ORIGINAL RESEARCH PAPER
Volume-6 | Issue-9 | September-2017 | ISSN No 2277 - 8179 | IF : 4.176 | IC Value : 78.46
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

CYBER CRIME AND FRAUD MANAGEMENT OF BANKING IN INDIA

Commerce

Sri. KAITH GARIB DASS IPS I.G.OF. POLICE, JAMMU & KASHMIR

Dr. P.B. REDDY Ph.D. Advocate Supreme Court of India New Delhi

Dr. MORUSU SIVA SANKAR Ph.D. Academic Consultant, Dept. of Commerce S.V. University, Tirupathi 517502

ABSTRACT

CYBER Technological revolutions both in communication and information technology have changed the way of doing business. In todays changed and changing environment electronic commerce and electronic banking has become an integral part of customers as well as bankers. On account of e-commerce and e- banking distances of locations have reduced and many international financial markets have been linked. While it can be appreciated that the computers have become an integral part of one's life, it has also created space for cyber crimes. In view of the fast changing world on account of significant contribution of the IT sector, the cyber crimes pose a significant threat. Cyber crimes are usually carried out by the criminals with technical knowledge and can outstrip and think one step ahead to penetrate into the computers to carry out the crimes.

KEYWORDS

Cyber Crimes
A cyber crime can be defined as "criminal activity carried out by using computers and internet". A cyber crime can also be defined as "use of computers and/ or other electronic devices via information systems like computer network, internet to handle illegal activities like transfer of funds, withdrawal of funds through unauthorized access"

Effects of cyber crimes:
1. Financial loss
2 Sabotage and theft to identifiable information
3. Exposed to reputation risks
4. Infringement of confidential information
5. Legal consequences
6. Operational risks

Reasons for cyber crimes:
Easy access to data:
If a cyber criminal is able to break into a computer's system, the access to the sensitive data including customer's confidential financial data, information can be copied into a small removable device.

Negligence on the part of the users:
Individuals and the employees, officers, executives and other professionals who use the computer systems should be vigilant to protect their information and sensitive data stored in the computers.

Lack of internal control in organizations and banks:
A computer system works based on instructions received from operating systems which are driven by a number of codes

Cyber crimes against Society:
Society is one of the important stake holders along with the Government/s. Sensitive websites of governments and the military are subject to hacking. These sensitive web sites are interconnected and unless otherwise properly controlled and protected, it can pave way for cyber crimes. Crimes like money laundering, sale of illegal and prohibited articles, forgery, etc are examples of crimes against society and government/s.

Some examples of cyber crimes:
1. Unauthorized access/control over computer system
2. Intellectual Property crimes
3. Internet time thefts
4. Cyber terrorism against the government or organization
5. Distribution of pirated software
6. Trafficking
7. Pornography (especially child pornography)
8. Fraud
9. Financial crimes

Financial Crimes
Any crime committed for financial gains is called "financial crime". With the changed banking environment on account of IT and communication revolutions, banks are offering many services like internet and mobile banking, online trading and more of e commerce facilities. Examples of financial crimes are: cheating, credit card frauds, hacking into bank servers, etc.

Fraud and Cheating:
Fraud or cheating can be referred to any dishonest and intentional action to deprive or dupe a person of his or her money, assets or legal rights. As regards cyber crimes frauds and cheating can be classified into:
1. On line cheating and/or fraud:-
a. This is the most popular cyber crime. Some examples are
b. Offer jobs and require you to furnish sensitive information
c. Calls for sensitive information like bank account details, credit card details, pass words, user IDs. through the communications purported to have generated from the Income Tax authorities, Government Agencies, Reserve Bank of India and other Institutions
d. Informing about winning a lottery or identifying the person as the beneficiary of huge fortunes left by somebody.

e. Encourage the customer to invest in schemes that offer unduly higher returns
f. On line shopping may end up in the "buyer buys goods or services" when purchased articles are never delivered.

2. Fraud committed on account of weakness in computer systems-
a. Input stage: data is falsified and entered in a manner that makes the data as genuine
b. Output stage: information is altered and/or destroyed to conceal un authorized transactions. Storage of data is altered or deleted

3. On account of forgery: Forgeries are committed by using computers. Some examples are: printing of counterfeit currency notes, stamp papers, certificates. Modern printers and scanners photocopiers are used to carry out such frauds.
a. Information Theft: Information theft arises when confidential information is stolen for various reasons either by intruders to the IT system and /or by insiders. It can result in situations such as (i) the reputation of an entire organization is lost (ii) customer confidential information/data is damaged (iii) regulatory violations are exposed

Other Important Issues

Cyber extortion: A crime involving an attack or threat of attack against an enterprise. It is a crime through which a criminal gains access to a victim's email account by stealing his or her password.

Computer Security: Computer system is very sensitive to security controls. In case of weak security control, computers are exposed to many risks.

Legal Loss: A cyber attack on a bank can result in legal cases initiated by customer against the bank. The bank might end up paying huge amount of compensation and legal costs.

Banks as financial intermediaries play a crucial role in the financial markets. Banks also act as trustees depending upon situations.

Integrated Communication Network for Banks Security and Control Systems

Banks are exposed to many risks in their activities relating to management of funds on line banking services. credit card and other e-banking products/services are also facing risks which are associated with the use of IT tools, channels, platforms. Banks should have a good and effective control system to handle IT related issues and risks.

Preventive Controls: This type of control stops errors or irregularities. Good design/ screen lay out reduces or stops the errors at the time of coding data or entering data from source document.

Detective Controls: Identification of errors or irregularities happens after they occur. For example: An input validation program identifies data input errors.

Corrective Controls: These types of controls remove or reduce the effects of errors and irregularities after they have been identified. If any data is corrupted during transmission the communication software (with inbuilt control) may request for retransmission of information/data.

Physical Controls: In computerized environment, the control of access is very important in view of the confidential and sensitive information/data which are being processed/stored at the data processing center.

Internal Controls: To ensure that the accounting data and other sensitive customer information are accurate and reliable and also to protect assets of the bank, a system of internal controls are built in the computerized systems. An effective and efficient internal control would assist the bank management to run the bank's operations in a better controlled environment.

Accounting Controls may be in the form of (a) dual controls and authorizations (b) validation checks on data (c) other controls on access to the software applications.

Some other controls include validation of each transaction against limits and balances, stop payments, post dated and stale dated cheques, etc.

Operational Controls: Operational controls are embedded in software whereas access controls can be enforced by the system software and application software at different levels.

Computer Audit covers, review of operations to ensure compliances of bank's systems and procedures and policies, standards.

Audit around the computer: The auditor examines the internal control system of the computer installation and related input and output of the application system. 'Around the computer audit' needs to be carried out to ensure/ verify:

(i) the systems are supported by well tested software
(ii) a clear cut system generated audit trail is available
(iii) proper physical controls are in place
(iv) Duties and responsibilities of various employees are well defined and segregated.

Audit through the computer: This is used to check whether logic and controls are available within the system and records produced by the system are in conformity with the input and expected level of output. Audit through the computers can be carried out by test checks, mock trial runs, and the tools like special audit modules embedded in the application systems to generate audit evidence.

a. Integrity of the system to safeguard the assets of the bank
b. reveals the status of the information system indicating any short comings as well
c. assists banks to take a better decision on the management control system of the bank

Off-site Audit

Banks should setup proper offsite monitoring cell (OSM) in audit department or put in place suitable similar structure. Such cell should review the MIS on critical items and sensitize the controlling offices and the branches, for corrective action on daily basis.

Information System Security (ISS)

In today's complex and competitive changing business environment, the information technology assists banks across the globe to offer wide range of services and products and also give competitive edge to the players with well supported information system. However, banks are also exposed to many risks on account of growing opportunities on account of information system.

Objectives of banks' IS Security Policy:

Confidentiality: The confidentiality of customer information and sensitive financial data should not be revealed to unauthorized persons. The IS security should ensure that the confidentiality is maintained

All the required controls should be in place to ensure availability of reliable and correct information to the authorized users and persons. These controls include access controls by PIN, pass words, proper approved authentication control, and effective internal controls.

E-banking allows on line banking services and as such the banks' should ensure high level of IS security as part of e banking.

Threats to IS Security: Banks are also offering Core Banking Solutions along with e banking or online banking. In view of these facilities, network security is a concern for banks.

External Factors	:	Natural disasters like floods, fire and earthquake etc.
Internal Factors	:	Hardware and Software failures,
Other Factors	:	virus attack, acts of terrorism

Information Technology Act 2000 provides legal protection for transactions carried out by means of electronic communication. In view of the recognition given to electronic records, electronic signatures, and electronic documents, the banks are also required to follow the amendments of other Acts, such as,

(i) The Indian Penal Code 1860
(ii) The Indian Evidence Act 1872
(iii) The Indian Negotiable Instruments Act, 1881
(iv) The Banker's Books Evidence Act, 1891 and
(v) The Reserve Bank of India Act 1934SSON ROUND UP

1. IT has revolutionized banking sector to a great extent.
2. While the IT and communication technological revolutions have created good opportunities for banks in their business expansion, they have also exposed banks to risks associated with them.
3. Banks have been able to offer virtual banking facilities to their clients and many innovations of making services available through 24x7 basis, internet banking and Core Banking Solutions, quicker transfer of funds through RTGS and NEFT.
4. On the other side, banks are also subject to impact of Cyber Crimes, Money Laundering activities etc.,
5. Recognizing the importance of risks in IT, the regulators, and banks' all over the world need to strengthen their risk management system.
6. Banks are the main intermediaries in the financial sector, therefore, they should be very careful in handling the funds of their clients, with an effective and proactive IT related risk management controls in place to effectively handle the cyber crimes.
7. With the fast growing e-banking and e-commercial activities,

banks should endeavor to have innovative ways to handle the issues relating to the IT and Communications.

References

1) Wikipedia journals
1) Banking system in India
2) H.R. Machiraju, Indian Financial System, Vikas Publishing House, Delhi, 2009