Asian Journal of Management Sciences
ISSN: 2348-0351

Published on: 29-03-2014

Dr. Reshma D. Doiphode
Assistant Professor
Peoples college Nanded.
.

QR Code for Mobile users

Conflict of Interest: None Declared !

E-Crime in Banking Sector.

Dr. Reshma D. Doiphode
People's College, Nanded (M.S.) India.

Cite this article as:
Dr. Reshma D. Doiphode.
E-Crime in Banking Sector.
Asian Journal of Management Sciences.
02 (03 Special Issue); 2014; 83-86.

Introduction

Several bank's IT infrastructure and applications are being exposed to system outages and cyber-attacks. One of Britain's biggest online banks was forced to shut down its website as customers were able to access each other's accounts. In Norway, a hacker led to a major software problem on the website of leading national bank. These cyber-crimes demand global solutions. Though some progress has been made in this direction, a lot remains to be done. For example, Bank for International Settlements has constituted a committee involving representatives of national regulations and supervisors, which closely examine the security and reliability of electronic money. It has called for the development of prudent risk management for e-money activities and stronger cooperation with banks to identify good practice supervisors. The European Commission has started similar initiatives.

Cyber crime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel. A computer is a electronic machine that accepts data and instructions as Input, allows it to be stored and manipulated; and processes (computes) the data at high speed and gives information/ data as output (result).

Thus, computer is a material medium. Internet is not a physical or tangible entity, but rather a giant network, which interconnects innumerable smaller groups of linked computer networks. It is a network of network some networks are "closed" networks, not linked to other computers or networks. Many networks, however, are connected to other networks, which are in turn connected to other networks in a manner, which permits each computer in any network to communicate with computers on any other network in the system. This global web linked networks and computers are referred to as Internet.

The objectives of the paper are as follows

- To study the various types of frauds in e-banking services
- To study the occurrence of various crimes with regards to e-banking services
- To suggest various preventive steps to be followed by the people with regards to e-banking services.

Types of Cyber Crime:

Hacking:

"Hacking" is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. Hacking had witnessed a 37 per cent increase this year.

A case of suspected hacking of certain web portals and obtaining the residential addresses from the e-mail accounts of city residents had recently come to light. After getting the addresses, letters were sent through post mail and the recipients were lured into participating in an international lottery that had Australian $ 23 lakhs at stake.

Computer hackers have also got into the Bhaba Atomic Research Centre (BARC) computer and pulled out important data. Some computer professionals who prepared the software for MBBS examination altered the data and gave an upward

Phishing:

Phishing is just one of the many frauds on the Internet, trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access.

Cafes ~ Emails:

Cyber cafes have emerged as hot spots for cyber crimes. Even terrorists prefer the anonymity of a cyber cafe to communicate with each other. The mushrooming of cyber cafes in the city, which provide the secrecy through cabins constructed for users, has also made the porn literature easily accessible to the people visiting them.

Credit Card Fraud:

Credit cards are commonly being used for online booking of airline and railway tickets and for other ecommerce transactions. Although most of ecommerce websites have implemented strong security measures (such as SSL, secure web servers etc), instances of credit card frauds are increasing. The victim's credit card information is stolen and misused for making online purchases (e.g. airline tickets, software, subscription to pornographic websites etc).

Sections 43 and 66 of Information Technology Act and section 420 of Indian Penal Code are attracted in such matters. All persons who have stolen the credit card information as well as those who have misused it are punishable there. Illegal financial gain is the motive by the misuser.

Online Share Trading Fraud:

With the advent of dematerialization of shares in India, it has become mandatory for investors to have demat accounts. In most cases an online banking account is linked with the share trading account. This has led to a high number of online share trading frauds.

The victim's account passwords are stolen and his accounts are misused for making fraudulent bank transfers as well as the victim's account passwords are

stolen and his share trading accounts are misused for making unauthorised transactions that result in the victim suffer losses.

Tax Evasion and Money Laundering:

Many unscrupulous businessmen and money launderers) are using virtual as well as physical storage media for hiding information and records of their illicit business.

The suspect uses physical storage media for hiding the information e.g. hard drives, floppies, USB drives, mobile phone memory cards, digital camera memory cards, CD ROMs, DVD ROMs, iPods etc.

The suspect uses virtual storage media for hiding the information e.g. email accounts, online briefcases, FTP sites, G space etc.

Prevention:

It is believed that even with the best laws, with efficient investigating agencies and full national and international co-operation, the successful investigation and prosecution of e-bank frauds will remain difficult, costly and time consuming. The emphasis, therefore, has to be on their prevention rather than on detection and investigations.

A lot of research has been done and still more research is going on to make the system completely secure. Philosophically prevention of e-banking frauds is real homework. Pursuit of the e-banking frauders is an unending race in the cyber space against the time, against the criminal, against data. If the E-banking frauds are to be prevented security measures are to be applied,

1. Target:

The target of E-banking frauds are the electronic messages, data, the test and other keys (private keys, PKI), the encryption/decryption, the authentication in passwords, PINS, PICS, Digital Signatures, etc. are to be guarded. They should be under the control of the senior but reliable officer.

2. Access:

Only authorised person should have access to a computer engaged in E-banking. Even close colleagues should not be allowed to use or misuse the E-banking computer. There should be full proof system of identification and authorisation of control and access. Access to E-computer is frequently controlled through passwords. The management should ensure:

Password should be personal, secret and unique, **one password one person** should be the rule.If the operator of the computer changes, the access password to the computer must change simultaneously invariably.

- Password should be biometric or longish alphanumeric. It should not be possible to pick or find out the number from various permutations or combinations by any unauthorised person. Access through biometric password is one of the most secure in e-banking for data protection. It permits access to the computer only to the authentic user. Retina images, fingerprints, voiceprints are being utilised for the purpose. They are individualistic and hence offer excellent security against intruders.
- Password should be changed periodically. The operator using the password must know that all work done on the e-banking computer with the password will be attributed to him and do not pass the password to any other person.
- Card authentication is another and additional security mode. The card is inserted in the E-banking computer. The computer checks the specified data/ information on the card and allows the entry only if the data is correct if the card is stolen then they should have the separate passwords or access cards to guard the same against the unauthorised users.

3. Bank staff:

The most important entity for security against e-banking fraud is the bank staff. The operator must be honest, intelligent, experienced and dedicated to their work; it is possible if they are,

- Properly selected.
- Adequate trained.
- Honest and loyal to the organisation in particular and to the public at large. There should be stringent rule and practical action modes to keep an organisation free from the dishonest employee at all levels.
- The security consciousness must be created to protect the e-banking transactions.
- The staff must be trained in security management and the sensitive assignments are not being given to the temporary or new staff.
- The supervisory staff must be literate to understand working with the computer system.

4. Logging-

Logging is keeping the record of work done on or with the computer. It is done with computer software. The following information is logged,

- The name of the user
- Date, duration and time of the use. The software contains the time stamping protocol in the new generations of the computers. It automatically records the date, the time and the duration of the time for which the computer is used.
- Proper logging is the main source of information for ultimate processing of computer frauds. It should therefore be introduced in the working schedule of the computers,

Incorporation of date, time, duration and users name are useful, especially when the computer is used by the number of persons. The information is useful if the computer is handled or mishandled by the user or the unauthorised person. The supervisory staff must check periodically that the logging is maintained properly and

that no unauthorised activities or work is being done on the computer.

5. Encryption and Decryption:

Encryption and decryption are in fact many responsible for making E-banking possible. They are being utilised extensively to transmit, to secure, to authenticate and to preserve the integrity and authenticity of the electronic data in the computers. Encryption and decryption are routinely used now to send and receive electronic data / documents and messages in E-banking. Encryption and decryption are also used in ATMs, Credit cards, Digital Signatures, and in every message or data being used in E-banking. Encryption and decryption technology to code the messages is therefore, the kings pin in E-banking. The encryption and decryption (done through computers) technologies are the real work mode in E-banking. They are highly complex and not easy to decode. They have made E-banking quick, safe and efficient.

6. Prompt Action:

E-banking frauds involve huge sums of money most of the time. The detection and the initiation of investigation take long time. The fraudster taking advantage of the time lag or is able to hide the loot successfully. Further the punishments are usually light. Prompt action is necessarily taken against the fraudster and should be harassed in such a way that no one even should think to do the fraud. Bank has been a job of trust. It should be continue to be so.

Hence, E-banking crimes are limited in India, yet. But their explosion is round the corner. E-banking frauds have frightening potential for unlawful gains, for mischief and for excitement. We must stronger our self to fight the imminent on slaughter of the danger.

Refernces

1. S.B.Verma- other “E-banking development of banks” Deep and Deep publication house.
2. Vasudeva “E-Banking” Commonwealth Publishers New Delhi P.13.
3. Management of security risks in Electronic banking services
4. http://www.info.gov.hk/hkma/eng/guide/circu_date/200007061_index.htm.