VOLUME-6, ISSUE-7, JULY-2017 • ISSN No 2277 - 8160 IF : 4.547 | IC Value 80.26

Original Research Paper Commerce

INTERNET AND SUPPLY CHAIN MANAGEMENT OF INDIAN BANKING SYSTEM

Sri. Kaith Garib Dass I.P.S 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

This paper is purpose of only research. This topic covers of Internet and providing of online distribution of digitalized products. This helps in quick turnaround reach to a large number of customers and eliminates the lead time between the place of order and delivery. This also enables a better inventory management and quicker transaction processing. Many enterprises have started using the new concept called Enterprise Resource Planning (ERP) systems. E-distribution (cyber distribution) activities when linked to these ERP systems assist the companies to achieve a greater efficiency in their entire Supply Chain Management.

Cyber Marketing: Limitations:

Internet marketing is also exposed to quite a few problems. Some of them are in-built and others are external problems.

1. Digitization: For cyber marketing, the products should be in digitized format. This process requires manpower, skills and technical knowledge. The digitization is one of the issues faced by e marketing.
2. Shopping experience: Customers especially in India are more used to touch and feel experience as against click and view mode of shopping.
3. Cyber crimes: Despite the popularity of internet and e commerce and e-marketing, on account of different cyber crimes users are concerned about e marketing.
4. Security: While shopping on internet, customers are required to furnish sensitive personal data which are being shared by marketing companies and create inconvenience to the customers and also pose threats to their privacy.

KEYWORDS : Enterprises Resources Marketing

While customers can have faster access to information and details about the range of products, customers are cautioned to be careful on account of various issues and risks associated with cyber marketing. In today's fast growing e commercial activities, banks' role is very important for the success of global e- commerce. e-commerce should be end to end covering various aspects like from the customer's end, the selection of on line products, placement of orders, and making and settling payments.

An effective global payment channel should be an integral part of global e commerce. Before setting up a global payment channel, an organization should consider certain aspects such as

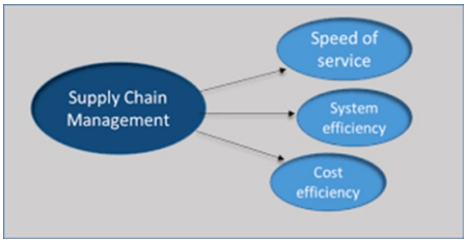
1. Payment Type: Payments can be made through different modes like credit cards, debit cards, or online transfer. Customers should be allowed to choose any of the method to settle payments. Internal checking and balancing act should be embedded into the system
2. Legal frame work/Regulatory compliance: The system should satisfy the legal and regulatory requirements in the centres
3. Taxes: Taxation laws are different in different countries. The payment system should have the capability to calculate and compute the required taxes, duties as per the local tax laws
4. Banking relationship: Global e commerce involves cross border trade activities and to ensure prompt settlement of payments, the system should be supported by the banks to process these payments. As per the rules and procedures applicable at different centres, the payment system should be supported by well established banks.
5. Risk: Global e commerce is subject to risks. On-line payment risks can be classified into:

Credit Risk: The customer may not have sufficient funds to make payment

Fraud: Payments may be made on a misrepresented identify

Repudiation: The customer may refuse to honour payment

Security: Global e commerce is exposed to various cross border nations, hence it is subject to different laws and regulations. Therefore, the payment system should be able to handle the country specific security regulations/guidelines.



Source :Google images

An efficient global payment processing system should have the following features;

- A single system should enable national and international payments
- It should be able to support multi=currency and multi= payment types
- The processing facility should be active for 24 x 7
- The system should be able to handle the high value transactions Interface facilities should be available in the system to enable the system in switching to one type of payment to another like (Real Time Gross Settlements (RTGS) Automated Clearing House (ACH)
- Inter connectivity with message switching systems like SWIFT should be part of the system
- It should also be able to handle current and future inflow/outflows
- Importantly, it should have the feature and facility to comply with the regulatory requirements

Risks:

Some of the important risks associated with payment systems are:
Credit Risk:Failure by a party to meet the financial obligations
Liquidity Risk:A party in the system fails to pay on account of

insufficient funds

Operational Risk:A risk can arise on account of human error, system failure, frauds etc.

Legal Risk:Non compliance of legal or regulatory framework can create a legal risk

Systemic Risk:It can have a chain effect into the system due to the default of one of the parties

Legal frame work:
The following Acts and Regulations handle the payment and settlement in India:

1. The Payment and Settlement Systems Act 2007

2. The Payment and Settlement Systems Regulation 2008

3. Board for Regulation and Supervision of Payment and Settlement Systems Regulations 2008

Sources :Google images

International Initiatives: Bank for International Settlements (Basel) has taken many international initiatives to ensure global financial stability. It is also taking actions to strengthen the global financial infrastructure. According to the Committee on Payments and Settlement Systems (CPSS), the core principles for a controlled payments and settlement systems are:

1. The system should be based on a clear legal framework under all relevant jurisdictions
2. All participants should be able to clearly understand the system's rules and procedures. There should be clarity regarding system's impact on each of the financial risks
3. Credit and liquidity risks are important risks in an e-commerce environment. Hence banks Payment systems should cover the area of credit and liquidity risk management
4. Liquidity management depends upon timely settlement of funds. In view of this, banks' settlement systems should ensure that settlements take place without fail on the value dates (during the day and/or definitely at the end of the day. In case of multilateral netting, at the minimum, the system should be able to complete daily settlements in case the participant of a single big ticket transaction is unable to make the settlement
5. The system should have an integrated high degree of security and operational reliability
6. The system should have a backup system to handle any contingency situations for timely completion of daily processing

Role of Central Bank in Payment Mechanism

The central bank of a country is responsible in applying the core principles for ensuring that an efficient and cost effective payments system is in place.

The central bank should:

1. Clearly define the payment system's objectives and should publicly disclose the role and major policies in respect the payments system
2. Ensure that the system is operating efficiently as per the core principles
3. As supervisor and facilitator oversee that banks comply with the system's core principles.
4. Co-ordinate and co-operate with other central banks for effective implementation of the payments system

RBI as the central bank plays a pivotal role in ensuring that a payment and settlement system is established in conformity with the international standards. Some of the initiatives taken by RBI in introducing different models

RBI has been very active in introducing new systems to take care of changing environment and also to safe guard the interest of bank customers, banks, financial instiutions,traders, and others. RBI also ensures that the payment and settlement systems operating in India are safe, secure, efficient, accessible and authorised. In addition to the above, RBI played a key role in the establishment of the Clearing Corporation of India Ltd (CCIL), a central organisation that settles transactions relating to government securities and foreign exchange transactions.

(INFINET) INdian FInancial NETwork- INFINET is the communication backbone for the Indian banking and the financial sectors. All banks in the public sector, private sector, co-operative etc. and the premier FIs in the country are eligible to become members of INFINET. It is a closed user group network for the exclusive use of the member banks and FIs and is the communication backbone for the National Payments System which caters to inter-bank applications like RTGS, Delivery vs. Payment, Automated clearing house, Government Transactions etc.

Integrated Communication Network for Banks Security and Control Systems

Banks in line with the IT and communication technology revolution and also to maintain better customer relationship management, offer core banking solutions, new on line payment systems like credit cards, debit cards, internet banking services, etc. While this technology based services offered by banks are better and quicker financial services/products, the banking operations are subject to many risks like cyber crimes. Cyber laws through the legal frame work, based on the Information Technology Act, 2000 aimed to setup a sound infrastructure guidelines and rules for e commerce activities through internet. The purpose of IT Act, 2000 is to promote the use of digital signatures for the growth of e-Commerce and e –Governance. It recognizes the digital signature in e-Commerce. The Act allows that any subscriber may authenticate an electronic record by affixing his/her digital signature. IT Act 2000 covers number of aspects relating to e-commerce and several cyber crimes like cyber terrorism, phishing and child pornography.

Digital Certificate and Digital Signature

Digital certificate is an electronic identity provided to an entity by a competent authority or a certification authority. It is a unique public key provided to each entity for establishing the entity's authenticity

Digital signatures: As per Sec 2(1) (p) of the Act a digital signature means an authentication of any electronic record by a subscriber by means of an authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the other provisions of the Act

Cyber crime and fraud management

Technological revolutions both in communication and information technology have changed the way of doing business. In today's 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.

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"

In cyber crimes, computers are either used as tools and/or targets. So the computer which is an electronic devise is used as a medium of cyber crimes.

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. Since information technology drives the functioning of corporate, individuals, banks and government departments and other professionals, the storage of unprotected sensitive data and information in their computers pose a significant threat.

References

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