4. ANALYSIS OF CHALLENGES OF TECHNOLOGICAL DISASTERS

Hardware & Software Related
Networking Related
Human behavior Related
Natural Disasters

4.1 Technology in Banks and Disaster (Banking in Today’s world)

Banking in today’s world is completely IT-based. IT is the backbone of banking sector. These days nobody goes to bank branch for carrying out transactions as all the banking activities are done online today. Be it payment transaction or retrieval transactions. But as people say ‘every good thing comes with some drawbacks’, IT also has its limitations which every bank have come across and has to overcome to maintain consistency and efficiency in day to day activities.

These limitations can be related to IT applications, Intranet, Treasury Application, ATM Application, EFT, RTGS, Communication Protocol(like TCP/IP) Database, Data Warehousing, Data Mining and System Failures.

Banking IT system has gone far away to overcome the above limitations. But as new technologies are coming to the market and are adopted and applied by the banks more and more, challenges have been faced by them. These challenges can be related to Hardware used in banks like Computers, Servers, CPU etc. Software in banks like Banking application, System software etc. Network to which banks are connected like Intranet. Employee Ignorance in banks like error in typing, error in transaction. Natural Disasters like flood, drought, wind, wing storm, Tsumani, Earthquake, Snow storm.
4.2 Technological Crisis

The term “crisis” is typically used as a catch-all concept, which encompasses all types of “un-ness” events. In this rather general perspective, the term “crisis” applies to situations that are unwanted, unexpected, unprecedented, and almost unmanageable, causing widespread disbelief and uncertainty. *Crises cannot be explained by listing a few easily recognizable factors.*

The research on causes of crises has become an interdisciplinary effort, paving the way for a multi-level approach that allows us to analyze the origins of any given crisis. At the micro level, such an approach would focus on the role of individuals. In most, if not all crises, human errors are found at the roots of the crisis. Therefore, it should be investigated all such humans err and under which conditions the inevitable human error can cause a crisis. If any type of crisis can be solved then it can be said as management of disaster. If it cannot be solved and left for the circumstances, it can be called as major disaster. If this problem cannot be solved permanently, it can be called as hurricane. Therefore, it is important to study all such technological crises. For making this study more elaborating, such *crisis can be divided in two parts.*

1. Interruptions 2. Disaster

Interruption refers to break in technology at local level. Disaster refers to major break in technology at higher level. Interruption can be like power outage, water main breaks. Disaster can be like failure of systems, destruction of system, crash of the system. Interruptions can be controlled and overcome. But the time to overcome them is not defined. It may take few minutes, few hours or few days. Disasters can sometimes be overcome and sometimes cannot be. There is no surety of restoration. Again the time for restoration is not defined.
In case of interruptions we have to face the situation for some time and have to make alternative arrangements so the normalcy can be restored soon. In case of Disaster, provisions have been made for such situations. Interruptions means ad hoc arrangements, while disaster means planning and managing alternative in advance.

Now, disaster and interruption can be explained. Disaster means major failure of the system Hard disk crash, Connectivity unavailable, Software crashed, Application crashed & abnormal behavior of technology.

4.2.1 Interruption

Banking and Financial sector has undergone a vast change in the last two decades like deregulation, liberalization and migration from legacy system to Core Banking.

Information Technology plays an important role in banks. Banks are now serving a larger customer base with innovative products through more channels and increasingly rely on IT applications to nurture and grow their business and also have to meet regulatory requirements to ensure financial stability and customer satisfaction. Thus, Banking processes have become increasingly IT oriented, handling very large volume of sensitive financial transactions online and managing critical financial data. This has created a need for qualified personnel to manage critical installations like Data Centres, Network Centres and other installations in the Banks, as well as to develop and upgrade products and applications. Sophisticated and interconnected Automated Teller Machine (ATM) networks, Tele-banking, Core Banking Solutions and Internet Banking Solutions for seamless customer access are available. Technology has its own characteristics. This includes servers, processors, computers, Hard disk, storage media like DAT/TAPE, CD/DVD/SAN etc., UPS, and Networking, cabling, monitor, keyboard & mouse.
Each and every customer of Bank only concerned with the money belongs to him or her. If money is not received on time, then every technology or method is worst for them.

**Interruptions** can occur anywhere, anytime. Massive hurricanes, tsunamis, power outages, terrorist bombings and more have made recent headlines. It is impossible to predict what may strike when. Interruptions can be explained in certain examples.

- In a branch, server is crashed i.e. Operating system is not working or Hard Disk is not booting.
- Networking equipments are not working.
- UPS is not working
- CBS application is not working.
- Connectivity is not available

In all above cases, branches can facilitate the customers by going nearby branch for their transactions or customer themselves can go nearby branches for their work & respective people, experts can be contacted for restoration of normal work in the branch.

There was heavy rain in Mumbai in 2005 when most of the data centre surrounded in flood. To maintain the system safer, banks took a decision to close the working of banks for 2 days. If the data centre was safe, then it would have been called as interruption. If flood had spoiled the premises and machines and computers, it would have been called as major disaster.

4.2.2 **Technological Disaster**

A DISASTER is defined as an interruption of mission critical information services for an unacceptable period of time. Disaster is time related. An interruption during the peak business hours may create greater problem than that occurs after the business hours. Similarly, the period of
interruption defines its characterization as a disaster – major or minor. Identification of major or minor disasters has a direct link to the anticipated time required for restoration to normalcy in the operation and retrieval of entire data / information from the system without any loss.

There is another type of technological failure or disaster. Abnormal behavior in technological devices make some abnormal functions in software, it may be converted in disaster. Storage devices can become non readable, it can lead to disaster. INSAT can be destroyed by someone or by another natural forces, it can be disaster. It should be understood clearly the difference between Disaster and interruption.

If any of these is not working, it may result malfunction of system, non-working of system and disaster of system. The type of disaster may differ based on its intensity. Interruption, crisis and disaster are the stages of such breakage in the services.

As the study is based on the various aspects of Technology in banking, the difference between Disaster and interruption will play an important role in arriving any conclusion.

While we refer the interruption, it means that any break in technology at local level to provide services to the desired class. Such break cannot be described in time or period. It may be few minutes, few hours, and a few days only.

But if we are talking about disaster, it means there is major break in technology at higher level. It denotes the failure of the systems, destruction of the system, crash of the system. The restoration of normalcy does not mean that it is interruption. Interruption can be solved whereas Crisis and Disaster can or cannot be solved.
Most crisis and disaster researchers agree that today’s crises cannot be explained by listing a few easily recognizable factors. The research on causes of crises has become an interdisciplinary effort, paving the way for a multi-level approach that allows us to analyze the origins of any given crisis. At the micro level, such an approach would focus on the role of individuals. In most, if not all crises, human errors are found at the roots of the crisis.

There may be so many technologies to provide various kinds of services to the customer, getting MIS and development. Uninterrupted working of such technology is most important. If technology fails, then what alternatives are available?

The floods in Mumbai brought to fore one such concern for banks. Bank ATM terminals are typically located on the ground floor of premises with the backup power generator being located in the basement. The unprecedented floods of July 2005 made all such ATMs non-functional. In such crisis situations, lack of access to financial resources could have severe repercussions. Without these resources, organizations and individuals would find it daunting to take measures to recover from the disaster. This would compound the already difficult situation being faced and could lead to anarchy and situations like run on banks. If the data center was safe then it could be called Interruption and if the flood had spoiled the premises, machines and computers, it would have been called as disaster.

The experience with terrorism has challenged both governments and disaster researchers. In the United States, all levels of government have invested substantial resources in emergency management, with much of that devoted to terrorism consequence management. With the investment of resources, governments expect more from the community of disaster researchers. To answer such questions regarding the need for and implementation of warning systems, appropriate mitigation measures, tactics
for response and recovery, researchers need to have a firm grasp on what a disaster is and what it is not.

Perhaps one reason why “disaster” will probably never be completely, immutably defined is because the definition depends on shifting portrayals and perceptions of what is significant about the phenomenon.

Disaster has been viewed in its extended scope and definition by taking into account all these perspectives and together these form the basis on which disaster vulnerability is understood and defined. The bottom line of all these paradigms is that disaster is supposed to represent total or near total breakdown of local systems. Ironically, the dilemma with all these paradigms is that while on one hand they define disaster as an objective reality, on the other hand measures to reduce disaster seem to be so far from reality, that in most cases one finds that disaster vulnerability is increasing at very fast pace. Disaster adversely affects the natural and human resources characterizing the space and creates sudden disruption in the local processes defining human environment relationships in that particular space.

This also determines disaster management actions as prevention or mitigation (before), emergency response (during) and long term rehabilitation and development (after), which together form part of disaster management cycle.

To achieve the above objectives, we should identify the areas likely to invite a disaster for the branch. The next stage involves investigation and analysis of the existing scenario, at each branch, in respect of several disaster avoidance facilities as classified below. The following figure shows types of disaster:
4.3 **Hardware Related Disaster**

Hardware includes servers, nodes or desktops, storage like backup, input, output and monitoring devices, network active devices (routers, switches and legacy devices like hubs and passive devices like cabling and stacking, power supply devices like UPS, electrical cables etc.

Physical security in respect of hardware equipment is most important part of avoiding disasters. Access to the hardware by unauthorized person may also result major disaster. Operational failure of hardware equipment is one of the common causes of disaster. Server is the most sensitive equipment
whose failure may lead to a complete halt in the system functioning at branches. Disaster can occur due to less free space available in hard disk. There are also some workstations or desktops from where services are provided to the customers. If these workstations are not working well, the required services cannot be provided. If Annual Maintenance Contract of the hardware is not given or renewed timely, the problem in hardware cannot be solved immediately.

Hardware can also stop working due to some reasons such as high temperature which causes damage to CPU, power supply unit and electric short circuit.

Dust and unused superfluous material, non-cleaning of system room may cause harm to workstations or server. Use of eatables or beverages also cause spread of insects in system room which resulted rats and other creatures who destroy and cuts the cables.

4.3.1 Power & UPS

The equipments relating to power supply to the hardware as well as building can also create disaster. In case of any interruption in power supply, the ignorance of sources and system of alternate power supply can also led a long interruption in the branch. Local or inferior equipments and wiring causes harm to the power devices and disaster. Overload on power supply and carelessness in uses of power may also result a disaster. UPS is one of the components of power support system. It is sized and selected at all branches to support a load required by the hardware, lighting and other equipments. Sudden failure of UPS may create disasters for the branch. At some occasions, it was notices that batteries created disaster. Inferior quality of batteries may cause fire and explosion in the UPS room.
4.4 Software Related

Data on the Server consists of various items. For e.g., Branch database, Application software. A backup procedure is always mentioned in every application or software. If backup is not taken as per requirements, the unavailability of centralized data base can create panic among the customers. The disaster can also taken place if backup taken on a media is not restored as and when required. Safe storage of backup media is also another requirement of avoiding disaster. On Site storage strategy is a preferred one due to easy access to back up data. Non-maintaining proper record of Storage Media can also lead to disaster. If backup has to be restored in emergency, identify the required backup media became difficult. Backups so held in offsite location must be periodically tested. Unauthorized user attempting access to the system and intrusion to the system is also liable for disaster. Unauthorized software like screen savers, free software also creates interruptions at various times. Hacker attacks & computer viruses also cause minor or major disasters.

4.5 Networking Related

The terrorist attacks of 11 September, for example, caused large-scale network outages besides the financial impact lost of data connectivity, the loss of voice contact with friends and family greatly affected many individuals on that day. Any attack on network can also convert normal working in disaster in banks. At present, the data is automatically received from central data pertaining to CBS branches. If the connectivity is not there, the data cannot be extracted.

Any loss of carrier services such as local access, wide-area network channels or Internet access, voice/data connectivity such as routers, switches, PBXs or VoIP systems, or natural or man-made disaster that causes an interruption in network connectivity relating to voice, data, Internet and wireless technologies provided IT operations. Problems or disasters pertaining
to interruption in network services and break in normal operations. Defects in network equipments and maintaining real time off site backups.

4.6 Natural Disasters

A natural disaster is a major adverse event resulting from natural processes of the Earth; examples include floods, severe weather, volcanic eruptions, earthquakes, and other geologic processes. A natural disaster can cause loss of life or property damage, and typically leaves some economic damage in its wake, the severity of which depends on the affected population's resilience or ability to recover.

Category of Natural Disasters

There are two broad categories of natural disasters

1. Climatic Disasters- Resulting from atmospheric phenomena Like Floods, drought, hurricanes.

   Floods occur when torrential rainfall or snowmelt causes river to overflow their banks and overflow surrounding areas

   Droughts are periods of below average rainfall that effect agriculture and water supply to the regions affected by drought.

2. Geologic Disasters: Like earthquakes, volcanoes, and other disasters that occur due to geologic changes.

   The direct effect of earthquake depends on the economy of the region. Earthquakes that strike rural areas tend to cause less physical damage because agriculture interests are not as affected as much as industrial interest. They do not kill large number of lives stocks but collapse the buildings in the area stuck by it.
Natural disasters affect certain macroeconomic variables that in turn help determine long term growth. These are:

1. Natural resources,
2. Physical Capital Accumulation
3. Human Capital Accumulation
4. Technology

With the help of Technology Government increase the understanding of natural disasters. It reduces the cost of uncertainty about whether a disaster will occur. The disaster risk of an area is defined as the probability the natural disaster will damage or destroy physical capital. Disaster risks add to depreciation.

Natural disasters cannot be immediately analyzed and generalized because of climate change the Japanese earthquake in 2011, The Hurricane Sandy in the States last year The floods in Thailand.

Earthquake and Floods are the main sources for possible disaster at branches. This may result from natural disaster, structural faults within the branch premises, plumbing leakage, and leakage from air conditioners. A flood is an overflow of an expanse of water that submerges land.

An earthquake is the result of a sudden release of energy in the Earth's crust that creates seismic waves. At the Earth's surface, earthquakes manifest themselves by vibration, shaking and sometimes displacement of the ground. The vibrations may vary in magnitude. It is usually the secondary events that they trigger, such as building collapse, fires, tsunamis (seismic sea waves) and volcanoes that are actually the human disaster. Some of the most significant earthquakes in recent times include: The 2004 Indian Ocean
earthquake, the third largest earthquake recorded in history, registering a moment magnitude of 9.1-9.3. The huge tsunamis triggered by this earthquake killed at least 229,000 people.

Cyclones are known by different names. The most intense extra tropical cyclones cause widespread disruption and damage to society, such as the storm surge of the North Sea flood of 1953 which killed 2251 people in the Netherlands and eastern England, the Great Storm of 1987 which devastated southern England and France.

A **tornado** is a violent, dangerous, rotating column of air that is in contact with both the surface of the earth and a cumulonimbus cloud or, in rare cases, the base of a cumulus cloud. It is also referred to as a **twister** or a **cyclone**.

Tornadoes come in many shapes and sizes, but are typically in the form of a visible condensation funnel, whose narrow end touches the earth and is often encircled by a cloud of debris and dust. Most tornadoes have wind speeds less than 110 miles per hour (177 km/h), are approximately 250 feet (80 m) across, and travel a few miles (several kilometers) before dissipating. The most extreme tornadoes can attain wind speeds of more than 300 mph (480 km/h), stretch more than two miles (3 km) across, and stay on the ground for dozens of miles (perhaps more than 100 km).

According to The **Economic Times (New Delhi) 12th Jan 2005** (Tsunami won’t hurt banks’ ratings: Fitch)

“Global rating agency Fitch on Wednesday said its outstanding ratings on Indian banks would remain unchanged as their financial health is unlikely to be affected by Tsunami that devastated coastal areas in southern India.
"With industrial activity not being affected in any significant manner, banks' exposure to the corporate sector is unlikely to deteriorate as an after effect of the tsunami," Fitch India's senior director of financial institutions, Ananda Bhoumik said in a statement here.

Except the loss of three SBI branches in the Nicobar islands, banks have not reported damages. While operations were temporarily affected in the most severely hit areas, they have now been brought back to normal, Fitch said.

Barring the loss of three SBI branches in the Nicobar islands, banks have not reported damages. While operations were temporarily affected in the most severely hit areas, they have now been brought back to normal, Fitch said.

Overall, the total loan loss provisioning requirement of banks as a direct result of tsunami is estimated at less than Rs 100 crore, which is a minute fraction of the Rs 8,60,000 crore loan portfolio held by Indian banks, Fitch said.

According to SAWADA Yasuyuki's analysis (Associate Professor, Graduate School of Economics, The University of Tokyo)

The analysis showed that the effects of disasters on a given country's economy differ depending on factors such as
1. length of time post-disaster,
2. disaster type, and
3. size of the country's GDP

When we look at global averages in short-term periods of one to three years, natural disasters produce the largest downward effects on per capita GDP. A single natural disaster can lower per capita GDP by an annual rate of
about 1%. Conflicts and wars cause the second largest effect on per capita GDP. Both lower the figure by an annual rate of 0.4 to 0.5%. Economic crises follow conflicts and wars, but their downward effect on per capita GDP is limited possibly to 0.2% per year.

**Table 4.1: Effects of Disasters on Per Capita GDP (Annual Rate)**

<table>
<thead>
<tr>
<th></th>
<th>Short Term (1 Year)</th>
<th>Long Term (20 Year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Disasters</td>
<td>-1 to -0.7%</td>
<td>+0.6 to +1.2%</td>
</tr>
<tr>
<td>Conflicts and wars</td>
<td>-0.5 to -0.4%</td>
<td>+0.4 to +0.9%</td>
</tr>
<tr>
<td>Economic Crises</td>
<td>-0.7 to -0.2%</td>
<td>-0.5 to 0%</td>
</tr>
</tbody>
</table>

In contrast, natural disasters, conflicts, and wars work in the opposite direction over the long term and can push up per capita GDP. Based on his analysis of their effects over 20 years, natural disasters increase per capita GDP by 0.6 to 1.2% per year, while conflicts and wars produce upward effects of 0.4 to 0.9%. However, the effects of economic crises remain negative at minus 0.5 to 0% even over the long term (as shown in the table).

### 4.7 Human behavior Related

Man-made disasters are disasters and the element of human intent, negligence or involving a failure of a man-made system that leads to human suffering and environmental damage. Man-made disasters are sometimes referred to as anthropogenic. The term anthropogenic designates an effect or object resulting from human activity.

Manmade disasters can be divided into different categories and they include technological hazards, sociological hazards and transportation hazards among others. These are broken down into several categories and while this is the case, there are some that cause more pronounced damage when compared to others. These are divided into different categories which include aviation, rail, road and space among others. Often these are as a result of
neglect or ignorance and over the years, they have claimed several lives. Road accidents are common in India due to reckless driving, untrained drivers and poor maintenance of roads and vehicles. According to Lifeline Foundation, the Ahmadabad based organization working for road safety, India accounts for 13 per cent of road accident fatalities worldwide. With 130,000 deaths in 2007, India tops in the number of people killed in road accidents, surpassing China’s 90,000. Most of these deaths occurred due to bad road designs and lack of proper traffic management systems to separate different streams of traffic.

Another type of disaster that falls in this category is nuclear bomb. When this occurs, it is often as a result of intent and the end results are even more catastrophic with a large percentage of those involved losing their lives or alternatively ending up with major defects or long term injuries. Other types of manmade disasters which are just as catastrophic include chemical spill, oil spill, arson and terrorism. There are also some technological hazards which include power outage.

Banks are using new products and applications in their systems. Employees are not trained accordingly or we can say employees are not given proper training to use those products or application. As a result they make mistakes this can lead to serious disasters.

Suppose a bank Employee Forgot to Logoff the WorkStation and someone on his/her bank stolen crucial information which gave to fraudsters or used against the favor of bank.

This essay question revolves around the one of the most pressing questions asked by media organizations at the scene or onset of a disaster, ‘what/who caused it?’ Was the disaster due to human error or a systems or a technological failure? This essay will attempt to identify some of the factors
that are involved in anthropogenic error and give examples of occasions when the failure to react appropriately or make effective decisions has lead to a disaster. Specifically it will look at case studies where disastrous events have been attributed to human error when, in fact, they may well have later been proven to be caused by a much wider, deeper and systemic malaise that exists and affects the organizational culture and senior management at large.

It is necessary to first understand what is meant by the term ‘human made disaster’, a credible answer may hypothesis that these events are actually better defined as anthropogenic hazards that through errors, misjudgments, failures or negligence of one or more parties have lead to disasters. These anthropogenic hazards show a threat from human intent, neglect and error that involves the collapse of an anthropogenic system. Anthropogenic disasters are human made, ‘anthropogenic’ in nature (caused by man), as opposed to natural disasters which result from natural hazards. Carter, defines human made disaster as, ‘A sudden or progressive event caused by a human, which impacts with such severity on a community that the emergency services or, in their absence, the affected community have to respond by taking exceptional measures.

It is obvious that these emotions occur during times of disaster. However, when such adversity is preventable, the effects are greater and more deeply felt. Take for instance the 9/11 terrorist attacks. This is far worse than Hurricane like because the 9/11 terrorist attacks were planned out to kill people and they were based on selfish reasons. Injury such as this, results in the collapsing of towers, the killing of innocent people and explosions to make matters even worse.
4.8 Cyber Crime

Oxford Reference online defines ‘cyber crime’ as crime committed over internet.

The Encyclopedia Britannica defines ‘cyber crime’ as any crime that is committed by means of special knowledge or expert use of computer technology.

CBI Manual defines it as:
1. Crimes committed by using computers as a means, including conventional crimes.
2. Crimes in which computers are target.

In general cyber crime is an unlawful act wherein the computer is either a tool or target.

Cyber crime has three categories
1. Against Property— financial crimes— cheating on—line— illegal fund transfer.
2. Against Persons— On—line harassment, Cyber Stalking, Obscenity.
3. Against Nation— Cyber Terrorism – Damaging Critical Information infrastructures.

4.9 IT ACT 2000

Objective: The IT Act 2000 aims to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce” which involves use of alternatives to paper based methods of communication and storage of information.
Salient features:

- Legal Recognition for E-Commerce
  - Digital Signatures and Regulatory Regime
  - Electronic Documents at par with paper documents
- E-Governance
  - Electronic Filing of Documents
- Amend certain Acts
- Define civil wrongs, Offences, punishments
  - Investigation, Adjudication
  - Appellate Regime

4.10 Civil Wrongs under IT Act

- Section 43 – Penalties and Adjudication
- Section 44 – Compensation for failure to protect data
- Section 65 – Source Code

Concealment, destruction, alteration of computer source code

- Section 66 – Hacking

Crimes like virus attacks, unauthorized access to computer resources, data theft etc.

- Section 66A – Sending Offensive Messages through Communication Services

Content that is grossly offensive or has menacing character

- Section 67 – Pornography

Obscene material in the electronic form

- Section 69 – Decryption of information

Controller issues order to Government agency to intercept or decrypt or cause to be monitored any information transmitted through any computer
resource. Order is issued in the interest of the sovereignty or integrity of India the security of the State.

- Section 70 – Protected Systems

  Acts covered by this section include switching computer on / off, using installed software / hardware, installing software / hardware, port scanning

- Section 72 – Breach of confidentiality and privacy

  Secured access to any material, discloses such material to another person without the consent of the subscriber

- Section 87 – Encryption for security of data

  The Central government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce by rules, provided for one or more modes or methods for encryption.

**Table 4.2**

**Computer Related Crimes under Indian Penal Code and Special Laws**

<table>
<thead>
<tr>
<th>Crime Description</th>
<th>Act Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sending threatening messages by email</td>
<td>Sec 503 IPC</td>
</tr>
<tr>
<td>Sending defamatory messages by email</td>
<td>Sec 499 IPC</td>
</tr>
<tr>
<td>Forgery of electronic records</td>
<td>Sec 463 IPC</td>
</tr>
<tr>
<td>Bogus websites, cyber frauds</td>
<td>Sec 420 IPC</td>
</tr>
<tr>
<td>Email spoofing</td>
<td>Sec 463 IPC</td>
</tr>
<tr>
<td>Punishment for cheating using electronic signature of another person</td>
<td>Sec 417A IPC</td>
</tr>
<tr>
<td>Punishment for cheating by impersonation using communication network or computer resource</td>
<td>Sec 419A IPC</td>
</tr>
<tr>
<td>Online sale of drugs</td>
<td>NDPS Act</td>
</tr>
<tr>
<td>Web Jacking</td>
<td>Sec 383 IPC</td>
</tr>
<tr>
<td>Online sale of Arms</td>
<td>Arms Act</td>
</tr>
</tbody>
</table>
4.11 Recent Cases

1. The Sun purchases bank details of 1,000 Britons for just £3 each

Case
- As communicated by The Sun, its reporter (Oliver Harvey), operating undercover, was sold top secret information on 1,000 bank accounts by Karan Bahree in Delhi. Bahree confirmed as to having obtained the data from contacts at call centers in and around Delhi.
- Bahree claimed that he had acted at the behest of another person to merely deliver a "CD presentation" without knowing that he was passing on classified information.
- However, Bahree has admitted to taking the money as a service charge.

Action Taken:
- Bahree sacked by his employer (Infinity eSearch).
- Gurgaon Police has initiated a suo moto preliminary enquiry into the case, and has seized the computer Bahree used to work on, at Infinity eSearch.
- His resume, appointment letter and termination letter have also been seized.

2. BPO employees arrested for hacking Case
- Two employees of IntelNet Global Service, a BPO firm, tampered with the credit card profiles of American citizens.
- According to sources, the two employees were paid over Rs 10 lakh through a wire transfer from a bank in Detroit, for modifying the personal and financial data of hundreds of credit card holders.
- These records were maintained by a US-based company, Trans-Union Services. IntelNet, a service provider, had undertaken the job to maintain the records of Trans-Union.
• The two employees had hacked into TransUnion’s database in August 2005 on the instructions of one Frederick Rodney, based in the US.
• As per police reports, Rodney had provided file numbers of card holders, and had asked the employees to make the changes in their financial profiles.

3. **India’s first case of “phishing” Case:**
   • Kamal Kumar, with assistance from his friend in Nigeria, develops a clone of the ICICI website (original – www.icicibank.com; clone – www.icicibank.net).
   • E-mails are sent by Kumar to ICICI customers, asking them to validate their details like credit card numbers, account numbers, banking passwords etc. Link at the bottom of emails would lead customers to the fake website.
   • Details provided by customers on fake website are used by Kumar to do shopping on the net, for which the real card holder ended up paying.

**Action Taken:**
   • Case lodged by ICICI Bank with Mumbai police on 7th February 2006.
   • Kumar is arrested by the Mumbai police on 2nd March 2006 on various counts of cheating, forgery and hacking, and the fake site has been brought down.

4. **Large Nationalized Bank Case:**
   • Shaikh working in the Credit Card department of State Bank of India had access to credit card details of customers, which he passed on to his friend kale who further passed on to his friend Lukkad who used this information to book air tickets.
   • These air tickets were sold to customers & institutions for money. One such customer got an alert message of ticket purchases when he was holding the card with him & had not done any transaction.
Action Taken:

• On Complaint the police found that all tickets were booked online. Police requested the log details & got the information of a private institution. Investigations revealed that the details were obtained from State Bank of India.

• Cyber Cell head DCP Sunil Pulhari and PI Mohan Mohadikar A.P.I Kate were involved in eight days of investigation and finally caught the culprits.

• In this regard Mr. Sanjeet Mahavir Singh Lukkad, Dharmendra Bhika Kale and Ahmead Sikandar Shaikh were arrested.

5. India's First ATM Card Fraud

The Chennai City Police have busted an international gang involved in cyber crime, with the arrest of Deepak Prem Manwani (22), who was caught red-handed while breaking into an ATM in the city in June last, it is reliably learnt.

The dimensions of the city cops' achievement can be gauged from the fact that they have netted a man who is on the wanted list of the formidable FBI of the United States.

At the time of his detention, he had with him Rs 7.5 lakh knocked off from two ATMs in T Nagar and Abiramipuram in the city. Prior to that, he had walked away with Rs 50,000 from an ATM in Mumbai.

While investigating Manwani's case, the police stumbled upon a cyber crime involving scores of persons across the globe.

Manwani is an MBA drop-out from a Pune college and served as a marketing executive in a Chennai-based firm for some time. Interestingly, his audacious crime career started in an Internet cafe. While browsing the Net one
day, he got attracted to a site which offered him assistance in breaking into the ATMs. His contacts, sitting somewhere in Europe, were ready to give him credit card numbers of a few American banks for $5 per card. The site also offered the magnetic codes of those cards, but charged $200 per code.

The operators of the site had devised a fascinating idea to get the personal identification number (PIN) of the card users. They floated a new site which resembled that of a reputed telecom company. That company has millions of subscribers. The fake site offered the visitors to return $11.75 per head which, the site promoters said, had been collected in excess by mistake from them.

Believing that it was a genuine offer from the telecom company in question, several lakh subscribers logged on to the site to get back that little money, but in the process parted with their PINs.

Armed with all requisite data to hack the bank ATMs, the gang started its systematic looting. Apparently, Manwani and many others of his ilk entered into a deal with the gang behind the site and could purchase any amount of data, of course on certain terms, or simply enter into a deal on a booty-sharing basis.

Meanwhile, Manwani also managed to generate 30 plastic cards that contained necessary data to enable him to break into ATMs. He was so enterprising that he was able to sell away a few such cards to his contacts in Mumbai. The police are on the lookout for those persons too.

On receipt of large-scale complaints from the billed credit card users and banks in the United States, the FBI started an investigation into the affair and also alerted the CBI in New Delhi that the international gang had developed some links in India too.
Manwani has since been enlarged on bail after interrogation by the CBI. But the city police believe that this is the beginning of the end of a major cyber crime.

6. **Thieves Clone NRI Businessman’s Debit Card (Friday 14th July 2013)**

Debit card of NRI businessman was cloned when he came to India in January 2013. After cloning that card was swiped at restaurants, malls and mobile stores in Delhi.

**How Cloning in done?**

**Step 1.** A waiter or shop assistance steal information from customer’s credit or debit cards.

**Step 2.** A pocket sized scanning slot is used (looks like pager, can be worn on a belt). This contraption is called a skimmer.

**Step 3.** As at restaurant and petrol pump we pay by card, unscrupulous employee swipe it in skimmer before it reaches the pay counter. This was information on the magnetic strip is copied.

**Step 4.** Stolen details are copied on counterfeit cards, complete with security hologram marking.

**Step 5.** Thief shops from our card. Credit Card Company or bank sends the victim queries about any unusual spending patterns.

The card was swiped at around 13 different merchant outlets between May 21 and May 23 even though it was in his wallet. Victim claimed that he left India on January 21. This case was registered under Section 66 of Information Technology Act.
4.12 Objectives of I.T. legislation in India:

It is against this background the Government of India enacted its Information Technology Act 2000 with the objectives as follows, stated in the preface to the Act it “to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.”

The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000, got President Assent on 9 June and was made effective from 17 October 2000.

The Act essentially deals with the following issues:

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cyber crimes.

Amendment Act 2008: Being the first legislation in the nation on technology, computers and ecommerce and e-communication, the Act was the subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some conspicuous omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology
based cases with the I.T. Act also being referred in the process and the reliance more on IPC rather on the ITA.

Thus the need for an amendment – a detailed one – was felt for the I.T. Act almost from the year 2003-04 itself. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the I.T. Act and comparing it with similar legislations in other nations and to suggest recommendations. Such recommendations were analyzed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures, the consolidated amendment called the Information Technology Amendment Act 2008 was placed in the Parliament and passed without much debate, towards the end of 2008 (by which time the Mumbai terrorist attack of 26 November 2008 had taken place). This Amendment Act got the President assent on 5 Feb 2009 and was made effective from 27 October 2009.

Some of the notable features of the ITAA are as follows:

Focusing on data privacy
- Focusing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognizing the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- Authorizing an Inspector to investigate cyber offences (as against the DSP earlier)
Section 43 deals with penalties and compensation for damage to computer, computer system etc.

Thus the new Section 43-A. dealing with compensation for failure to protect data was introduced in the ITAA -2008. This is another watershed in the area of data protection especially at the corporate level.

As per this Section, where a body corporate is negligent in implementing reasonable security practices and thereby causes wrongful loss or gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. The Section further explains the phrase ‘body corporate’ and quite significantly the phrases ‘reasonable security practices and procedures’ and ‘sensitive personal data or information’.

Thus the corporate responsibility for data protection is greatly emphasized by inserting Section 43A whereby corporate are under an obligation to ensure adoption of reasonable security practices. Further what is sensitive personal data has since been clarified by the central government vide its Notification dated 11 April 2011 giving the list of all such data which includes password, details of bank accounts or card details, medical records etc.

Reasonable Security Practices
- Site certification
- Security initiatives
- Awareness Training
- Conformance to Standards, certification
- Policies and adherence to policies
- Policies like password policy, Access Control, email Policy etc
- Periodic monitoring and review.
The knowledge that cyber crime is geography-agnostic, borderless, territory-free and sans all jurisdiction and frontiers and happens in ‘cloud’ or the ‘space’, has to be spread and proper training is to be given to all concerned players in the field.

Banks are using new products and applications in their systems. Employees are not trained accordingly or we can say employees are not given proper training to use that product or application. As a result they make mistakes which can lead to serious disasters.

Suppose an Employee Forgot to Logoff the WorkStation. Some other employee can steal secret information and misused it against the bank or give it to fraudsters.

Arson is the criminal intent of setting a fire with intent to cause damage. The definition of arson was originally limited to setting fire to buildings, but was later expanded to include other objects, such as bridges, vehicles, and private property.

Highest degree of threat to human life, as well as to business operations posed by fire, ranks it.

4.13 The Data Recovery Challenges in Banks

As the banking IT system improve and increase its services, they face challenges in reducing business risk due to IT outages.

As banking applications grow there is a pressure on IT managers to reduce the time and resources for conducting regular ‘recovery drills’

Meeting RTO objectives can become tricky as it means organizing access to experience and scarce expertise.
It is mandatory for IT managers to gather requires documentation to demonstrate that adequate systems and process are in place to ensure regulatory compliance.

Some of the key challenges that banks face are as follows

- As banking services are available for 24 * 7, there is a little downtime for DR drills.
- Complete IT applications running on heterogeneous technologies require manual intervention and expertise to test recovery readiness.
- Managing and propagating changes done on primary site to DR site. While making these changes sometimes inconsistent application environments, causing recovery system at the DR site to fail.
- IT landscape in a bank usually consists of multiple IT applications that are interdependent and have to be accounted for when planning for recovery.
  
  Example: - Internet banking and ATM needs core banking. These dependencies increase recovery complexity.
- IT managers have little visibility of how well their solutions are meeting recovery SLAs. They can find it out only at the time of drill.
- Coordinating the required information to submit to regulatory authorities is a time consuming task

4.14 Disaster Recovery Planning (DRP)

DRP has become a very difficult task for Indian banks. We come across high profile natural and man-made disasters.

DR Methodology of banks is a straight forward application which follows a project plan similar to System Development life cycle (SDLC)

- Networks are more complex than before. Multiple layers of devices(optical/physical, Ethernet, IP)
• Complexity of operating a network is directly proportional to Number of device Relationships in the network. The number of device relationships can reach up to square if the number of devices.

• Devices are more complex. Number of parameters requires to describe an interface are more than a decade ago. More interface per device.

• Services are more complicated as they have to coordinate behavior of more devices.

• Regular Software updating and management of computers is complex to manage, problem with troubleshooting, telecom network operations personnel have very less experience with new issues.

• Maintaining stable network operations under all possible operating conditions is difficult to achieve as number of standards with extensions and interpretations differ among vendors.

4.15 Disaster Recovery Risk assessment

IT disaster recovery focuses on the following risk scenarios. Loss of these scenarios has negative impact on banks

- Loss of access to premises
- Loss of data
- Loss of IT functions
- Loss of skills

Risk assessment focuses on the risks that can lead to the above outcomes. According to Peter Barns, FBCI managing director of London based 2C consulting “The key activities from an IT perspective are to consider the impact on the business if delivery of critical applications and services were to be denied as a result of a fire or server failure. For example to access the risks that such a scenario might arise.”
Key Aspect is to know what services run on which parts of the infrastructure.

It was suggested by Andrew Hiles, FBCI, managing director of Oxfordshire-based “Kingswell” International that

“It sounds obvious, but one major insurance company had grown by acquisition and suddenly had several data centers. They did not have a clue of the risks associated with their new acquisitions.

Disaster Recovery Risk Assessment (DDRS) and Business Impact Analysis (BIA)

DDRS and BIA both are crucial steps in building DRP. Before looking for DDRS and BIA bank has to locate disaster recovery risk assessment.

IT disaster recovery process has a standard process flow

4.16 Network Disaster Recovery Plan

Network Disaster Recovery Plan document is prepared so that at the time of disaster banks can refer that document and bring network to normal state as soon as possible.

Things which should be documented in network disaster recovery plan are

1. **Hardware and Software**
   - Configuration setting of every networking hardware of data centre (example ROUTERS)
   - Ports which are open on firewall
   - Firmware versions used on each of the hardware device
2. **Network Diagram**

Network Diagram of the data centre is must.

Example: *Router of the data centre is stuck by lightening. At this time bank can refer to configuration document of old devices which will help to replace that old router with the new one. The new router is configured.*

Problem: If the two routers are not identical then engineers have to find out which network cables will be plugged into each port.

Solution: Network Diagram helps to figure out the correct network cables and ports. LANsurveyor is a tool from Solar winds which helps produce network diagram. Network mapping applications can also be used some of which are available free of cost.

3. **Contact Information**

Contact Information of those employees who are useful at the time if emergency
Employees in IT unit
Vendors

Technical support contact numbers (and your account number for the tech support lines) for the hardware and software manufacturers.

4. **Product Information**

Serial Number and Model Number of all the hardware
License Information of software (when software publisher is called for support)
Operating System that software is running on.
Steps to Create a Disaster Recovery Plan

1. **Define Unacceptable loss**
   
   Before developing a plan, the bank should decide how much it will lose when plan is not there. This will help us decide how much time, effort and money should be spent on the plan.

2. **Backup Everything**

   Everything should be backup
   - Data
   - Metadata
   - Instructions needed to get them back

   Backup facilities includes
   - Building
   - Phones
   - People

3. **Organise Everything**

   Suppose bank has proper documentation of disaster recovery plan but at the time of disaster we cannot locate it. Then the hard work behind documentation is of no use. Therefore backup plans should be properly and safely kept in an organized manner so that backup facilities are the hardest part of the DR plan.

4. **Protection against disaster**

   Disaster recovery plan should be planned to protect the bank against all types of disasters mainly technological because today’s banking industry is based on IT.
5. **Documentation of Everything**

   The person who is documenting the plan should document in such a way that anyone can follow these steps after or during a disaster.

6. **Test**

   Testing of documentation of disaster recovery plan is necessary as without testing plan is mere a proposal.

7. **IT Hardware**

   IT hardware includes
   
   - Servers and Storages like backup, input, output and monitoring devices
   - Network devices like routers, switches and legacy devices like hubs.
   - Passive devices like cables and stack

   All the devices are used to ensure information security audit firewalls, threat prevention systems and antivirus gateways. Power Supply without fail should be available. Bank should regularly audit power efficiency, supply and chances of downtime. Cooling is also important since data centre equipment works 24*7. Data centre and Disaster Recovery site(s) should be on different seismic zones. All the laptops, desktops, smart phones and tablets belonging to the bank employees, customers, and vendors should be audit.

8. **IT Software**

   Database and application should be audited regularly. Best practices of disaster recovery audit are as follows:

   a. **Customize Disaster Recovery Templates**

      Disaster Recovery audit should be done strategically as it contains confidential information about the bank. Confidential information is like bank functions profit centers, bank stress points. Template should be made and implemented according to bank’s need.
9. **Have a Mix of Internal and External Audits**

   Bank should have internal and external auditors. The benefits of mixed auditors are that, internal auditors bring their expertise in representing bank functionalities and critical things of banks. The external auditors give unbiased person view of the bank’s risks, loopholes which got unnoticed by internal auditors. Before inviting external disaster recovery auditor’s internal team should be done away with GAP analysis of the bank. Based on the trust in external auditor’s understanding of the banking business and involved risks, formulate a disaster recovery audit program.

10. **Conduct Regular audits and Certificate program**

    Once a bank is complete with disaster recovery audit program and set of security policies, regular audits are necessary as technological up gradations takes place and as a consequence employees have to trained new skills. Bank can certify them in the areas like

    - ISO 27001 (information security)
    - ISO 9001 (Quality Management)
    - ISO 14001 (Environment Management)

11. **Have Emergency Procedures and Drills**

    At the time of earthquake offices are evacuated on priority.

    - Ensure all processes are switched over to the DR site located at a different seismic zone.
    - Resume activities in the primary site at the earliest.

    Regular tanning and DR drills are must. Unplanned audits by internal as well as external auditors to explore loopholes and non-compliance.

    Proper documentation of checks and drills is done to prepare users for unforeseen circumstances. Replication and policy based backup of other databases ensure safety and recovery of these documents.
Regularly audit service level agreements (SLA) signed between various hardware and software vendors. This ensures good integration between banks SLA during disaster recovery audits to ensure unified uptime. Inlinked SLAs will ensure availability on all technological fronts.

**DR Plan includes the following**

1. **Risk Analysis**
   
   It is the 1st step for DR and contingency planning. It takes a list of possible risks to operations. Risk Analysis involves
   - Risk identification
   - Assess of likelihood of the event to occur
   - Define severity of events consequences
   
   Risk can be anything from power outage, hardware failure to earthquake or flood.

2. **BIA**

   BIA evaluates critical Banking functions. It identifies and quantifies the impact of those functions (Functions can be operational and functional) would have on the organization.

**Figure 4.3**

Keystone BCM Lifecycle
3. **Building DR Plan**

‘DR plan provides structured approach for how to respond to unplanned incidents’. Provides step-by-step procedures for recovering disrupted systems and networks to resume normal operations. Plan identifies critical IT systems and networks, prioritize recovery time. Objectives and outlines the step needed to restart, reconfigure and recover.

![Figure 4.4](image)

4.13 **Business Continuity Management (BCM)**

BCM is a function which consists of a complete set of processes. These processes identify potential threats which impact banking processes in the bank. It provides a framework for building resilience for an effective response which safeguards the interest of key stakeholders, reputation, brand and value creating activities. It is inclusive of disaster recovery, crises management, contingency planning as well as alternative planning.
BCM includes conducting

BIA- Process of analyzing the affect of interruptions to business operations or processes on all banking functions.

BCP- Process of developing prior arrangements and procedures that enable banks to respond to an event in such a manner that critical banking functions can continue within planned levels of disruption.

Information Policy (IP)

IP classifies the available information based on sensitivity. It outlines the owners of the information to which it is end use of the information to which it is subjected. Therefore it is essential that clear, specific and Comprehensive Information Policy is framed so that timely and relevant information is available for banks development effectiveness.

The major rationale for forming an information policy is

- Importance of transparency in bank’s mission
- Commitment to foster ownership
- Build Dialogue
- Strengthen public oversight of development initiatives

Principles of access to information set path in the foundation of IP. There are standards for collection, compilation, storage, retrieval and dissemination of information on which framing and implementation of IP is based. IP should be reviewed and updated periodically.

Information Security Policy (ISP)

ISP is a documented banking business rule for protecting information and the systems which store and process this information. ISP provides high-level description of various controls of the bank will use to protect information. Information should be based on the principles of integrity,
reliability and validity. Protecting confidential information of banks is the priority. ISP should be reviewed and updated at periodical intervals. It may mansion and gives details of principles for protecting information from unauthorized access, use, disclosures, disruption, modification or destruction.

It inter-alia, relate to policies such as firewall, email, network security, and password. It mansions prevention of cyber attacks by deploying technologies such as two-factor authentication.

**Audit of IT Process and Infrastructure**

Audit of IT Process and Infrastructure are done to ensure confidentiality, integrity, authenticity and timely availability of information. To ensure this there are various types of audits
Organizational IT audit (Management control over it)
Technical IT audit (infrastructure, data centers, data communication)
Application IT audit (business/ financial/operational)
Development/Implementation IT audit
(specification/requirements, design, development and post- implementation phases)

Compliance IT audit

These audits may be conducted at periodic intervals keeping in view the requirements for the bank. Audits may conduct up to national / international standards.

Interruptions can occur anywhere and at anytime. Like tsunami, power outage, terrorist bombing were in headlines in the last decade.

In today’s 24 * 7 *365 world it has become very important to prepare DR plans. Anything can happen anytime and banks should be prepared for it. With the increasing dependence on banks for both electronic and traditional
banking services, it has become mandatory for banking sector to plan for ‘Business Continuity’.

Today almost all the activities are dependent on banks. They are tuned into business models to deliver service in the age of BOUNDRYLESS COMMERCE.

In 2005 flood in Mumbai since ATM terminals are located on ground floor with their backup power generator located in its basement, due to rain all ATMs were non-functional. In such situations lack of access to financial resources could have severe implications, without those resources other organizations and common man finds it difficult to recover from these interruptions.