Security issues involved in doing business through electronic mode

Dr. Pradipta Banerjee
Assistant Professor, Department of Commerce
Sidho-Kanho-Birsha University, Purulia, West Bengal-723104

Abstract

Electronic commerce (e-commerce) has emerged as the major technological development in the corporate world which has revolutionized the way of doing business and opened up a new vista in the corporate world. The growing application of internet and intense advancement of information and communication technologies, have made access to global market from anywhere and at any point of time through computer screen irrespective of geographical location of the consumers and corporate boundaries. More and more consumers of today's world are indulging in electronic transactions for their dealings to enjoy the litheness, liberty and convenience of purchasing products and services. To cope with the changing trend of the modern consumers, organizations around the globe are offering e-commerce platform for trading on their goods and services and developing innovative ideas and newer business models for doing business over internet for attracting customers, sustaining in the value chain and achieving competitive advantage. But, at the same time, it has imposed major security risks and threats to the business houses as information exchanged through internet consists of valuable, confidential and business critical corporate data as well as confidential information of the customers. In order to ensure proper security of customers and also to secure corporate database, entire business process and image of the company, developing proper security arrangements is very much needed both at server and network levels. Moreover, as the cyber criminals are persistently inventing newer ways of committing cyber crimes, it has appeared to be a real challenge to the business houses to maintain the proper security in doing businesses through e-commerce mode in particular and capitalizing the advantages of e-commerce in building a competitive edge to the organization.

In the present paper besides some preliminary discussion on concept, types, models, etc. of e-commerce, security issues involved in doing business through e-commerce mode have been outlined encompassing different factors in e-commerce security, security threats in e-commerce, e-commerce security protocols, levels of e-commerce security and how structured management strategies can be developed to investigate security risks and handle such risks with the objective to minimize the security threats to the organizations.

Keywords: E-commerce, security threat, server level security, network level security, cybercrime.

Introduction:

The term 'e-commerce' or 'electronic commerce' basically refers to buying and selling products and services electronically over internet and other telecommunication networks through electronic processing and transmission of digitized data including text, sound, image and video. IBM defines e-commerce as 'the transformation of key business processes through the use of internet technologies. E-commerce is about using technology to streamline business models, creating savings and increasing efficiency. It is about lowering cost and establishing closer, more responsive relationships with your customers, suppliers and partners.' The present day's e-commerce is defined as the internet enabled Electronic Data Interchange (EDI) which was developed in early sixties. The EDI resulted in paper-less environment by providing corporate houses a means of performing business operations electronically such as purchase order, invoice, payments and other standard business operations using their own electronic networks. Gradually, private networks were replaced by internet and EDI was merged with e-commerce in the mid nineties. Due to immense advantages of e-commerce both from the view of buyers and sellers such as easy access to global markets without any barrier of time and geographical location, lower operating cost, better profit margin due to lower operating cost and global operation, shorter delivery time, instant response both from buyer and seller, more transparency in doing business, end-to-end information flow, wider customer base, building customer loyalty, achieving more competitive advantage and many others, business transactions under this mode has grown extraordinarily over the years and its scope also has expanded to other areas like, inventory management, marketing and advertisement, customer service, etc. (though these do not specifically fall under e-commerce rather fall under e-business). Modern e-commerce typically uses the World Wide Web at least at some point in the business transaction lifecycle.

In the present study, along with describing briefly different e-commerce models, security issues involved in e-commerce and dimensions of e-commerce security, how a structured and integrated management strategy can be implemented in an organization to investigate and handle security threats to the organizations has been outlined.

Section II: Different models of e-commerce

A business model is essentially a set of structured processes aiming at achieving specific business objectives. It specifies the mechanism or method of doing business by which a firm can generate surplus and sustain itself. In e-commerce, transactions take place between parties to meet different purposes. There are different models or types of e-commerce transactions and these can either be categorized on the basis of parties involved in the transactions or the functions that it performs. On the basis of parties involved in transaction, e-commerce is classified into the following important models:

Business to Business (B2B): When two or more companies use electronic means for various business transactions among themselves, it is termed as B2B e-commerce. It is the most common e-commerce model that enables different transactions between supporting businesses to meet the customers' need. Examples of B2B transactions are transactions between manufacturers and wholesalers, between wholesalers and distributors, etc.

Business to Consumer (B2C): B2C is the online selling of products and services by companies to customers. This model of e-commerce is extensively used for retailing by manufacturer, distributors, etc. and examples of such transaction are online trading through flipkart, snapdeal, amazon, etc.

Consumer to Business (C2B): In this type of e-commerce, transactions take place between individual consumers and business houses wherein the transaction is initiated by the consumer by specifying the price and specification of required goods and services. After receiving the buying orders, the website channelizes the order to participating sellers and if the seller is willing to sale the product or service at the specified price and specification of the consumer, actual trade executes. It, thus, reduces time involved in bargaining and enhances flexibility of trading both from the view point of the buyers and sellers.

Consumer to Consumer (C2C): It involves online financial interactions between non-business entities in which consumers sale some products and services (usually used items, antique items, etc.) to other consumers directly using web through online classified advertisements and auctions or indirectly through brokers using the web. An example of this type of transaction is selling through OLX site.

Business to Government (B2G): When business houses sale their products and services to government agencies, it is termed as B2G transaction. In B2G, the governments are involved in online procurements through bidding from prospective sellers which results in substantial savings in cost and time.

Business to Employee (B2E): Here business houses offer their products and services to their employees by setting up B2E networks to automate employee related corporate processes.

Mobile Commerce (M-Commerce): An emerging type of e-commerce in present times is the M-commerce in which transactions are made using wireless technology such as mobile handsets and other hand-held wireless devices. The enormous penetration of mobile phones offers a great prospect of m-commerce and poses a different sort of challenges to many industries as well.

On the basis of functionality, on the other hand, e-commerce models are classified as Merchant model, Subscription model, Advertising model, Brokerage model, Affiliate model, Utility model, Infomediary model, etc.

Section III: Security issues involved in e-commerce

The advent of e-business has posed new risks to business organizations due its dependence on open access electronic and communication channels. In fact, the strengths of an e-business from a business perspective may become its weaknesses from security perspective unless the security issues are managed and tackled using sophisticated tools and measures. Compared to personal website, developing e-commerce website is much more complex as it needs to incorporate many components, from simple text, picture, etc. to financial transaction processing system (payment gateway). Under e-commerce, confidential and valuable corporate information and data are shared with customers, suppliers and business partners over internet for performing business transactions. As internet is an open public network and using that network business-critical corporate data as well as confidential personal data of customers are exchanged freely round the clock integrating many other systems, various security issues pose challenges in doing business under electronic mode which need to be addressed with utmost care in a systematic and structured manner to protect business critical information and transactions from unauthorized access in particular and achieve and sustain competitive advantage and business success at large. Security in e-commerce consists of two components namely, server (server) level security and network (internet) level security.

The servers store valuable and confidential data and these are vulnerable to computer virus, worm and trojan as well as hacker attack. The virus attack can disrupt normal functioning of the server and jeopardize the entire business processes. The hackers, on the other hand, can manipulate and damage corporate database leading huge monetary loss as well as damage of image and reputation of the business. The burglars can also alter and misuse transaction data of customers to make fraudulent transactions. For instance, the burglars may pilfer and use the debit card information of customers such as user name, password, etc. to make illegal purchases. To ensure security of server, proper security arrangements need to be implemented in the form of firewall and password authentication. On the other hand, network level security means securing network through encryption and other security measures such as firewall, intrusion detection and handling system, etc.

Security in e-commerce is not merely a technical process, rather people, processes and technology together play important role in establishing a secured environment for e-commerce. It is the responsibility of the management to ensure a secure environment for performing business operations in electronic mode through implementing appropriate tools and strategies to protect the networks and servers from electronic and cyber threats. Generally, firewalls, proxy servers/dual host system, digital signature, encryption mechanism, public key infrastructure, etc. are used to tackle the issue and various security protocols like, secure socket layer, secure hypertext transfer protocol, cryptographic protocol, secure electronic transaction protocol, secure electronic payment protocol, etc. are used to protect the communication channels of the business.

Section IV: Dimensions of e-commerce security

The dimensions of e-commerce security refer to the different security factors or security aspects that need to be considered in framing and implementing a secure e-commerce infrastructure for both the business and its customers. The major dimensions of e-commerce security are- privacy, confidentiality, integrity, availability, authenticity and non-repudiation.

Privacy: This is the most important facet of e-commerce security. Privacy in e-commerce means protecting the personal information of customers from unauthorized use. The information provided by a customer for making online business transaction should be used in a controlled way to meet the purpose for which it is provided and not beyond that.

Confidentiality: It ensures that only the authorized person can have, view and use the transaction data.

Integrity: Integrity in e-commerce transaction ensures that information and data displayed on the website or exchanged through internet are original and not altered by any unauthorized person.

Availability: It ensures that the website is available for use round the clock.

Authenticity: Authenticity refers to the legitimacy of the identity of persons involved in business transactions.

Non-repudiation: It means the parties involved in online transaction can not deny their role and responsibility in that transaction.

Section V: Implementing structured and integrated management strategies to investigate and handle security threats to the organizations

In order to minimize security threats to the organization, structured, integrated and appropriate security framework and management strategies need to be developed and implemented so that the nature of security risks as well as the procedure and mechanism to tackle such threats can be identified. Security mechanism for an e-business consists of two aspects-technological and legal. Again, security aspect should encompass front-end, mid-tier and back-end security. Front-end security means ensuring proper security of customer while a customer is accessing an e-commerce site. In this type of security, availability, confidentiality, authorization and authentication factors of security issues are handled. In order to ensure this type of security various mechanisms like, secure socket layer, firewalls, cryptographic protocol, intrusion detection system, integration verification system, etc. are generally employed. Mid-tier security ensures trusted operating system, secured handling of confidential information and data. The back-end security, on the other hand, deals with protection of database, information and processed information. In spite of adopting all these technological security measures, security aspect of e-commerce may be jeopardized due to accidental data loss or theft and for that appropriate legal framework is needed to prevent such situation as well as to protect such data from misuse by unauthorized persons. An integrated security framework of an e-business generally consists of the following parts- risk assessment, implementation plan, access control and security audit.

Section VI: Conclusion

E-business does not mean merely developing a website and selling products and services over the internet, rather its success depends on optimization of business processes through electronic means and developing competitive advantages in doing business over the internet. For leveraging information and communication technologies in doing business through electronic mode an organization needs to develop an integrated and well-structured management strategy to identify and tackle security risks associated with e-commerce in an instantaneous basis which will help the enterprise to minimize security threats to the organization, curtail the chance of loss of value-relevant and business-critical information and data, reinstate its reputation and reliability to the customers and achieve market leadership and competitive advantages.

References:

Agrawal, D., Agrawal, R.P., Singh, J.B. and Tripathi, S.P. (2012), 'E-commerce: True Indian Picture', *Journal of Advances in IT*, Vol. 3, No. 4, pp. 250-257.

Bandyopadhyay, K. (2009), *e Commerce: Past, Present and Future,* Vrinda Publications (P) Ltd., Delhi.

Franco, C.E. and Bulomine Regi. S. (2016), 'Advantages and Challenges of E-commerce Customers and Businesses: In Indian Perspective', *International Journal of Research – Granthaalayah*, Vol. 4, No. 3, pp. 7-13.

Khan, A.G. (2016), 'Electronic Commerce: A Study on Benefits and Challenges in an Emerging Economy' *Global Journal of Management and Business Research*, Vol. 16, No. 1, pp. 18-22.

Khan, M.S. and Mahapatra, S.S. (2009), 'Service Quality Evaluation in Internet Banking: An Empirical Study in India', *Indian Culture and Business Management*, Vol. 2, No. 1, pp. 30-46.

Kiang, M.Y. and Chi, R.T. (2001), 'A Framework for Analyzing the Potential Benefits of Internet Marketing', *Journal of Electronic Commerce Research*, Vol. 2, No. 4, pp. 157-163.

Kulkarni, P. and Chande, P. (2007), *IT Strategy for Business*, Oxford University Press, New Delhi.

Kulkarni, P., Jahirabadkar, S. and Chande, P. (2012), *E-Business*, Oxford University Press, New Delhi.

Krishna, S. Jaya (2004), *E-business- Emerging Models, Strategies and Practices*, The ICFAI University Press, Hyderabad.

Laudon, K.C. and Carol Traver (2007), *E-commerce Business, Technology, Society*, Pearson Eduucation, New Delhi.

Malhotra, P. and Singh, B. (2007), 'Determinants of Internet Banking Adoption by Banks in India', *Internet Research*, Vol. 17, No. 3, pp. 323-339.

Shahriari, S., Shahriari, M. and Gheiji, S. (2015), 'E-Commerce and its Impact on Global Trend and Market', *International Journal of Research – Granthaalayah*, Vol. 3, No. 4, pp. 49-55.

Subramani, M. and Eric Walden (2001), 'The Impact of e-commerce Announcements on the Market Value of Firms', *Information Systems Research*, Vol. 12, No. 2, pp. 135-154.

Wong, Poh-Kam (2003), 'Global and National Factors Affecting e-commerce Diffusion in Singapore', *The Information Society*, Vol. 19, No. 1, pp. 19-32.