A STUDY ON E-COMMERCE AND ELECTRONIC SECURITY

Lalit Kumar*

Nikhil Patel**

ABSTRACT

E-commerce has revolutionized the business environment by developing the digital economy that enhances value to consumers and improves the efficiency of business operations. However, optimizing the influence of e-commerce depends on the environmental context of industries and individual firms.

The information revolution has provided part of the world's population with a de facto information superhighway that we know as the Internet. Use of these networks for on-line purchases and some transactions forms just part of the growth in global electronic commerce (e-commerce), which is actually a broader use of information technologies by business and government.

Any e-commerce on the Internet becomes potentially subject to interception, tracking or attack and thus warrants the use of cryptography to code transmissions for security and privacy. The encrypted data becomes reasonably secure assuming safe handling at each end. Whether or not government or organizations should have access to encrypted transmissions is a current argument. There is a need for digital certificates to establish the authenticity of on-line users and also a Public Key Authentication Framework for security.

E-commerce is in its boom everywhere and India is no exception. All businesses whether they are small or big have their websites. But e-commerce is much more than just buying and selling over the Internet. According to Robert J. LeBlanc, Vice President Software Strategy, IBM, having a Web site doesn't mean you're ready for e-Business. Today e-Business is about using Internet technologies to transform key business processes. It's about strengthening relationships with stakeholders...capitalizing on new business opportunities...increasing efficiency...and becoming more customer-centric.

Choi, Stahl and Whinston (2002) found business-to-business activities in electronic commerce include:Internal electronic mail and messaging, online publishing of corporate documents, online searches for documents.

Companies are using electronic commerce to enter new markets that would have otherwise been excluded from due to geography, cost, or other reasons. Companies look to electronic commerce to extend their products to new sets of customers and new parts of globe. The Web enables a company to introduce a new product into the market, get immediate customer reaction to it, refine and perfect it, all without incurring huge investment in a physical distribution infrastructure or buying a shelf space at a retailer of distributor.

Key words- *E-commerce, information technologies, organizations, physical distribution.*

*Lecturer,Dept of Computer Science

*M.M.Engineering College,M.M.University, Mullana,Ambala,Haryana,India**.**

INTRODUCTION

The new concept of electronic commerce (e-commerce) is the use of on-line networks to promote or sell products or services. It is also the process of using electronic methods and procedures with information technology as a tool, to conduct all forms of business activity. Electronic commerce utilizes different technologies and forms such as electronic banking and trading, electronic funds transfer (EFT), electronic data interchange (EDI), electronic mail (e-mail), facsimile transfer, electronic cataloguing, video-conferences and multimedia communications and all other forms of sending electronic data messages between enterprises. Earlier applications of EDI were too costly and complex to succeed. The use of smart cards adds a further dimension to enable on-line transactions around the globe.

E-commerce allows users to exchange goods and services electronically with no barriers of time or distance. Electronic commerce has expanded rapidly over the past five years in many countries and should continue to proliferate in the business context. In the near future, there would be a blurring of boundaries between "conventional" and "electronic" commerce as more and more businesses move sections of their operations onto the Internet. With electronic commerce, everything starts out and stays digital; only different applications are needed to transfer and process the data as it winds its way through the whole process flows.

When the concept of electronic convergence arrived earlier this decade, studies outlined likely scenarios for the provision of the new communications systems that linked to information and broadcasting technologies. They identified possible service types for home entertainment, communications services, transactions, business and on-line information. These raised a wide variety of policy issues including matters of the user demand for such services, the level of service access available to the community and of information flows generally. Further considerations included the degree of privacy found on-line, content controls (particularly relating to violence and pornography) and the imposition of taxation to on-line services. Wider issues included the impact on culture, as well as cross media and foreign ownership of the service providers. There also remained a bandwidth management problem, requiring regulation or pricing, and varying standards.

Ecommerce has an edge over traditional commerce." In the future, there will be no distinction between'dotcom'and traditional businesses, just winners and losers. Internet strategies that focus on speed, efficiency and customer experience will mark the winners", says Michael Dell, Chairman & CEO, Dell Computer Corporation.

E-commerce tools that support information management in supply chain and logistics include the Internet, intranet and extranet that support various linkages such as business-to-business (B2B), business-to-consumer (B2C), business-to-business-to-consumer (B2B2C), and other relationship enabled by e-commerce. E-commerce link business collaborates, customers, suppliers, top management or decision-makers, and employees. In the context of shipping, the adoption of e-commerce by shipping companies would enable customers to access updated information on freight charges, schedules, tariffs and delivery or fulfillment time requirements, and other transport cost to enable them to decide on which service to engage from which company. However, from the perspective of logistics, the greatest barrier to the adoption of e-commerce tools is the high initial investment cost. Nevertheless, with expected cost reduction and decreased cycle time, there are various ways of achieving returns on investment. One is faster business processes because information and financial flows accompany the physical goods. This means that information replaces inventory to reduce warehouse costs. Another is the creation of savings from faster business processes causing cutbacks in expenditures on distribution, inventory, and warehouse functions. Business firms do not need to build warehouses since they can utilize the warehouse facilities of suppliers and coordinate delivery through network systems of information exchange. (Kalakota and Whinston, 1997)

ELECTRONIC ENCRYPTION

For some time now, most of us have used electronic transaction systems such as automatic teller machines (ATMs) and electronic funds transfer (EFT). These utilise closed, supposedly secure, networks that are generally safe from interception by using encryption or secure data coding. Digital mobile telephone systems have also employed encryption to help keep private conversations secure. However, their somewhat limited system standard has enabled eavesdropping, perhaps indicating that no technology is totally secure. Information security has objectives including confidentiality (secrecy), data integrity (non-alteration), authentication (identity corroboration of an entity and data origin), and non-repudiation (prevents the denial of previous commitments).

The science of encryption is called **'cryptography',** which, until recently, had been largely the preserve of secret defense intelligence agencies, spies and diplomatic officers. Encryption transforms data by the use of cryptography to produce unintelligible (encrypted) data to ensure its confidentiality. The inverse function of decryption then converts transmissions back to normal form. Cryptography is the study of mathematics related to aspects of information security while cryptology is the study of cryptography. Cryptanalysis is the use of mathematics to crack cryptographic techniques as employed by a cryptanalyst. Cryptographic functions include encryption, authentication and digital signatures, while cryptographic tools are ciphers, hashes, codes and signatures. Computer ciphers have two parts: a method, or algorithm, plus a key number for access. Cipher algorithms change symbols or strings of data. In traditional coding, both parties to a secret message had to firstly share a private password or key in order to cipher or decipher their messages. The sharing of this key was in itself a weakness of the system if any other party could get hold of the key. In the 1970s, scientists devised a way of splitting the key into two parts, one public and one private, linked by a complex mathematical relationship. Now it was possible for one party to release a 'public key' to all other parties, to enable them to encipher messages but only the holder of the 'private key' could decipher them upon return. With computing advances, the ability arose of including such complex cipher routines in ordinary software. Sophisticated cryptographic software now enables almost any computer user to encode their transmissions for security. There are many forms of encryption available that help make e-commerce transactions reasonably secure.

To enable Internet users to establish their credentials for any transactions, the concept has arisen of 'digital certificates or signatures'. These are software packages containing personal references and a private key. A digital signature is a number dependent on some secret known only to the signer and on the signed message content. To create a digital signature, users begin with an electronic message and hash it, that is, calculate a number using the contents of the message.

The public key certificates are a means by which public keys may be stored, distributed or forwarded over insecure media without the danger of undetectable manipulation. This allows one's public key to be made available to others such that its authenticity and validity are verifiable. Nonetheless, a weakness remains at each end of the secure communications where the message and or private keys might be revealed or available to third parties, or included within software. A further weakness is the ability of advanced computer systems to work out the mathematical formulae defined in keys and thus decode messages within a reasonable time. This is achieved by trying every possible combination of bits of information until the code is broken.

A new technique for sending secret messages involves digital authentication and not message encryption. Called 'chaffing and winnowing', the technique splits the message into tiny pieces. Each of these data bits are labelled with a number and digitally signed before being interspersed with nonsense data that also has numbers and appears to be signed. Only the correct authentication key can separate or winnow the wheat of the message from the chaff.(16) Maybe this will serve as the ultimate encryption technique to preserve individual privacy and security on the Net. This also shows that any regulatory attempts to thwart encryption use may well be bypassed in future.

Key escrow is a system to provide encryption of user traffic such as voice or data so that the session keys used are available to properly authorised third parties under special access circumstances. Law enforcement agencies promoted the concept while other uses might be for recovery of encrypted data following its loss or destruction due to equipment failure. The United States Escrowed Encryption Standard involved a computer ('Clipper') chip with a unique identity number and a two-piece secret key stored by two different agencies. However, users can already backup keys and there is no guarantee for liability or that any escrow agency itself is trustworthy. Thus, key escrow appears dead, bypassed by the widespread availability of encryption products. However, key backup is useful for good management reasons in applying to archival data.

Authentication

'Certification' is the endorsement of information by a trusted entity. A certificate consists of a data part and a signature part binding identity to a key number. However, a system is needed to authenticate the identity of public key holders, as otherwise, illicit organisations might distribute sham public keys among users. Major risks include corruption, errors, criminal hacking and the organisation's vulnerability. This requires a public key authentication authority (PKAF) as a separate public or private organisation to vouch for each identity and the public key.

'Smart cards' are credit card like, portable, plastic envelopes encasing an integrated circuit, that combine personal digital certificates and private keys within the sealed confines of an electronic chip. Smart cards have uses as 'stored value cards', with money stored as an electronic value in the chip, and/or as applications run from the card's computer chip. Loaded with information and/or electronic cash protected by an encryption scheme, smart cards may be a convenient, versatile medium for business transactions. As stated earlier however, any software package is liable to manipulation so there remains a degree of uncertainty about the security of digital certificates, although this situation also applies to normal written signatures. However, cryptographers have already identified techniques for breaking the security systems built in smart cards. They cracked the codes by monitoring power consumption as the card circuits performed cipher operations. Hackers can use less expensive equipment to monitor a smart card's electronic responses and hence gain user electronic account access as long as they have a card to examine. More devious means of using smart cards may involve viruses or malicious key copies.

Purses contain **digital certificates** for on-line use as a form of digital cash or coins or **electronic cash (e-cash)** and stored value money cards. Such a card with value of up to a few hundred dollars need only be reasonably secure compared to digital certificates and may provide for anonymous transactions. Digital coins or electronic e-cash are like bank notes with a message signed by the issuer that specifies the issuer, value, expiry data, serial number and the Internet address of the issuer, all as a digital signature. Using blind signature technology, a technique that hides the document content from the user, the customer chooses the serial number and then blinds it. The coin issuer signs the blinded version and returns it to the customer who then un-blinds it. This protects the payer's identity and prevents any double spending. There may also be other similar techniques.

The **Secure Electronic Transaction/Trading/Technology (SET)** is a proposed industry standard for payment card acceptance over the Internet. At the system heart is a pair of digital keys, one public and one private, held by each party to a transaction. In practice, banks will give both keys to a customer together with a digital certificate for authenticity. When customers wish to purchase over the Internet, they firstly give the public key to the merchant along with the certificate to prove its authenticity. Likewise, the merchant provides its own public key and certificates to prove its own bona fides to allow the transaction to proceed. Problems may arise in key distribution and customer identification in order to ensure that accounts and clients match.

THE BUSINESS BATTLE FOR E-COMMERCE CONTROL

Credit Cards versus On-line Banks

The development of different types of electronic money could have considerable impact on e-commerce growth and may not necessarily involve any government agencies. There may be a new era of free banking, where privately issued currencies compete with legal tender as the preferred medium of exchange. These new currencies may be in market determined units to allow versatility, security, low cost and privacy. Such development along with any erosion of government revenue bases and possible law and tax avoidance, means that an appropriate regulatory framework must be achieved.

Industry Codes of Practice

Modern business has to consider e-commerce security strategies just as it has ever since credit card numbers were accepted over the telephone without signatures. Business has to consider external and internal threats, encryption, enterprise authentication, firewalls, virtual private networks, SET and e-cash through risk assessment. According to media reports, the information industry faces uncertainty due to the lack of a detailed national electronic signature scheme. In general, the wide variety of corporate initiatives undertaken to facilitate e-commerce, have only resulted in different standards, software quality and security levels. However, a number of industry codes of practice exist.

The **Smart Card Industry Code of Conduct** deals with the collection and handling of personal information and consumer protection. The Code establishes minimum standards of practice for the collection, use, storage, security and disclosure of information by smart card vendors. Code participants must also recognise privacy principles. The privacy issues posed by smart cards fall into categories of loss of anonymity, information collection and the potential for them to develop into a national identification card.

Privacy on the Net

Successful e-commerce depends upon proving the identity of persons on-line and linking them to a transaction without repudiation. It must prevent system access by unauthorized persons and computer applications, while preserving privacy and security. Since e-mail is transmitted in plain text over unknown pathways, residing for various periods on computer systems, it allows illegal scanning of message contents using filter software. An additional e-mail problem is the easy ability to forge sender or recipient identity. While personal data might be kept private in one country, any trans-border flow may not be secure upon the transmission to another nation. Surveys of attitudes to privacy on-line consistently reveal that the majority of Internet users remain unconvinced that their on-line transactions are secure.

Cyberspace Crime

There are many aspects to crime on the information superhighway. These range from illegal interception, theft or piracy of telecommunications services, to telemarketing fraud and transmission of offensive materials. Electronic vandalism and terrorism, electronic funds transfer crime and money laundering are further problems. The extent of such telecommunications related crime tends to defy detection, quantification or territoriality. Law enforcement agencies may need special powers and initiatives to counter such crime.

Cyberbetting' or Internet gaming is an interactive and growing business that uses a browser to provide client access to different types of real or virtual gambling and betting systems. While the United States and Singapore have acted to prohibit such activities, other governments such as those of Queensland and the Northern Territory have legalized them, with regulations to license operators within consumer protection guidelines. There appears to be some technological capacity to control or ban on-line gaming but any national legislation would have to consider the relevant financial, telecommunications and foreign affairs implications. It is not difficult to conceive of criminal activities associated with cyberbetting.

LITRATURE REVIEW

- Rodgers, Yen and Chou (2002) provided that e-commerce establishes links among business partners, suppliers, employees and customers through three online systems, the Internet, intranet and extranet. The Internet enables product offering and service delivery together with the related transactions through online venues such as websites. Intranet systems connect employees by giving them a way of accessing and sharing information through a network system exclusive to the company. Intranet systems similarly operate as interactive, transactional and information-sharing systems but limited only to the members of he business firms. This operates based on the assumption that informed employees decide, act and perform better.
- Greenstein and Feinman (2000) identified vision as one success factor for e-commerce. Integration of e-commerce into the vision of a business firm guides organization-wide action towards the achievement of e-commerce. This means that performance depends on the extent of achievement of e-commerce objectives. The vision of a business firm determines the key parties, the respective contributions of these parties, the activities and competencies needed, and the expected results. Thus, the vision of a firm comprises the underlying basis for the e-commerce initiative.
- Follit (2000) identified leadership as another success factor for e-commerce. E-commerce comprise a business innovation, there should be a champion for e-commerce in the company to influence the acceptance and cooperation to the adoption of e-commerce as a business solution. It is important for the leader to assume a strong position in directing the e-transformation of the business. The e-commerce leader should hold a strong position in controlling the e-transformation of the organization to ensure the effective adoption of e-commerce.
- Corbitt (2003) identified corporate culture as another success factor in e-commerce adoption. In adopting e-commerce, change in corporate culture and the concurrent change management strategy are requirements in ensuring the alignment between the requisites of e-commerce and the norms, practices and values of the organization in using online tools to facilitate business processes. Culture change requires a shift in the view of managers and employees over e-commerce tools relative to their work and the performance of the business. Without a change in perception, e-commerce tools would

not likely receive the acceptance and enthusiasm needed for the effective use of e-commerce in achieving goals.

- Marzulli (2000) also identified the aggregate of strategic planning, corporate communication, and organizational flexibility as another success factors in adopting e-commerce. Planning enables businesses to identify objectives, anticipate potential problems, and develop contingency solutions. Corporate communication secures acceptance and cooperation by making sure that all managers and employees understand the importance of e-commerce to the business. Flexibility supports the capability of business firms to adjust to the changes needed in adopting e-commerce.
- Nickles (2000) identified security problems as another challenged faced by business firms in engaging in e-commerce. The extent of security depends on the extent of investment in e-commerce and the selection of the appropriate components of he e-commerce initiative. Some actions could be considered to ensure that companies address the security problem.

Methodology

E-commerce (electronic commerce) solutions bring the open standards and universal access of the Internet to the core business processes of buying and selling goods and services, integration and link up all related parties in one similar industry. The methodology reflects these three areas.

Research Design

Mixed method combining the qualitative and quantitative study was the research design applied in the study. Mixed method enables the achievement of both completeness and confirmation values. This design combines qualitative and quantitative data and retains the validity component of these two types of data to achieve a high validity.

Method of collection

Primary data collections are done by the interviews and Observation of the current scenario and identification of surroundings sensitive issues emerging from e-commerce with proper questionnaire.

Secondary data has been collected from different publication material and web site as well as the books and material from different libraries, the hand note of the various seminar and research related to the issue are taken into account.

The study was carried out in India and the focus in this study was on the different companies in India. As the research was aimed to study characteristics of the e-commerce companies' top-level management is most concerned with it. So only CEO, MD or GM was interviewed from each organization. The size of sample for study is 150**.** To make the sample more authentic and representative Indian brand companies were randomly selected.

OBJECTIVE

- To identify key characteristics of the firms engaged in e-commerce in India
- Determining the change in policy to foster the effective adoption of e-commerce tools as part of competitive strategy.
- To ensure information security to the firms using in e-commerce to be competitive in the market.

CHALLENGES

- The challenge is to identify the areas requiring resolution to ensure a successful e-commerce initiative.
- Cost consideration poses a strong challenge to business firms that could dissuade business firms from engaging in e-commerce even with expectations of great potential benefits to the business firm.
- Security problem is another challenge faced by business firms in engaging in e-commerce.

CONCLUSION

E-commerce is in its boom everywhere and India is no exception. All businesses whether they are small or big have their websites. But e-commerce is much more than just buying and selling over the Internet.

Today e-Business is about using Internet technologies to transform key business processes. It's about strengthening relationships with stakeholders...capitalizing on new business opportunities...increasing efficiency...and becoming more customer-centric.

Concentrating on software selling firms in India what researcher endeavor to do in this research is

1. To examine the growth of e-commerce in both physical and financial terms.
2. To identify key characteristics of the firms engaged in e-commerce.
3. To conduct constraint analysis of e-commerce and
4. To develop a strategic plan for effective dissemination of e-commerce in India.

A typical software company has static web pages, fast access website and automation at backend, while it does not have provision to calculate price performance ratio before selecting hardware or software. It does not use aesthetics in designing its website.

In this research it was found that a typical Indian software company has its base in a metropolis, strength of employees more than hundred, capital investment more than one crore and is limited company. It has online display of product information, company profile and no online display of price information, a dealer/wholesaler directory and its website is not linked to industry trade associations and other data sources.

In technical features a typical Indian software company has static web pages, fast access website and automation at backend, while it does not have provision to calculate price performance ratio before selecting hardware or software. It does not use aesthetics in designing its website.

REFERENCES

1. C. R. Blackman, 'Convergence between telecommunications and other media: How should regulation adapt?', Telecommunications Policy, vol. 22, no. 3, April 1998.

2. P. Budde, Information Technology Management Report 1997, Paul Budde Communication Pty Ltd, Bucketty, 1997.

3. M. L. James, 'Wait - there's more: the Internet on your very own home television!', Research Note no. 24, Department of the Parliamentary Library, Parliament of Australia, Canberra, February 1997.

4. Kalakota, R., and Whinston, A. (1997). Readings in Electronic Commerce.

5. Journal of Business Logistics. 13(2). Retrieved January 29, 2009, from http://www.fedex.com/us/services/logistics/create.html.

6. Journal of Information Management. 18(1), 1-27.

7. Smith, J. (1994). Managing Privacy: Information Technology and Corporate

8. Wong, P. K. (1998). Leveraging the Global Information Revolution for Economic

9. Development: Singapore's Evolving Information Industry Strategy. Information Systems Research. 9(4), 95-117.

10. Zott, C., Amit, R., & Donlevy, J. (2000). Strategies for value creation in e -commerce: best practice in Europe. European Management Journal, 18(5), 463-475.