Strengthening of Cyber Security

R Subramaniakumar

...our country shall provide a completely Cyber Secure architecture that is secure and reliable for the digital transactions. However, it is to be continuously upgraded, as new threats emerge. Security is a journey. Awareness will enable to face and mitigate the risk

Digitalization is the rise of the digital transaction where bank, customers, merchants, industries and other stakeholders form an interdependent financial system network. Digitization is not an option for banking industry, rather it is inevitable, because every industry is being digitized and banking sector is no exception.

Digitalization

Banking and Financial transactions play a significant role in our daily lives. For many of us, a day will not end without at least a single financial transaction with merchants or at banks. Hence, financial institutions should be at the fore-front to adopt latest technologies and to enhance customer experience thus eliminating rural and urban gap.

The following factors influence the digitalisation in banking-

- Changing consumer behaviour in favour of digitalization.
- Financial Inclusion and government initiatives.
- Leveraging increased smart phone usage and mobile penetration.

A Less-cash Economy is an economy in which many of the transactions are carried out through digital means. It includes various modes such as internet banking, mobile banking, debit and credit cards, card-swipe or Point of Sales (PoS) machines, Unified Payments Interface(UPI)-BHIM, QR Code (Quick Response) based transactions, Touch-n-Go cards.

BHIM UPI – Bharat Interface for Money – Unified Payments Interface

BHIM UPI is a revolutionary payment system introduced in India which is a first of its kind across the globe. With sixty banks being a part of BHIM UPI, 21 million users have downloaded BHIM apps. Around 82 lakhs transactions per month are taking place in the BHIM platform.

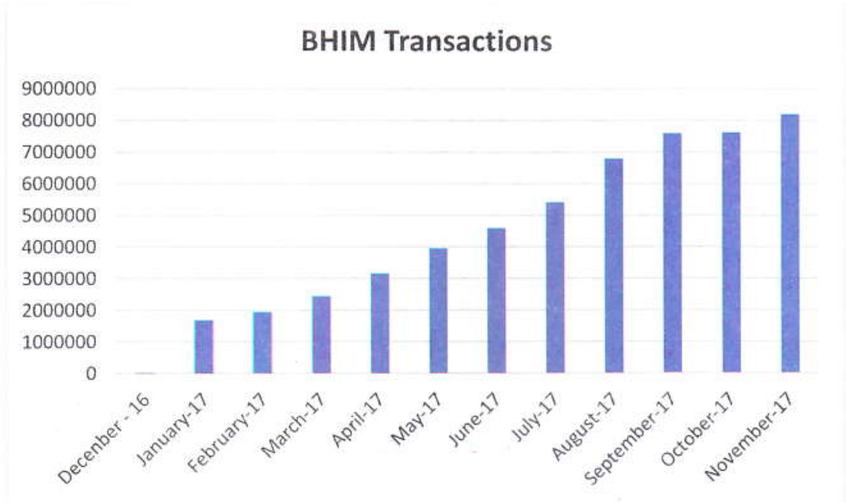
After the launch of BHIM app in the month of December 2016, the number of transactions have grown 200 times exponentially from around forty thousand to eighty two lakhs transactions per month.

BHIM Aadhaar is a digital payment acceptance solution enabling merchants to receive digital payments from customers over the counter through Aadhaar authentication. Customer performs transaction by providing his Aadhaar number and biometric authentication.

Cyber Security

The sky rocketing intrusion of digitalisation in the banking industry

The author is Managing Director and Chief Executive Officer, Indian Overseas Bank. Being a techno Banker, he has contributed in various Indian Banks' Association (IBA) and Institute for Development & Research in Banking Technology (IDRBT) committees on technology and financial inclusion, and was core member of the Smart Card and Micro ATM Standards Committee.



has given more thrust on the implementation of Cyber security in the digital platform. The whole eco system of digitalisation includes the following stakeholders.

- Customer/Originator
- Originating institution
- Processing agency
- Beneficiary Institution
- Beneficiary

Security is to be ensured at all the touch points of the digital transactions. The complete eco-system is to be Cyber-sanitised for all the transactions to be flawless and with the following Security triangulation intact along with Non-Repudiation-

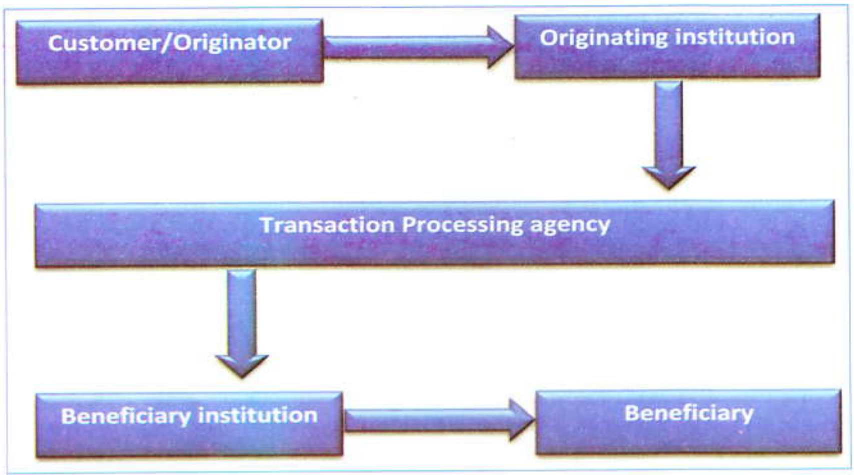
- Confidentiality
- Integrity
- Availability

Let's see how the stakeholders can make sure that the transaction is unimpaired in its whole journey.

Customer/Originator

The originator of any transaction shall ensure that his device from which he is originating is completely Cyber-sanitised. The device should have been patched up with latest Anti-Virus signatures. Care should have been taken to type the website addresses if it is an online transaction and not clicked from e-mail.

"No lunch is Free Lunch" – Any mobile/online tools which are offered free or given free should be dealt or used with much due diligence. Password/ PIN which is used by the originator should be kept confidential with him and not to be shared with any one or through any link online. This will enable the transaction processing to confirm with the confidentiality of the transaction.



Originating/Beneficiary Institution

The transaction traverses from the originator of the transaction to its originating institution which could be the IT systems of any financial institution. Any home, whether it is a hut or a lavish bungalow, should have a lock and key. Similarly, any IT system, which could be state-of-the-art or of the legacy technology, should be secure with tight security controls. The secure controls shall ensure the integrity of the transaction cycle.

Integrity ensures maintaining the consistency, accuracy, and trustworthiness of data over its entire life-cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered in an unauthorized manner.

Processing Agency

Most of the digital transactions pass through a central nodal agency which could be either NPCI, Mumbai (National Payments Corporation of India) or IDRBT, Hyderabad (Institute for Development and Research in Banking Technology).

The IT architecture of the financial institutions which are interacting online with these systems shall conform to the Standards and Procedures as stipulated by these nodal agencies. The availability of the systems across these parties are ensured by the nodal agency.

Beneficiary

Beneficiary shall be comparatively less Cyber-responsible since this entity receives funds. The only caution which beneficiary should follow is to share the correct account number/IFSC Code or VPA (Virtual Payment Address) to the originator.

Various measures as discussed below are being taken by the

Government of India to strengthen the Cyber Security in the complete digital eco-system on a continuous basis.

National Cyber Security Policy, 2013 (NCSP)

National Cyber Security Policy was released in 2013 as a formalized step towards cyber security by the Ministry of Communication and Information Technology under Department of Electronics and Information Technology.

The Policy has been built to offer a secure and resilient cyberspace for citizens, businesses and the Government. Its mission is to protect cyberspace information and infrastructure, build capabilities to prevent and respond to cyber-attacks, and minimise damages through coordinated efforts of institutional structures, people, processes, and technology.

Few Strategies adopted by the Policy include:

- Creation of a secure cyber ecosystem through measures such as a national nodal agency, encouraging organisations to designate a member of senior management as the Chief Information Security Officer and develop information security policies.
- Creating an assurance framework for IT and security.
- Encouraging open standards
- Strengthening the regulatory framework coupled with periodic reviews, harmonization with international standards, and spreading awareness about the legal framework.
- Creating mechanisms for security threats and responses to the same through national systems and processes.
- National Computer Emergency Response Team (CERT-in) functions as the nodal agency for coordination of all cyber security efforts, emergency responses, and crisis management.
- Securing e-governance by implementing global best practices, and wider use of Public Key Infrastructure.
- Protection and resilience of critical information infrastructure with the National Critical Information Infrastructure Protection Centre (NCIIPC) operating as the nodal agency.
- To promote cutting edge research and development of cyber security technology.
- Human Resource Development through education and training programs to build capacity.

Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre)

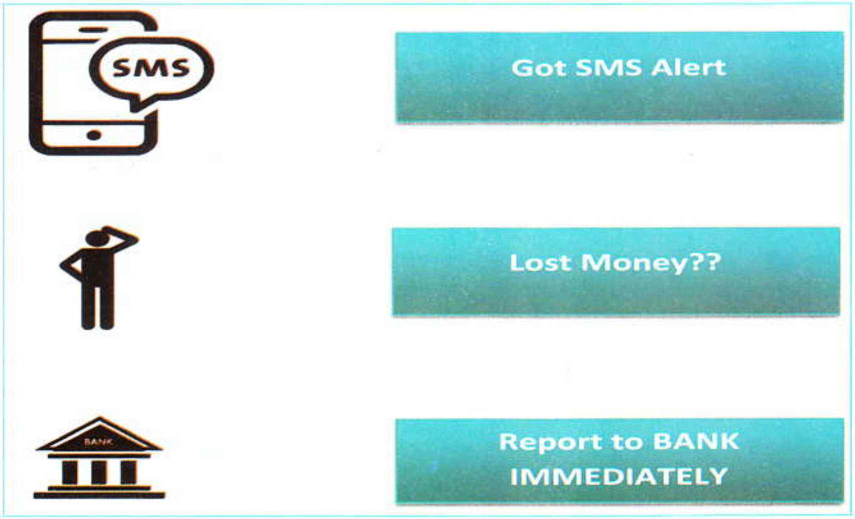
To combat cyber security violations and prevent their increase, Government of India's Computer Emergency Response Team (CERT-in) in February 2017 launched 'Cyber Swachhta Kendra' (Botnet Cleaning and Malware Analysis Centre). The centre has designed new desktop and mobile security solutions for cyber security.

The Centre is operated by CERT-in under Section 70B of the Information Technology Act, 2000. The solution, which is a part of the Ministry of Electronics and Information Technology's Digital India initiative, will detect botnet infections in India and prevent further infections by notifying, enable cleaning and securing systems of end-users. It functions to analyze BOTs/malware characteristics, provides information and enables citizens to remove BOTs/ malware and to create awareness among citizens to secure their data, computers, mobile phones and devices such as home routers.

The Cyber Swachhta Kendra is a step in the direction of creating a secure cyber ecosystem in the country as envisaged under the National Cyber Security Policy in India.

The Centre offers the following security and protective tools:

- USB Pratirodh, was also launched by the government which is aimed at controlling the unauthorised usage of removable USB storage media devices like pen drives, external hard drives and USB supported mass storage devices.
- An app called Samvid was also introduced. It is a desktop based Application Whitelisting Solution for Windows Operating System. It allows only pre approved set of executable files for execution and protects desktops from suspicious applications from running.
- M-Kavach, a device for security of Android mobile devices has also been developed. It provides protection against issues related to malware that steal personal



data and credentials, misuse Wi-Fi and Bluetooth resources, lost or stolen mobile device, spam SMSs, premium-rate SMS and unwanted / unsolicited incoming calls.

- Browser JSGuard, is a tool which serves as a browser extension which detects and defends malicious HTML and JavaScript attacks made through the web browser based on Heuristics. It alerts the user when he visits malicious web pages and provides a detailed analysis threat report of the web page.

Information Technology Act

IT Act, 2000 is the primary law in India dealing with cybercrime and electronic commerce which had subsequent amendment in the year 2008.

IT Act describes the following:

- Digital and Electronic Signature.
- Electronic Governance.
- Attribution, Acknowledgement Despatch of Electronic Records.
- Secure Electronic Records and Secure Digital Signatures.
- Regulation of Certifying Authorities.
- Electronic Signature Certificates.

The description of the electronic offences and the Penalty are detailed in the IT Act for the offences given below:

- Tampering with computer source documents.
- Hacking with computer system.
- Receiving stolen computer or communication device.
- Using password of another person.
- Cheating using computer resource.
- Acts of cyber terrorism.
- Failure to maintain records.
- Failure/refusal to comply with orders.

- Failure/refusal to decrypt data.
- Securing access or attempting to secure access to a protected system.
- Misrepresentation.

Online Frauds and IT Act

IT act has detailed the various cybercrimes and also specified the penalty for the cyber wrong doings by fraudsters online. Phishing is the most common banking fraud which happens online.

Phishing

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

The following Sections of the Information Technology Act, 2000 are applicable to the Phishing fraud:

Section 66 - Hacking with Computer system

If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.

Penalty for this section is imprisonment up to three years, or/and with fine up to ₹500,000.

Section 66 B-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.

Imprisonment up to three years, or/and with fine up to ₹100,000 would be the penalty for the same.

Section 66 C-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 shall be the penalty

Section 66 D-Cheating using computer resource

If a person cheats someone using a computer resource or communication, the imprisonment is up to three years, or/and with fine up to ₹100,000.

Credit Card Fraud

Credit Card Fraud is another online banking fraud where a customer's card is spoofed and the same is used online. In this fraud also IT Act and IPC rescues the victim and assures penalty from the fraudster.

The below Sections of IT Act shall be applicable:

- Section 66 - Hacking with computer system
- Section 66C-Using password of another person
- Section 66D-Cheating using computer resource

Section 420 of Indian Penal Code is also applicable for Credit Card fraud which deals with cheating and dishonestly inducing delivery of property. The maximum punishment which can be awarded is imprisonment for a term of 7 years and fine.

Even though a customer has the aforesaid protections under IT Act 2000/2008, RBI has also directed all banks in the country to re-assure protection against cyber frauds.

RBI Directions

Reserve Bank of India has given directions to protect interests of the customer in its circular on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions.

RBI has thrust upon 'Zero Liability' and 'Limited Liability' for bank customers against any fraud provided if the same is reported to the bank immediately.

A customer will have zero liability in respect of a fraudulent transaction if there is contributory fraud or negligence on the part of the bank. The customer will also not be liable if there is a third-party breach, without bank involvement, which is reported to the bank within three working days of receiving communication regarding the unauthorized transaction. Also, the defrauded amount shall be credited in the accounts concerned within 10 days.

RBI has made it mandatory for banks to register all customers for text message alerts and permit reporting of unauthorised transactions through a reply to the alert message. This shall alert the customers on the frauds instantly.

Banks shall enable reporting of unauthorized transactions on their website itself for easier customer grievance redressal. Fraud can be reported through any of the channels, including phone banking, SMS, email, call centre and interactive voice response systems.

However, in cases where the loss is due to negligence of the customer, he/she shall have to bear the entire loss until he/she reports the unauthorized transaction to the bank.

In case of loss caused by a third party, the customer will be liable for the transaction value if he fails to report the fraudulent transaction within 4-7 days of receiving the alert from the bank. In case the fraud is reported within 4-7 working days, a customer's maximum liability will be from Rs. 5,000 to Rs. 25000, depending on the type of accounts and credit card limit.

Wrap Up

With all the measures towards strengthening of Cyber Security, our country shall provide a completely Cyber Secure architecture that is secure and reliable for the digital transactions. However, it is to be continuously upgraded, as new threats emerge. Security is a journey. Awareness will enable to face and mitigate the risk. □

(E-mail:mdsec@iob.in)

Integrated Command & Control Center Projects Being Developed in 20 Cities

The Integrated Command & Control Center projects which enable fast and efficient citizen service delivery in an integrated way, are being developed in 20 cities and are already operational in cities like Pune, Surat, Vadodara, producing positive results. 10 more cities have issued tenders for developing command and control centers in their cities. For smart reuse and wastewater projects, 33 cities have issued tenders, and work has begun in 16 of them. In order to promote renewable energy usage in the cities, projects for providing solar projects on rooftops of government buildings have been encouraged. Till date, 44 cities have issued tenders, and work has begun in 38 cities

City-wise service level improvement plans (SLIP) for all the 500 cities and State Annual Action Plans (SAAP) for all the 36 States/UTs with a project investment worth Rs. 77,640 crores were approved. Under AMRUT, 215 projects worth Rs. 157 crores have already been completed, 1606 projects worth Rs. 32,459 crores are at various stages of implementation and about 1800 projects worth Rs. 23, 568 crores are under tendering stage.

Details of the three-tiered approach being followed by the Ministry of Housing and Urban Affairs for states and cities to implement the reform Agenda are as follows: "First Tier: the performance grant of the 14th Finance Commission of about Rs 18000 Crore is used to accelerate on-going key financial and service level reforms in cities. The 14th Finance Commission gave recommendations for assured transfers to Local Bodies for a period of five years (2015-16 to 2019-20). A total of Rs. 87143.80 crores will be transferred to Municipalities during the award period. Second Tier: AMRUT Reforms consisted of launch of 11 Urban Management and governance reforms comprising of 54 milestones. These reforms have been achieved by all the States / cities. Hence five more have been added to the new list of AMRUT New Reforms which included Value Capture Financing, credit rating and Municipal bonds, municipal cadre professionalization, trust and verify approach for frontline services like building permissions and land titling. Third Tier: Incentive fund with a focus on 'rapid' and transformational reforms along the three main pillars: governance, planning, and financing focusing on strengthening devolution, own source revenue mobilization, and flexible urban planning. These reforms will enhance downstream accountability mechanisms like making local ward committees responsible for O&M of projects etc.