious Outsider	Existential Data	2.3
15	Ahwa	17/03/2015	Unknown	India	Government	Malicious Outsider	Existential Data	2.3
16	Defense Research And Development Organization	13/02/2013	Unknown	India	Government Malicious	Outsider	Existential Data	2.3
17	Lucknow University	27/11/2015	Unknown	India	Non Government	Malicious Outsider	Identity Theft	2.2
18	Essar Group	26/07/2015	Unknown	India	Non Government	Malicious Insider	Existential Data	2.2
19	Naaptol	8/6/2015	Unknown	India	Retail	Malicious Insider	Existential Data	2.2
20	Bharti Airtel	13/04/2015	Unknown	India	Technology	Malicious Insider	Existential Data	2.2

Cost to Data Breach Analysis

The study of cost to data breach means the expenses incurred to prevent the system from data breach. For the purpose of study the paper evaluates the report of an international institution of Prevention and information security named Ponemon Institute.

Ponemon Institute - Background

Ponemon Institute established on 2002 by Dr. Larry Ponemon is a research center dedicated to provide protection policy of data and information of any business concern. It is a parent organization of the Responsible Information Management Council (RIM) at present the headquarters of the Institute is at Traverse City, Michigan, USA.

Report Analysis

The global research study 2015 of Ponemon Institute about cost of data breach reflects the cost incurred by 11 countries around the world. Here the total cost is divided into two parts called direct and indirect. Direct costs include Forensic Export Expenditures, Hotline Support Expenditures, Free credit monitoring subscription and Discount for future products and services. On the other side indirect costs include In house Investigation and communication costs and Extrapolated Value of

customer loss resulting from turnover or diminished customer acquisition rates.

It is revealed from the report that in 2015 the cost of data breach increased due to following reasons:

1. On account of Infrastructural development. As the variety of threats increases, the protection cost for the same also increases. Last year, these attacks represented 42% of root causes of data breach and this increased to 47% of root causes in this year's study.
2. For the purpose of prevention, the system analyst need to incur some associated expenses for detection and escalation like forensic and investigation expenses, assessment and audit service expenses etc. As per the report the average cost increased from $0.76 million last year to $. 0.99 Million in this year.
3. There are many business concerns which were already affected by data breach in last year. To recover themselves from that situation they have incurred huge expenses for Recovery of lost customers, increasing customer acquisition, recovery of old reputation or goodwill etc. This type of costs increased in this year from $1.33 million to $1.57, million.

Here is a statistics of 11 countries incurred the maximum amount of expenses for preventing data breach.

Amount: in $ million Source: Self Created

From the graphical representation we can see that the 1st world countries like USA, France or UK are spending massive amount for the purpose of prevention of their system and network for the effects of data breach, whereas the Asian countries like Japan is much slower than them. In spite of plenty of examples or incidents of Breach country like India is spending very small amount of money to prevent it. This tendency or carelessness in policy making cannot prevent any country from the curse of unethical hacking. The citizens of the country often witnessed the circumstances like hacking of defense's Website; National Level Institution's Site, Company's

System hacking, hacking in Core Banking Solution System of the National and Private Banks etc. India should conscious about maintaining tight security protocol system to protect its assets.

Prevention Procedure to Counter Data Breach

As observed by the Ponemon Institute (Institute of Research dedicated to privacy, data protection and information security), the insiders of the organization are the major sources of data breach. On the other hand the external threat category includes hackers and state sponsored activities. Here some of the prevention techniques are discussed---

1. Equipped employees for handling sensitive information: Education and training of the employees for the purpose of security is very important. There are some decorum for protection like reduction of unnecessary data, defragmentation of data, purging of data responsibility of the expired one.
2. Establish comprehensive data protection plan: Every concern should maintain a proper anti malware or firewall system to protect its organized data or information.
3. Compute a periodic risk assessment: Every concern should assess its level of risk or "risk score" through breach level index or some other procedures on a regular interval. As the viruses and threats are upgraded day by day, the concern should be aware of the specific protection protocol.
4. Regular updating of the security softwares (or patches): An unpatched or unprotected system, operating with a weak and updated spot will be exploited by hackers. Admittedly, applying patches takes time and resources. So senior management must provide guidance on allocations and expectations.
5. Make parity between the vendors and the partners: It's important to define the security requirements upfront with vendors, third party service providers may be required to maintain appropriate security measures in compliance with certain state or federal regulations.
6. Provide training and technical support to mobile workers: The concern must ensure that some standards for data security are applied regardless of location, by providing mobile workers with straight forward policies and procedures, ensuring security and authentication software is installed on devices and kept up to date. Providing adequate training and technical support for mobile workers are also essential.

Conclusion

Data breach, as accepted all over the world, is an essential security issue. These untoward processes not only jeopardize individual organization's interest but also endanger the economy of the country as a whole or

its defense mechanism. Assessment of risk, huge expenditure and effort to counter data breach and search for finding remedial are therefore felt as a desperate need of the present days. We must keep our vigil on this important issue to protect ourselves as also the country.

Bibliography or References

1. Fites, P., and M. Kratz. Information Systems Security: A Practitioner's Reference. New York, NY: Van Nostrand Reinhold, 1993
2. Altamonte Springs, FL: The Institute of Internal Auditors, 1991.
3. Ponemon Institute, 2014 Annual Study: U.S. Cost of a Data Breach.
4. Ponemon Institute, 2015 Annual Study: U.S. Cost of a Data Breach.
5. "Mobile Device Security: Threats, Risks, and Actions to Take" (podcast, http://www.cert.org/podcast/show/20100831frederick.html)
6. Data Breach Risk Index: (http://breachlevelindex.com/#!risk-assessment)
7. Data Breach Response Checklist, Privacy Central Assistance Central, (www.ed.gov/ptac)
8. Internet Crime Schemes: Identity Theft (http://www.ic3.gov/crimeschemes.aspx#item-9)
9. Internet Crime Schemes: Phishing/Spoofing (http://www.ic3.gov/crimeschemes.aspx#item-14)
10. "Cyber security for Electronic Devices" (http://www.us-cert.gov/cas/tips/ST05-017.html)