IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Crime: An emerging Challenge to Indian Banking Industry

Rahul Sharma
B.Com, FCA, MBA (Fin.), Ll.b., CAIIB
Senior Manager – UCO Bank,
152/41, Shipra Path, Opp. Patel Marg,
Mansarovar, Jaipur - 302 020

Increased use of e-products :- On the recommendation of the Committee on Financial System (Narasimham Committee) 1991-1998 when founding stones of information and technology were laid in Indian banking sector nobody knew that later on this will be proved a turning stone & not a mile stone and will changed completely the face of banking industry . In changing scenario system of receipt/payment has changed remarkably – swiping of debit cards or credit cards, payments through wallets (using QR codes) and e payments through net & mobiles have become our habits.

As of now India is the fourth largest internet user country in the world. The reach of internet banking has also increased due to the increased internet usage.

Data for e banking services in India are as follows :-

Volume of e-banking
(Numbers)

Particulars of E Service	**31.03.2013**	**31.03.2014**	**31.03.2015**	**31.03.2016**	**31.03.2017**	**31.03.2018**
Automated Teller Machines	116378	162543	182480	199954	207813	207920
Debit Cards	336866879	399652017	564707913	671187187	780795417	903656781
Credit Cards	19553677	19226475	21288891	24860730	30374102	37782876
NEFT (Millions)	394.13	661.01	927.55	1252.88	1622.1	1946.36
RTGS (Millions)	68.52	81.11	92.78	98.34	107.86	124.46
Mobile Banking (Millions)	53.30	94.71	171.92	389.49	976.85	1872.26

The Reserve Bank of India constituted a working group on Internet Banking. The group divided the internet banking products in India into 3 types based on the levels.

Ø **Information Only System:** General purpose information like interest rates, branch location, bank products and their features, loan and deposit calculations are provided in the banks website. There exist facilities for downloading various types of application forms. The
communication is normally done through e-mail. There is no interaction between the customer and bank's application system. No identification of the customer is done. In this system, there is no possibility of any unauthorized person getting into production systems of the bank through internet.

Ø **Electronic Information Transfer System:** The system provides customer- specific information in the form of account balances, transaction details, and statement of accounts. The information is still largely of the 'read only' format. Identification and authentication of the customer is through password. The information is fetched from the bank's application system either in batch mode or off-line. The application systems cannot directly access through the internet.

Ø **Fully Electronic Transactional System:** This system allows bi-directional capabilities. Transactions can be submitted by the customer for online update. This system requires high degree of security and control. In this environment, web server and application systems are linked over secure infrastructure. It comprises technology covering computerization, networking and security, inter-bank payment gateway and legal infrastructure.

Risk Assumption due to increased e transactions :-On one hand, technology has created advantage for banks and financial institutions but on the other hand, there have been risks involved in it as well. Apparently banks assume operational risks due to Technology advancements but implicitly it can also exacerbate other risks like credit risks and market risks. Given the increasing reliance of customers on electronic delivery channels to conduct transactions, any security related issues have the potential to undermine public confidence in the use of e-banking channels and lead to reputation risks to the banks. Inadequate technology implementation can also induce strategic risk in terms of strategic decision making based on inaccurate data/information. **As a whole we have assumed risk in almost all the areas of banking due to increased use of technology**.

Cyber wrongdoings (crimes) and their types:- Broadly speaking following type of wrong doings (crimes) are associated with cyber world **DDoS Attacks** These are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on users' computers. The hacker then hacks into the system once the network is down. **Botnets** Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks. **Identity Theft** This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fraud. They can also open a phone/internet account in your name, use your name to plan a criminal activity and claim government benefits in your name. They may do this by finding out user's passwords through hacking, retrieving personal information from social media, or sending phishing emails. **Cyberstalking** This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically cyberstalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety. **Social Engineering** Social engineering involves criminals making direct contact with you usually by phone or email. They want to gain your confidence and usually pose as a customer service agent so you'll give the necessary information needed. This is typically a password, the company you work for, or bank information. Cybercriminals will find out what they can about you on the internet and then attempt to add you as a friend on social accounts. Once they gain access to an account, they can sell your information or secure accounts in your name. **PUPs** PUPS or Potentially Unwanted Programs are less threatening than other cybercrimes, but are a type of malware. They uninstall necessary software in your system including search engines and pre-downloaded apps. They can include spyware or adware, so it's a good idea to install an antivirus software to avoid the malicious download. **Phishing** This type of attack involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer. Cybercriminals are becoming more established and many of these emails are not flagged as spam. Users are tricked into emails claiming they need to change their password or update their billing information, giving criminals access. **Prohibited/Illegal Content** This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content includes materials advocating terrorism-related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network. **Online Scams** These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are "too good to be true" and when clicked on can cause malware to interfere and compromise information. **Exploit Kits** They are readymade tools criminals can buy online and use against anyone with a computer. The exploit kits are upgraded regularly similar to normal software and are available on dark web hacking forums. **ATM Cloning and Skimming :** Cloning is also called skimming and requires copying information at a credit card terminal using an electronic device or software, then transferring the information from the stolen card to a new card or to rewrite an existing card with the information. **Dark Web** The dark web refers to encrypted online content that is not indexed by conventional search engines. Sometimes, the dark web is also called the dark net. The dark web is a part of the deep web, which just refers to websites that do not appear on search engines. It is a platform of illegal business on net, here information is traded – stolen card numbers, web based managing account, medical records and access to servers.

Indian Legal system and punish ability of Cyber Crimes :- Cyber Crime is not defined officially in IT Act or in any other legislation. Hence, the concept of cyber crime is just a "combination of crime and computer". Following provisions of information Technology act are relevant to us as banker. It has been tried to make them understandable through case laws :-

Section	Offence	Applicability in some	Penalty
43	Penalty and Compensation for damage to computer, computer system,	***Mphasis BPO Fraud: 2005***In December 2004, four call centre employees, working at an outsourcing facility operated by MphasiS in India, obtained PIN codes from four customers of MphasiS' client, Citi Group. These employees were not authorized to obtain the PINs. In association with others, the call centre employees opened new accounts at Indian banks using false identities. Within two months, they used the PINs and account information gleaned during their employment at MphasiS to transfer money from the bank accounts of CitiGroup customers to the new accounts at Indian banks. By April 2005, the Indian police had tipped off to the scam by a U.S. bank, and quickly identified the individuals involved in the scam. Arrests were made when those individuals attempted to withdraw cash from the falsified accounts, $426,000 was stolen; the amount recovered was $230,000. ***Verdict***: *Court held that Section 43(a) was applicable here due to the nature of unauthorized access involved to commit transactions.* **Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, Bugs**All of the above are some sort of malicious programs which are used to destroy or gain access to some electronic information.*Provisions Applicable:- Sections 43, 66, 66A of IT Act and Section 426 of Indian Penal Code.*	Will be liable to pay damages to the affected person and also penalty up to Rs. 500000 and imprisonment up to 3 years
65	Tampering with computer source documents	***Syed Asifuddin and Ors. Vs. The State of Andhra Pradesh***In this case, Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones theft were exclusively franchised to Reliance Infocomm. ***Verdict:*** *Court held that tampering with source code invokes Section 65 of the Information Technology*	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	***Kumar v/s Whiteley*** In this case the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed the passwords to deny access to the authorized users.Investigations had revealed that Kumar was logging on to the BSNL broadband Internet connection as if he was the authorized genuine user and 'made alteration in the computer database pertaining to broadband Internet user accounts' of the subscribers.The CBI had registered a cyber crime case against Kumar and carried out investigations on the basis of a complaint by the Press Information Bureau, Chennai, which detected the unauthorised use of broadband Internet. The complaint also stated that the subscribers had incurred a loss of Rs 38,248 due to Kumar's wrongful act. He used to 'hack' sites from Bangalore, Chennai and other cities too, they said. ***Verdict:*** *The Additional Chief Metropolitan Magistrate, Egmore, Chennai, sentenced N G Arun Kumar, the techie from Bangalore*	Imprisonment up to three years, or/and with fine up to ₹500,000

		to undergo a rigorous imprisonment for one year with a fine of Rs 5,000 under section 420 IPC (cheating) and Section 66 of IT Act (Computer related Offense).	
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen. **New mobile phones are covered under the definition of computer**	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	A person fraudulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.**Online Share Trading Fraud** It has become mandatory for investors to have their demat accounts linked with their online banking accounts which are generally accessed unauthorized, thereby leading to share trading frauds.*Provisions Applicable: Sections 43, 66, 66C, 66D of IT Act and Section 420 of IPC*	Imprisonment up to three years, or/and with fine up to ₹100,000