”Data Protection Positions In London- An Online Study on Hsbc Bank”

Dr. Varsh s. Sukha deve
Dr. J. Pandu rangarao

1.1 PRELUDE:

In the age of technology information is treated as wealth. Many people are showing interest to have their personal data and trying to share with rest of the people through face book, blogs, and other public networks. As long we use this data for sharing and using for positive purposes no problem to either individuals as well as organizations and for countries. The organizations particularly financial institutions maintain huge amount of data of their customers. For many firms poor data security is currently a serious, widespread and high-impact risk. If any unwanted loss or theft or misplace of the data taken place it may lead to many number of ills. The reasons may be physical, technical or manual the effect may be loss of money or loss of confidence among the customer group[1]. In many number of countries there are laws and principles so as to protect the data, whether it may be a personal data[2] or sensitive personal data[3]. Data loss may be taken place as a category includes gaining unauthorized access and downloading or extracting data stored in computer systems or networks. Such actions may result in civil prosecution. Some times the data loss may be taken place in the form of tampering with computer source code, hacking with an intent to cause damage, and breach of confidentiality and privacy, all of which attract criminal prosecution.

Offences such as misappropriation of property, theft, or criminal breach of trust attract imprisonment and fine under the specified law. Even copying a computer database, or copying and spreading the data base amounts to infringement of copyright for which civil and criminal remedies can be initiated.

In the regime of outsourcing it is a big question to the developed countries to what extent the data is safe and secure. If any specific law failed the companies can approach self regulatory processes such as the BS 7799 and ISO 17799 standards to standardize information security management and to protect it.

……..

(1) Data Security in Financial Services, a report by FSA, 2008.

(2) Personal Data means “Information that relates to a living individual who can be identified from the data or a combination of the data and other material held by the data controller”.

(3) Sensitive Personal Data means “all information relating to an individual’s health, ethnicity, religion or political beliefs. Postnote, Parliamentary Office of Science and Technology, January 2005, Number 235.

Any research work on data protection should be done under three diversified issues. Those are, "privacy rights of interested people in real space and computer generated space", the second one is the "mandate of freedom of information" and third one is "mandates of right to know of people at large". So any law that is pertaining to data protection should primarily reconcile these conflicting interests. So, the data of the individuals and organizations should be protected in such a manner that their privacy rights are not compromised. At the same time right to information and the right to know[1].

Advances in computer technology and telecommunications made every thing possible which is highly impossible in earlier. With a simple click of mouse one can be equipped with lot of information regarding any aspect from the other corners of world. Almost instantaneously, the advancement in technology increased the capacity of every one to store, retrieves, and accesses the lot of data. Information in many databases can be cross checked to estimate the behavior of the people. Particularly governmental and judicial institution goes for this verification and banking and financial institutions have no exception.[1] Major uses of this personal information is direct marketing, telemarketing or any other form of approaching the person. In case of banking sector, they may use this information to know the credit capacity of the borrower.[2]

Uncontrolled sharing of information may increase the number of junk mails in the inbox, some times there are much more serious considerations like: electronic trail by people (hacker) after we use internet, on the basis of the web sites browsed, habits and lifestyles many companies like travelers, marketing companies can create disturbance. Credit card usage can provide indirectly the information like what we bought, quantity, brand, how often we are using card etc., and Employees privacy is under siege, when employers trap the emails of their employees. So, in this digital technology era**, if a person fails to protect what he owns, he owns nothing**.

…….....

(1) Praveen Dalal and Shruti Gupta, "The unexplored dimensions of right to privacy", IJCL, V-III No w, P 45 May 2004.

(2) Britannia encyclopedia and wikipedia

In current world most of the crimes are done by the professional with the advancement of IT and Electronic gadgets. Yearn for information is action as a channel in the growth of cyber crimes. Though this world simplified our life style, there are some anomalies in practice, which resulted in involuntary disclosure of data. It is big headache for the corporate houses, banks and other business and government organizations to protect their data base against the miscreants. So, they need a strong Act or law to get rid of.

One can take following examples in addition to the reasons explained in page two, Para three, that can support the strong requirement of the legal protection to the data.

- Phone call signals may be tacked by the militants to know the movements of police.
- The most dangerous theft of the miscreants is the theft of Source code.
- Unsolicited e-mails are another type of headache.
- Movement across the web can be observed by the placing cookies in order to solicit the tourist packages.
- Through hacking, the hackers can transfer funds from one account to another account.

By keeping in mind the above examples the need for Privacy of the data is not only important to the individuals but also to the governments in order to fulfill the following requirements. Those are:

(1) To have cardinal relations with international countries.
(2) Security of the nation both defiance and public safety.
(3) Identification, investigation, and prevention of crimes.
(4) Internal deliberations of the government.

The need for protection of personal data may come across between patient and doctor in case of health issues, between client and legal advisors in case of trade secrets.

The Data Protection Act (DPA) 1998 is base in UK, in order to processing of data on identifiable living people. It is the main piece of legislation that gives priority for the protection of the personal data. This law was enacted with a view to bring UK law into line with the European Directive of 1995 which required the member states to protect the personal data of the public. Prior to DPA 1998 there are two laws in UK, one is Data Protection Act 1984 and the second one is Access to Personal Files Act 1987. These two were replaced with the new act. With the need and necessity in the computer era, a new act was made in the year 2003 that is "The Privacy and Electronic Communications (EC Directive) Regulations 2003. This act

emphasized the importance of the consent requirement for most electronic marketing to "positive consent such as opt in box.

The DPA act 1998 defines eight data protection principles. Those are:

1. **Fairly and lawfully** only the personal data can be processed. In particular, the data shall not be process unless – at least one of the conditions in Schedule 2 is met, and in case of Sensitive Personal Data, at least one condition in Schedule 3[1]
2. Once the data is collected for lawful purpose, it cannot be used other than that purpose.
3. Collecting the data over than the required also offence as per DPA 1998.
4. The personal data should be maintained accurately, and up to data.
5. The data collected for one particular purpose can not be hold longer time than the required.
6. This principle deals with the rights of the individuals.
7. In order to protect the data appropriate technical and organizational measures should be taken to prevent damage and unlawful usage of the collected data.
8. Personal data could not be transfer to any foreign countries which are not aware of the data protection acts, and where there is no guarantee for the processed data.

(3) The data also covers the personal information of living individuals including their name, date of birth, anniversary dates, addresses, telephone numbers, email id etc., As per this act the people or organizations that are maintaining the personal data should register their names with **Information Commissioner**, which is formed as per law and which has been appointed as the government official to oversee the Act. This Act put restrictions on the collection of the data, it also take care for which the data was collected.

……

*(1) The meaning of words **fairly and lawfully** means, the fairly processed would fulfill at least one of the following six conditions.*

1) *Owner of the data (Subject) should give consent.*
2) *Processing is essential for making contract.*
3) *Where processing is required as per law.*
4) *To protect the vital interest of the subject.*
5) *In order to carryout any public interest and*
6) *Processing is necessary in order to pursue the legitimate interests of the third party.*

There are high profile incidents of data loss in public and private sectors. A bird view eye on this issue can give knowledge to public regarding how the data may be stolen or lost and that can be used for crimes like **identity fraud.** Any one committed for getting data protection wrong can bring commercial, reputation, regulatory and legal penalties. The interest of the organizations towards data protection can bring rewards in terms of customer trust and confidence.

HOW LOST DATA IS USED FOR IDENTITY FRAUD:

One cannot conclude that all data losses may not for misuse or Identity fraud or black mailing; in case of physical losses i.e. loss of Laptop, Hard disk, CDs, may be because of the cost of those devises. But in most of the cases the data loss creates serious problems particularly in case of highly confidential information such as national insurance numbers, payment card and banking information. According to the Serious Organized Crime Agency (SOCA)'s Threat Assessment report 2006/07 the frauds include false credit applications, fraudulent insurance claims, fraudulent transaction, some times complete account takeover by making the customers victims.

As per PriceWaterhouse Coopers, the data stolen may be sold freely in social settings such as pubs and clubs and subsequently trades through underground networks by force them to participate in illegal activities for instance teenage pornography. Data loss is not only inconvenient to the customers but also create serious and critical problems such as drug trafficking, human trafficking and terrorism. Some times the hackers or thieves may create inconvenience to the firms and which required 2 or more days to make things right.

HISTORY:

The world's first computer specific statue was enacted in German state of Hesse, in the year 1970 in the form of Data Protection Act. The misuse of records under the Nazi regime had demanded the use of computers and storage of the data in computers. Sweden is the first nation that introduced the first national statue in 1973.

……

(1) www.soca.org
(2) Pricewaterhouse Coopers report, 2007.

In 1995 the European Union adopted it Directive (95/46/EC) of the European Parliament and of the Council of 24 October 1995 on the maintenance and free flow of the personal data. Even EU countries won't send the data to the countries that are not meet the EU requirement of "adequacy standards" as per (Art 25(6)) [1]. USA in order to meet this specific requirement they prepared a list of companies that are able to meet the "adequacy" in the name of "Safe Harbor". Along with USA other members like Hungary, Switzerland, Canada, and Argentina also came under the policy of "Safe Harbor" scheme.

As per Financial Crime and Intelligence Division (FCID) in 2007 only nearly 56 cases of data loss by financial services firms were recorded. It is also evident that many a number of cases are not recorded yet. No one in the UK can be ignorant of the potential harm of data loss following several well published incidents. These included:

1) Two CDs holding data on all recipients of child benefit lost in transit from **HM Revenue & Customs**.
2) A laptop containing a large amount of customer data stolen from a member of **Nationwide Building Society Staff;**
3) The British financial watch dog has fined the bank under study **HSBC**, around $5 million for failing to protect customers' data. The fine details are as follows: HSBC Life fined with 1,610,000 euros in 2008 as it lost an unencrypted CD containing the details of 180,000 policy holders in the post. HSBC Actuaries fined with 875,000 euros in 2007 as it lost an unencrypted floppy disk in the post containing the details of 1,917 pension numbers. And HSBC Insurance Brokers fined with 700,000 euros for their loss of data.
4) The HSBC banking group has admitted losing a computer disc with the details of 370,000 customers, in post in Southampton town.
5) New York based Citibank accounts being looted from a BPO in Pune, India.
6) A call center employee in Bangalore, India Peddling credit card information to fraudsters who stole US$398,000 from British bank accounts.
7) UK's Channel 4 TV station ran broadcast footage of a sting operation exposing middlemen hawking the financial data of 200,000 UK citizens.
8) The Information Commissioner's Office's Public Censure of many firms found to be disposing of customer data carelessly.

1.2 CHALLENGES TO DATA PROTECTION:

A detailed investigation was made by Douwe Korff et all[2] with a view to identify the challenges to protect the personal data in the current social and technical phenomena viz., internet, globalization, the increasing interest to have more personal data, increasing power of computers, biometrics, RFID makers etc., and increased dataveillance.

1) Advancements in technology are the major technical challenge.
2) Even governments also sharing more information regarding their citizens particularly for the fear of bomb attacks by terrorists.

3) Technical developments influencing the technical and social trends of the day. International terrorism, teenage pornography and serious international organized crimes are one side of the coin; the other side is that the state is thinking to promote good behavior to the citizens. They also using this technology to fight against teenage pregnancy, obesity etc., they are also using to share their latest e-government system etc. Some portals are sharing information regarding tax returns, safety against social ills etc.
4) France, US, Canada, Germany and UK promoted Electronic Patient Records (EPRs), digital version of medical records so as to maintain accurate data regarding the patients.
5) Major part of the business is E-business, best example for this is Amazon,
6) "Web 2.0" provided facility to upload photos and videos in blogs, You Tubes. My face, face book and Flickr all these are questioning the strengths of Data Protection Acts. To avoid misuse of finger prints and eye race copying in air ports E-passports are implemented.

……

(1) Art 29 of Data Protection Act, [OJ L 184, 17-7-1999, P23 et seq.]

(2) Prof. Douwe Korff of London Metropolitan University, and Dri. Ian Brown of the Oxford Internet Institute of Oxford University, et., al., European Commission – Directorate – General for Justice, Freedom and Security (DG JFS) "New challenges to data protection".

1.3 NEED OF THE STUDY:

This report explains the importance of data protection particularly in financial services in the UK and what precautions are going to be taken by the financial firms. It is on the part of government so as to create market confidence among the customers while utilizing banking services. It is also important to create awareness among the citizens regarding the data protection and impact of the same in case of poor maintenance. The reduction of **financial crime** [1] needs high attention of the House of the Lords to protect the customers.

With the above opening remarks it is evident that economic position of the firm is based on the development of banking and banking services. The strength of the banking operations are based on the customer data and security provided to that data. Misuse of the customer data costs much both to the bank, [banking industry] and customers. Banks are also gathering much personal data form the customers for many reasons like Know Your Customer **(KYC)**. At the same time banks should consider the Treating Customers Fairly **(TCF)**. Hence it is the time to debate on the issue of Data Protection. Here an attempt was made by the researcher to through the light on the Data Protection Acts in UK and their protection in safekeeping the data of the selected bank customers.

1.4 OBJECTIVES OF THE STUDY:

The main objective of the study is to examine the data protection capacity of the selected bank under study in UK. The study attempts to identify the problems and suggest measures for the improvement in safekeeping of customer's data. More specifically, the objectives of the study are:

(1) To present an overview of data protection in UK and role of banking sector in promotion of economic development.

……

(1) Financial Crime includes money laundering, market abuse and fraud or other dishonest practices.

(2) To review the main reasons for data loss.

(3) To give an idea on impact of data loss to customers, firms, and to all stakeholders.

(4) To know the perception of the bank customers regarding procedure of the data maintenance and the laws or Acts of data protection.

(5) The study also aimed at opinion of the specific bank customers towards the data maintenance capacity of the HSBC bank.

(6) To suggest measures to improve the data protection measures by the selected bank while rendering services to the public.

1.5 RESEARCH METHODOLOGY:

DATA SOURCES AND METHODOLOGY:

The data required for the analysis of data protection position of UK banks, the researcher had collected information both from primary data and secondary data. The term 'Primary Data' means the information collected for the purpose of particular research work under study. On the other hand 'Secondary Data' means the information collected other than the specific work under study. The basic method adopted by the researcher to get needed information is sample method which is collected randomly from the total population.

Collection of Primary Data and used Techniques:

For the purpose of collected primary data from various levels of employees who are working in Nisa Today's organization, schedules have been designed and executed among the respondents. The observation method has been used in few cases to cross check the information collected through questionnaire method. To have clear information and understanding many a time the researcher has short interviews with the respondents.

Collection of Secondary Data:

The secondary sources of the data are collected from the published reports of the bank under study. The annual reports of the bank and legal evidences along with audited accounts

were thoroughly reviewed and collected the data required. The web sites of the selected bank and other legal bodies also helped in this regard.

SAMPLE DESIGN:

For the purpose of the study, a group of people were selected from the town of London on random basis. The study is based on the opinions of 200 respondents who are working in Nisa Today's organization. Out of 200, 100 members were selected from administration department and 50 members from managerial wing and remaining 50 are supporting staff. For all these respondents a structured questionnaire was served. (*See appendix 1 for model structure questionnaire.)*

The important characteristics of the sample respondents presented in Table – 1.1

Table – 1.1

Sl.NO.	Variable	No. of respondents	Percentage
1	Administrative Department	100	50
2	Managerial Staff	50	25
3	Supporting Staff	50	25
	Total	200	100

Statistical techniques used for analysis of the data:

The collected data was processed, tabulated and analyzed in a systematic manner and for the data analysis various statistical tools have been used such as averages, percentage, growth rates, trend analysis, standard deviation and regression and diagrams. For measuring the satisfaction of the bank customers Likert type a four point scale with the rating of 'strongly disagree', disagree', 'agree', and strongly agree was used. The detailed methodology and scales that are used to quantify the qualitative data is explained at relevant places.

REVIEW OF LITERATURE:

In 2007, Financial Crime and Intelligence Division (FCID) conducted a survey on 56 small, medium and large companies with the approval of House of Lords Selected Committee on Science and Technology in December 2006. They had given their findings and suggestions in

the form of do's and don'ts in the area of governance, training and awareness programmes to the employees, staff recruitment process, various controls like password, eye race scanning, physical security and disposal of customer data.

Praveen Dalal conducted a study on "Data Protection Law in India: A constitutional perspective. This study emphasized how Indian law can act in three different situations such as Right To Information (U/A 19(1)(a), Right To Privacy (article 17) and Right To Know U/A 21**.**

Majmudar & Co international Lawyers explained how BPO companies are abides by the BS 7799, ISO 17799 standards in managing the data of international clients. As per this study Tier I BPO companies have certifications of Sarbanes Oxley Act, the Safe Harbor Act, the Gramm Leach Bliley Act for financial services, the Fair Debt Collection Practices Act for banking.

European Commission, Directorate General Justice, Freedom and Security also conducted a comparative study on Different approaches to new privacy challenges, in particular in the light of technological developments and submitted their final report on 20th January, 2010. The study aimed at identification of challenges for the protection of personal data produced by current social and technical phenomena such as internet, globalization, CCTVs, Social networks etc.,

Data Protection Commissioner submitted a report on Data Protection Guidelines on Research in the Health Sector in 2007. The document aimed at to strike an appropriate balance between the patient's right to personal data privacy and the making data for research. As per this report, without the consent of the subject even researchers cannot use that data for any purpose, unless other wise there is a benefit to society or intervention of the Law.

Center for Digital Strategies (CDS) at Dartmouth College, New Hampshire, examined in 2007 the accidental loss of data through peer-to- peer file sharing networks at a group of large financial firms. Sensitive data with full information was shared when ever people search for songs with the name of companies.

University of Namur, CRID submitted a repot on Personal Data protection Law in India, in the year 2005 with the objective of delivery of good level of compliance, support to individual data subjects and provision of appropriate redress to the injured parties.

Now in world particularly in UK Data Protection is a hot topic among the professional groups and associations viz., Jericho Forum, the British Bankers Association, APACS, CIFAS, the Information Risk Executive Council, the Security Institute, the North East Fraud Forum and the Information Systems Audit and Control Association. Time to time all these associations and professional bodies are conducting many studies on data protection.

1.5 SCOPE OF THE STUDY:

. Though the study aims at examining Data Protection Acts and their role in promoting and protecting the account and financial information of the bank customers, an in-depth analysis is restricted to only one bank viz., HSBC. This study also emphasis the principles or norms to be followed by the organization so as to protect the interests of the customers. This study is going to be giving an idea on principles that are essential to the organization.

PRINCIPLE 1: The firm must conduct its business with due skill, care and diligence' and principle.

PRINCIPLE 2: The firm must take reasonable care to organize and control its affairs responsibly and effectively, with adequate risk management systems.

PRINCIPLE 3: The firms must be confined to the required standards and should take reasonable care to establish and maintain effective systems and controls.[1]

The researcher interviewed personally all important roles, who are related to the information security, fraud, staff vetting, IT operations, Compliance and internal audit. Much information was obtained for the clear understanding of the attitude of the organization in the subject matter data protection.

……

(1) Rule 3.2.6R in our Senior Management Arrangements, Systems and Controls sourcebook (SYCE).

DATA ANALYSIS AND INTERPRETATION

21st century themes for regulating the privacy and integrity of personal information must involve greater emphasis on trust, confidence, governance, transparency, and accountability. For all corporate firms and government bodies privacy and safeguarding become major reputation issues. Europe has a long and proud history of data protection standards and legislation. All these are implemented and followed by the rest of the world. European Data Protection Commissioners are committed to provide leadership for the future. Still these Commissioners give priority to promote fundamental rights and freedoms, encourage the firms to follow best practices including privacy by design.

This chapter which proposes to present the opinions of Nisa Today's employees with an evaluation, attempts to examine the opinion on the data protection abilities of the HSBC bank. The very objective of this chapter is to examine whether the organizations are taking seriously the concept of data protection or not. It is also proposed to present the views of the concerned on the subject cited. All these analysis is expected to project the effectiveness of the data protection policy in the sample unit. In this chapter each question was explained with the support of the statistical data so as to find out the opinions of the respondents towards the HSBC and to provide suitable interpretations of the researcher a long with graphical representations.

3.1 AGE WISE DISTRIBUTION OF THE RESPONDENTS

TABLE NO. 1

	No. of respondents	**Percentage**
20-30 years	45	23
30-40 years	75	37
40-50 years	54	27
Above 50 years	26	13
Total	200	100

INTERPRETATION:

Most of the respondents are belonging to the age group of 30-40 years and they are very much familiar with the history of the HSBC bank. The researcher tried to identify the differences in perceptions of the respondents on the basis of their age. The respondents above the age group constituted only 13 percentage of the total sample.

3.2. . EDUCATION QUALIFICATIONS OF THE RESPONDENTS? :

TABLE NO.2

	No. of respondents	**Percentage**
Intermediate	24	12
Graduation	96	48
Post Graduation	50	25
Professional	30	15
Total	200	100

INTERPRETATION:

Most of the respondents are graduates and who are working in administrative department of the organization. This percentage also includes the respondents who are working as managerial and supporting staff. The next highest community came with the qualification of Post Graduation. The researcher also tried to identify the differences in the understanding levels of the respondents in data protection need, importance, policies, laws and systems. Until they get any personal loss no one is bother about the data protection policy of the bank in which they have account.

3.3. ANNUAL INCOME LEVEL OF THE RESPONDENTS:

TABLE NO.3

	No. of respondents	**Percentage**
Less than 10 million Euros	104	52
10- 20 million	54	27
20-30 million	26	13
30 and above million	16	08
Total	200	100

INTERPRETATION:

Respondents are also categorized on the basis on their income level. As per the Data Security in Financial Services a study report by (FSA) most of the organizations have some kind of attitude. In their opinion fraudsters may aim at only the data of large companies and also on the high net worth people. In this study the researcher also tried to analyze the opinion of the people on the basis of their income level. Most of the selected sample members belong to below 10 million euros and very less respondents came in to the category of above 30 million income. Irrespective of their income levels every one who participated in the survey expressed confidence regarding the financial services offered the HSBC bank.

3.4. THE FREQUENT USAGE OF THE BANK SERVICES:

TABLE NO.4

	No. of respondents	**Percentage**
Daily	26	13
Fortnightly	84	42
Monthly	69	35
Rarely	21	10
Total	200	100

INTERPRETATION:

Number of times the banking services used by the respondent also influences his/her decision regarding the opinion of the quality of the banking services by the particular bank. In this survey 42 percentages of the respondents are using this bank services once in a 15 days. Most of the respondents i.e. 35 percentages of the respondents are using banking services once in a month. Even though there is information regarding data loss in HSBC they expressed their confidence.

3.5 AWARENESS AMONG THE RESPONDENTS TOWARDS DATA PROTECTION METHODS/TECHNIQUES?

TABLE NO.5

OPENION	MANAGERIAL	ADMINISTRATIVE STAFF	SUPPORTING STAFF	TOTAL
YES	12 (80)	16(64)	90 (51)	122 (61)
NO	03 (20)	09(36)	70 (49)	78(39)
TOTAL	15 (100)	25 (100)	160 (100)	200 (100)

- The figures in the bracket show the percentage.

INTERPRETATION:

Whenever, the researcher posed the question that whether they are aware of the data protection techniques or methods? Those are followed by the HSBC bank. Actually 80 percent of the managerial staff is aware of the need of data protection and the capacity of the study bank (HSBC) in protecting its customers. 64 percent of the administrative are aware of the data protection need and methods, and 36 percent said no idea. While coming to the major group supporting staff nearly 50 percent of the respondents have knowledge in data protection methods and techniques and remaining half of the people are poor in data protection knowledge. However out of total 200 sample respondents 61 percent of the respondents have broad idea on data protection methods and techniques. Even though the customer is aware of the data protection methods or not, it is the responsibility of the firm to protect their personal data form unwanted users.

3.6 WHAT ARE THE MAIN CAUSES FOR DATA LOSS?

TABLE NO. 6

Reason for data loss	**No. of respondents**	**Percentage**
Low preference to customers data by the organizations	10	05
Low Technology and poor electronic gadgets of the firm.	08	04
Poor data protection methods	18	09
Poorly trained HR	54	27
Poor organizational policies and senior managers attitude	22	11
Poor risk assessment	25	13
Poor appreciation on the gravity of the risk	05	02
Less punishments and loopholes in Laws	38	19
Third party negligence	20	10
Total	200	100

This question is supposed to pose to the bank employees; strictly speaking the respondents are not fully aware of the reason for the data loss in banks. However the respondents replied to this question as per their past experience and also based on the news regarding the data loss in various companies. So, the responses of the respondents may not be fully relating to the bank under study.

Most of the respondents 27 percent are opinioned that inability of the HR is the main reason for data loss. They also showed their dissatisfaction on the existing Laws and Acts that are punishing the fraudsters. Still there is no control or punishment towards hackers. Tracing out of hackers also required much technical knowledge to the staff of the bank. Poor risk assessment and third party negligence is the next reasons for the data loss as per the respondents.

3.7. DO YOU KNOW THE LAWS / ACTS THAT ARE APPLICABLE IN CASE OF ABUSE OF YOUR FINANCIAL DATA BY ANY THIRD PARTY?

If your answer is 'YES' please specify the name of the Act / Law

TABLE NO.7

	No. of respondents	**Percentage**
YES	128	64
NO	72	36
Total	200	100

INTERPRETATION:

Even though in UK Data Protection Act 1998, Serious Organized Crime Agency (SOCA), CIFAS – The UK'S Fraud Prevention Agency, Financial Crime and Intelligence Division (FCID) and many more are working to prevent and regulate the data theft. These Acts and Laws have been updated from time to time. The researcher came to know that still in UK many number of people are not aware of the Acts that are applicable in case of data misplace. 64 percent of the total respondents are familiar with the data protection Acts and rest of the 36 percent are not known about the serious working nature of the Laws. They also view this data theft along with other frauds and crimes. Most of the respondents who responded to the above question with the answer 'YES', named the DPA-1998.

3.8 ANY TIME HAVE YOU FACED THE PROBLEM OF LOOSING YOUR PERSONAL DATA?

TABLE NO.8

	No. of respondents	**Percentage**
YES	24	12
NO	176	88
Total	**200**	**100**

INTERPRETATION:

As per the latest news even the bank under study also the victim of data loss by the third party. The detailed information is available in the chapter one under the heading 1.3. As per the survey conducted by the researcher it is highlighted that very less people i.e. 12 percent only the victims of the data loss and 88 percent are safe zone. Still the respondents expressed confidence and faith on the bank under study.

3.9 HAVE YOU SATISFIED WITH THE ROLE OF FINANCIAL SERVICES AUTHORITY (FSA) IN DATA PROTECTION AND DATA SECURITY?

TABLE NO.9

	No. of respondents	**Percentage**
YES	74	37
NO	126	63
Total	**200**	**100**

INTERPRETATION:

Financial Services Authority conducted a survey on Data Security in Financial Services. The main aim of this FSA is to prevent the loss of the customer data particularly in the area of Financial Institutions. As a Self Regulatory Authority FSA can conduct surveys and it also create awareness among the public regarding importance of the data, precautions while providing the data to the third party and while sharing the information in social networks. Out of total number of respondents 126 numbers said the role of FSA is limited in prevention of the data frauds. A strong legal body only can punish the criminals with power and authority. They also gave support to make the FSA strong. Still 37 percent of the respondents expressed their positive opinion on the working of the FSA.

3.10 HAVE YOU SATISFIED WITH THE LAWS THAT ARE AVAILABLE IN CASE OF THEFT OF PERSONAL DATA?

TABLE NO.10

	No. of respondents	**Percentage**
Satisfied	74	37
unsatisfied	26	13
No Idea	100	50
Total	**200**	**100**

INTERPRETATION:

The scope of this question is very less, why because out of total 200 respondents: only 12 percent of the respondents faced the problem of data loss. Whenever the researcher asked this question rest of the respondents expressed their opinion as 'no idea'. Most of the respondents i.e. 50 percent said that they have no idea regarding the working nature of the protecting Acts. 37 percent of the respondents are satisfied with the working nature of the existing Acts and Laws. Very less percent 13 expressed their opinion as unsatisfied.

3.11 HOW FREQUENTLY THE DATA IS GOING TO BE MISUSED BY HACKERS IN HSBC?

TABLE NO.11

	No. of respondents	**Percentage**
Once	18	09
Rarely	36	18
Frequently	24	12
Not at all	122	61
Total	**200**	**100**

INTERPRETATION:

The opinion of the respondents is based on their past experience or the data available in news papers or word of mouth. The response of the respondents to this question is relevant to the actual situation. 61 percent of the respondents said loss of data may be taken place not at all in the bank under study. Next to the above 18 percent of the respondents are opinioned that rarely this kind of loss may be occurred to their personal data. One cannot predict how many times the data may be lost by the organization. But it is on the part of the organization, so as to prevent or eradicate the sources of data loss. The organization also has the responsibility to fill the respondents with satisfaction.

3. 12. WHAT MAY BE THE LEVEL OF LOSS OF MISUSE OF THE FINANCIAL DATA?

TABLE NO.12

	No. of respondents	**Percentage**
In thousands	126	63
In lakhs	65	33
In millions	09	04
Total	**200**	**100**

INTERPRETATION:

Still there is opinion that many times misplace of the data may not for identity fraud. Some time it may happen by the knowledgeable IT professionals for making fun or to show their technical knowledge. The data loss may also occur due to poor technical power of the organization. The data loss means not only by the hackers but also by the third party. . In many cases the loss of the data is only by third party for example post offices, or courier staff. It is also evident in many previous research reports the data loss may occur because of the physical devices like USB ports, CDs, Floppy, Laptops etc., in these instances the main reason for the data theft is not for the information what it contains only for the cost of the device. So if it is the case the loss of the data is almost negligible. If the data is stolen by any one who is the part of the organization, then the loss may be in thousands or in millions. As per the opinions of the respondents the expected loss of the data misplace is in thousands to the organization and to the individuals.

3. 13. WHAT IS THE REACTION AND REMEDIAL ACTIONS OF THE BANKING AUTHORITY AGAINST YOUR COMPLAINT?

TABLE NO.13

	No. of respondents	**Percentage**
They are co-operative	76	38
They are neutral	26	13
Immediate action	98	49
Total	**200**	**100**

INTERPRETATION:

In many of the complaints regarding the data protection is due to low technical knowledge of the working staff or negligence of the staff while transferring data from one place to another place, low preference to the personal data of the customers, lack of proper policies and bad attitude of the senior level managers towards the data of the customers. Data loss may be happened either from out of the organization or inside of the organization. But while the problem occurred to the customers the response of the bank staff plays an important role. The bank staff must be in a position to supply the required information to the customers directly or indirectly. As per the study it came to the lime light that the staff members of the HSBC are taking initiative and adopting immediate remedial actions to retrieve the lost data. Their response to the queries of the customers is very responsible and 38 percent of the bank staff are very co-operative and maintain stability while giving response to the employees. Only 13 percent of the staff members are neutral in these situations.

3. 14. WHEN COMPARE WITH OTHER BANKS WHAT RANK YOU CAN GIVE TO YOUR BANK HSBC IN DATA PROTECTION ACTIVITY?

TABLE NO.14

Rank	**No. of respondents**	**Percentage**
1	80	40
2	96	48
Unable to compare	24	12
Total	**200**	**100**

INTERPRETATION:

The rating of any organization based on their satisfied customer opinions is influenced not only by the concept on which the researcher is trying to get answer but also other factors like past services of the bank, behavior of the staff members, quality of the services, cost of the services and other relevant and irrelevant reasons. As per the questionnaire survey conducted by the researcher 40 percent of the respondents had given Rank 1 to the HSBC towards the data protection. Where as 12 percent of the respondents said their inability to classify the banks on the basis of their data protection abilities. But 96 number of the respondents are given 2nd rank to the HSBC in UK.

3. 15. HAVE YOU TAKEN DECISION ANY TIME TO CHANGE THE BANK DUE TO POOR DATA PROTECTION METHOD?

TABLE NO.15

OPINION	No. of respondents	Percentage
YES	06	03
NO	98	49
Not at all	96	48
Total	**200**	**100**

INTERPRETATION:

A single event cannot change the opinion of the customer either to shift from the current organization or to discontinue taking services from that firm. The confidence or trust builds on series of incidents. It is also evident in this research that only three percent of the respondents showed interest to discontinue from the HSBC, whereas 49 percent said they have no such kind of idea. Apart from the above two options, the researcher also tried to know the strong decision of the respondents towards the bank under study. 48 percent of the respondents said what ever may be the problem they are not in a position to change the current organization. They continue in the same organization forever.

3.16 DO YOU KNOW THAT HSBC WAS FINED BY FINANCIAL SERVICES AUTHORITY (FSA)?

TABLE NO.16

OPINION	No. of respondents	Percentage
YES	98	49
NO	102	51
Total	**200**	**100**

INTERPRETATION:

Actually this question was posed to the respondents with a view to know how the customers are trying to know the happenings in their banks. In contrary to this all banks follow Know Your Customer, (KYC) here the researcher tried to know the observation of the customers towards their banks. 49 percent of the respondents said they know the news of data loss in HSBC, where as the equal percent of the respondents said they have no interest to know much regarding their bank.

Finally an open-ended question was posed to the respondents to offer their valuable suggestions for the better data protection in financial institutions. Most of the respondents had given their suggestions to reduce the third party involvement in data handling. Some respondents wrote with their own hands to provide good training to the HR of the bank. Some respondents pointed out the ethical and responsive behavior of the staff. Many respondents emphasized the importance of the senior level managers in the data protection.

FINDINGS AND SUGGESTIONS

FINDINGS:

1. Most of the respondents belong to the age group of 30-40 years. Generally people under this age bracket are risk takers. They also show interest to know much about the issues through internet, BBC or any other mode of communication.
2. As in the sample itself many of the respondents comprised from supporting staff, and the education qualification of the major respondents are graduation.
3. Income wise distribution of the customers was also done so as to understand their opinions or preferences. Sometimes the level of income also changes the attitude of the respondents.
4. From this survey another important finding was that many of the respondents are utilizing the banking services once in a fortnight or twice in a month.
5. Actually 80 percent of the managerial staff is aware of the need of data protection and the capacity of the study bank (HSBC) in protecting its customer's data. 64 percent of the administrative staff is aware of the data protection need and methods, and 36 percent said 'no idea'. While coming to the major group of supporting staff nearly 50 percent of the respondents have knowledge in data protection methods and techniques and remaining half of the people are poor in data protection knowledge.
6. While coming to the reasons for data loss, most of the respondents i.e. 27 percent are opinioned that inability of the HR is the main reason for data loss. They also showed their dissatisfaction on the existing Laws and Acts that are punishing the fraudsters.

7. The knowledge of the respondents towards data protection acts is as follows: 64 percent of the total respondents are familiar with the data protection Acts and rest of the 36 percent are not known about the serious working nature of the Laws.
8. Most of the respondents i.e. 50 percent said that they have no idea regarding the working nature of the protecting Acts. 37 percent of the respondents are satisfied with the working nature of the existing Acts and Laws. Very less percent 13 expressed their opinion as unsatisfied.
9. Most of the respondents are expressed their opinion that the staff members are very responsive towards the complaints of the customers.
10. Majority of the respondents (48%) had given second rank to HSBC, where (40%) had given 1st rank to the data protection procedure in the bank under study.
11. No customer shows interest to shift from current bank to any other bank due to their data protection method.

SUGGESTIONS:

1. In all organizations, the customer's data should be maintained at two levels. One is primary level; this data can be used by junior level officers and freely accessible to any needy one. The second level is most important level; this data can be used with the prior permission of senior level or accessible with any password.

2 It is also advisable to the firm not to give any maintenance of their own customers data to any third party.

3. Before transforming data from one place to another place through any electronic devices such as USB ports, CDs, Floppies, Laptops etc., the firms should ensure that the device is encrypted and the mode of transport is safe and secure.

4. Internal and external auditors should have an idea on data security and they should give proper suggestions for safekeeping of the data.

5. It is also suggested to all firms whether it is a financial or non-financial they should obtain Protective Registration from (CIFAS).

6. It is also advisable to the corporate offices that many of them have different attitude towards the data of their customers for instance, the data is limited and piecemeal, and hoaxer may concentrate only on high net worth people, only large firms may be targeted, and over confidence on working employees; so they should avoid this kind of attitude.
7. Organizations should adopt more improved systems and controls so as to protect the data of the customers.
8. Data protection is not only the duty of IT people but also the responsibility of all people in the organization. So, everyone should feel responsible and show their corporate governance while protecting the data of their customers.
9. Companies should be proactive not reactive in this issues, why because the risk of data loss is much in terms of money, time and customer satisfaction.
10. Customers are also advised to maintain proper secrecy to their personal data, instead of sharing with unknown people in social sites.

CONCLUSION:

In olden day's data or information sharing almost impossible, unless other wise one has to move from his place to particular place to refer books in limited number of libraries. With the invention of computer by Charles Babbage, and advancements in Telecommunications made the person equipped with lot of pages of information with a simple click of mouse. Many search engines like Google are famous to deliver the required data for the netizens. It is also on the part of the people not to misuse the available information for any illegal purpose. Sharing of data can increase the knowledge of many number of people like students, unemployed, small organizations etc., So while using any data some ethical norms should be followed by individuals.

BIBLIOGRAPHY:

1. www.soca.org (Serous organized Crime Agency)
2. www.ICO.org (Information Commissioners Office)
3. Law enforcement directory
4. annual reports of trade associates
5. forensic accountants
6. www.cifas.org.uk (The UK's Fraud Prevention Agency)
7. BBC Watch dog
8. www.financial risk outlook
9. www.fcid.com (Financial Crime and Intelligence Division)
10. Financial risk outlook 2008.

Appendix – 2

QUESTIONNAIRE
ON
DATA PROTECTION ACT IN INDIA & UK

Dear Bank Customer,

I am pursuing Ph.D. from LONDON University on the topic of above mentioned. I shall be obliged if you kindly provide the information on various questions in "questionnaire". It is assured that the information provided by you will be used only for research purpose and will be kept confidential. It is your kind co-operation that will help me to achieve proper results in this field.

Thanking you Sir, with regards,
Kaleem

A. PROFILE RELATED QUESTIONS:

1. Name : Mr./Mrs./Miss.....
2. Place : .....
3. Age : .....years.....months
4. Education :
   a) Schooling ( ) b) +2 ( )
   c) Graduation ( ) c) Post Graduation ( )
   d) Other (please specify) …….

5. Annual Income Level
   a) Less than 10 million Euros ( ) b) 10 to 20 Millions ( )

c) 20 to 30 Millions ( ) d) 30 & above ( )

6. What frequently you are using bank services:
a) Daily b) Fortnightly c) Monthly d) Rarely

7 Do you have any idea regarding Data protection?
a) YES b) NO

8 In your opinion what is the reason for data loss?
a) Low preference to customers data by the organizations ( )
b) Low Technology and poor electronic gadgets of the firm. ( )
c) Poor data protection methods ( )
d) Poorly trained HR ( )
e) Poor organizational policies and senior managers attitude ( )
f) Poor risk assessment ( )
g) Poor appreciation on the gravity of the risk ( )
h) Less punishments and loopholes in Laws ( )
i) Third party negligence ( )

9. Do you know the Laws / Acts that are applicable in case of abuse of your financial data by any third party?
a) YES b) NO
If your answer is 'YES' please specify the name of the Act / Law

10 Any time have you faced the problem of loosing your personal data?
a) YES b) NO
If your answer is YES please explain the incident……

11. Have you satisfied with the role of Financial Services Authority (FSA) in data Protection and data security?

a) YES b) NO

12. Have you satisfied with the laws that are available in case of theft of personal Data?
a) Satisfied b) Unsatisfied c) No Idea

13. How frequently the data is going to be misused by hackers?
a) Once only b) Rarely c) Frequently d) Not at all

14. What is the level of loss of misuse of the financial data?
a) In thousands b) In Lakhs c) In millions

15. What is the reaction and remedial actions of the banking authority against your complaint?
    a) They are co-operative b) They are neutral c) Immediate action

16. When compare with other banks what rank you can give to your bank HSBC in data protection activity?
    a) One b) Two c) Unable to compare

17. Have you taken decision any time to change the bank due to poor data protection method?
    a) YES b) NO c) Not at all

18. Do you know that HSBC was fined by Financial Services Authority (FSA)?

    a) YES b) NO IDEA

19. Give your suggestions for better protection of the customer's data?

    ……
    ……

Thank you very much!

DR. VARSHA S. SUKHADEVE
M.Com, MBA, MA, M.Sw, B.L, NET, Ph.D
Prof. Smt L.R.T. College of Commerce,
AKOLA, MS
Varsha_72@rediffmail.com

DR. J. PANDU RANGARAO.
MBA, Ph.D
Prof. RISE GROUPS OF INSTITUTIONS:: ONGOLE
VALLLURU – 534272, AP
jettirangarao@rediffmail.com
09441069978