# Relevance of Cyber Security on Data Theft of Clients

Deepa Kini P
Electronics and communication
Assistant Professor
Coorg Institute of Technolgy
Ponnampet, Coorg India

Gurudath Shenoy
Business Administration
Assistant professor
SDM College, Ujire

***Abstract* -In present world confidential information is a very valuable asset for any organization irrespective of its size, strength, expertise, competency etc. An industry normally maintain the data base of its clients, financials, data containing key details, data maintained from its business with its clients over a period of time, such as client location, client business, clients financials (payables and receivables) etc. these data stored as soft copy can be easily copied or hacked by professional hackers. It is very important for everyone to make sure that the data is protected and it does not reach out to the wrong hands. This paper focus on data theft and its impact on clients providing the data.**

***Keywords -- Confidential, Valuable, Financials, Professional and Data theft.***

## I. INTRODUCTION

In this digital age when the data is provided in electronic form or stored in electronic form, it can be easily accessed by system administrators and office employees working for organizations with well access to technology. Many of economics and incidents took place in the past makes it clear that some of the admins and the employees breached their company's data and sold these data's to the hackers or to those who can clearly misuse this data. Some of the data's that are very much confidential and sensitive are breached. These data's of unknown clients (victims) are stolen keeping in view malafide intentions. If data is protected, privacy is maintained separate identities are made it can help the company to protect personal information of millions of customer.

Why data theft takes place? Data is stolen because of malafide intentions. The possible reasons could be the following:

1) To make money by reselling their information to another firm or company.
2) To take out financial confidential and personal information.
3) Political reasons.
4) Disrupt the services and play a game with company.
5) Connection with terror group can also hack secret information which may result in a threat to nation's security.

## II. IMPACT OF DATA THEFT ON CLIENTS

If the nature of data stolen or hacked is pertaining to personal matters, confidential and private matters, financial matters etc. it may have serious implications on the client. The following possibilities are possible:

a) Data may reach unauthorized people who may misuse the same.
b) Can be used to withdraw money from account through unauthorized transactions.
c) Gangsters can have an access to the financial history through which they may plan for kidnapping and extrusion activities.
d) Companies purchase these data from these third parties. These data are further used to call the customers asking for loans, insurance credit cards etc. They may disturb the client in his working hours or the client may end up himself understanding a wrong dial.

## III. IMPACT OF DATA THEFT ON COMPANY

e) Reported incidents taking place relating to data thefts can result in the following:
f) Tarnishing the image of the company and its reputation.
g) Employees of such companies are always looked down as suspicious.
h) Loss of customer trust.
i) Customers demand stronger proof of acknowledgement from their previous experiences, as they will not be in a position to trust company blindly.
j) Company will very soon be out of business and will lose its complete reputation in the market.

## IV. MAJOR CAUSESFOR DATA BREACH

For fraudsters data is an eminent source by the virtue of which they become easily rich, earn millions of money. Data is breached from many sources available within the reach and also from the locations where data is collected from the users and stored for verification purposes. The major causes for data theft can result out of the following:

1) Banks leaving its server unprotected which carry data of millions of customers.
2) Railways where tickets are booked in larger numbers in daily basis.
3) When users purchase Sim cards from service providers they provide personal information through PAN,Adhar etc.
4) When reservation tickets are made for travelling in bus, where a photo id proof is demanded.
5) Banks selling customers credit card and debit card details for a particular price.

6) Data hacked from hackers from health care websites.
7) Hospitals maintaining records of large number of patients in its data base and providing the same on a deal.
8) Temples and other religious places where religious rituals are performed by providing personal details.
9) Hotels, lodges, tourism centers, home stays etc. where a register is maintained completely containing customer data.
10) When we use “Apps” which ask permissions and where we allow such apps to access every information. These apps can reveal locations threatening individual safety.
11) Information that can be easily accessible through unprotected servers. At just dial.
12) Data that is accessible from face book and twitter through any kind of malicious third part apps.
13) Through messages and unauthorized calls asking for personal and financial details, credit card and debit card details.
14) Insurance company employees providing access of high profile clients and recent claim settlements with huge amounts.

## V. POSSIBLE ACYTIONS OF HAKERS FROM DATA THEFT

After clients data is hacked from reputed organizations hackers can come up with the following:

- Hijacking user name and passwords.
- Transfer money unauthorized from your bank accounts.
- Destroy your credit history which can affect CIBIL score.
- Can make unauthorized purchases by misusing your credit cards.
- Obtain cash advances by using your cards.
- Threat to your social security numbers.
- Sell your information to any third parties for a particular price, the information may be used for illegal purposes.

## VI. PREVENTION OF DATA THEFTS

When data’s are provided to the third parties outside it can remain no longer personal or private. It becomes public. When data becomes accessible it can be easily stolen or hacked by professional hackers which results in data theft.

1) Carryout frequent data audit so that you can keep track of all your information.
2) Restricting third parties to access your confidential data by not allowing or providing the same to others.
3) Auditing periodically to ensure that there is no data leakage.
4) For information stored in pc, laptops etc. a stronger passwords should be used for protection purpose.
5) Using encryption and firewall.
6) Restricting moment of information through any modes.
7) Using antivirus software and spywares.
8) Making passwords of all employees strong.
9) Employees to be asked to not to bring personal devices to access company information.
10) Being gentle and maintained o relationship with employees educate them periodically.
11) Update software as soon as options are available for the same.

## VII. CONCLUSION

When it is well known that data itself is one of the key assets of the organization, since client provide the same with a kind of mutual trust with the company. When it is well known that there is a wider presence of hackers prepared for data theft, a common wisdom says that any organizations can face attack at any time if data is not kept confidential. The aim of hackers is to proceed with the activity of data breach, hence it is very important to clearly understand how and why and from who breaches happens, when it is normally expected. If this is well known in advance companies can plan for a better defuse to protect data of company and its clients from getting breached and the image of the company getting tarnished.

## REFERENCE

[1] Andrew Honi “Cyber security” Asia pacific holdings (p-p) (96 – 99) 2017.
[2] Alax Moore “Cyber self-defense” Lyons press (114 - 117) 2014.
[3] David Sutton “Cyber security offences” Asia pacific holdings (p-p) (37 – 43) 2018.
[4] John Smith “Legend cyber security and privacy” Asia pacific holdings (p-p) (80 -86) 2018.
[5] Michal sikorsiki “Practical Malware analysis” No starch press 2012.
[6] Peter W Singer “How to be anonymous online?”Auerbach Publications 2013 (61 – 68).
[7] Wiley “The art of deception” Oxford university press (p-p)(101 – 107) 2011.