IMPACT OF E-BUSINESS AND E-GOVERNANCE IN DEVELOPING INDIA

Prof (Dr). Manju Gupta*

Dr. Sheetal Badesra**

In this competitive world electronic needs are generating at a high speed. Electronic business and Electronic Governance are the two topics which are interlinked and interdependent and booming in this electronic world. As E-Business is generating at a high speed due to lack of time and can reach global market instantly. E-Business methods enable companies to link their internal and external data processing systems more efficiently and flexibly, to work more closely with suppliers and partners, and to better satisfy the needs and expectations of their customers. The internet is a public through way. Firms use more private and hence more secure networks for more effective and efficient management of their internal functions. That is the basic reason E-Governance is innovated by E-Business.An integral aspect of decision making in business is the analysis, evaluation and application of information about customer, competitors and environmental factors. To make effective sales, managers need to collect adequate information about what is happening and what might happen in future. Good and timely information is a valuable tool because it reduces uncertainty and risk associated with decision making.

KEY WORDS: E-Business, Sales Management, Customer Service and E-Governance.

Introduction

India is on its way to becoming the largest e-commerce economy in the world. The business of e-commerce, or e-business is growing at a very fast pace, facilitated by cashless online payment methods. With the advantage of a fast-growing GDP, an increasing spending capacity, ease of doing business, and healthy competition in the consumer market, e-business is at an all-time high. And this will keep growing, the way India's economy is progressing. The recent image of German Foreign Minister making PayTm payment while shopping in Chamdni Chowk is proof of the dynamic

* Professor, Department of Commerce, Maharaja Agrasen Institute of Management Studies, Rohini, Delhi

** Assistant Professor, Department of Commerce, Maharaja Agrasen Institute of Management Studies, Rohini, Delhi

e-economy that is India. In these times it is very important to be anle to regilate e-commerce and to streamline e-governance. This paper will look into the e-governance aspect of this form of commercial activity.

Defining E-Business and E-Governance

Electronic business commonly referred to as **"business" or "e-business",** or an internet business, may be defined as the application of information and communication technologies (ICT) in support of all the activities of business. Commerce constitutes the exchange of products and services between businesses, groups and individuals and can be seen as one of the essential activities of any business. Electronic commerce focuses on the use of ICT to enable the external activities and relationships of the business with individuals, groups and other businesses. Hence, E-business may be defined as the conduct of industry, trade, and commerce using the computer networks. The term "e-business" was coined by IBM's marketing and Internet teams in 1996.[1]

E-business involves business processes spanning the entire value chain: electronic purchasing and supply chain management, processing orders electronically, handling customer service, and cooperating with business partners. Special technical standards for e-business facilitate the exchange of data between companies. E-business software solutions allow the integration of intra and inter firm business processes. E-business can be conducted using the Web, the Internet, intranets, extranets, or some combination of these.

Basically, electronic commerce (EC) is the process of buying, transferring, or exchanging products, services, and/or information via computer networks, including the internet. EC can also be beneficial from many perspectives including business process, service, learning, collaborative, community. EC is often confused with e-business.

Several dimension and factors influence the definition of e-Governance. The word "electronic" in the term e-Governance implies technology driven governance. E-Governance is the application of Information and Communication Technology (ICT) for delivering government services, exchange of information communication transactions, integration of various stand-alone systems and services between Government-to-Citizens (G2C), Government-to-Business (G2B), Government-to-Government(G2G) as well as back office processes and interactions within the entire government frame work. Through the

1 Andam, Zorayda Ruth B., "Chapter 1", *E-commerce and e-business,* e-ASEAN Task Force, 2003 available at: https://digitallibrary.un.org/record/524541/files/61164_Ecommerce%2520and%2520E%2520Business.pdf

e-Governance, the government services will be made available to the citizens in a convenient, efficient and transparent manner. The three main target groups that can be distinguished in governance concepts are Government, citizens and businesses/interest groups. In e-Governance there are no distinct boundaries.[2]

Generally four basic models are available-Government to Customer (Citizen), Government to Employees, Government to Government and Government to Business.

Difference between E-Governance and E-Government

Both the terms are treated to be the same; however, there is some difference between the two. "E-government" is the use of the ICTs in public administrations- combined with organizational change and new skills- to improve public services and democratic processes and to strengthen support to public". The problem in this definition to be congruent with the definition of e-governance is that there is no provision for governance of ICTs. As a matter of fact, the governance of ICTs requires most probably a substantial increase in regulation and policy- making capabilities, with all the expertise and opinion-shaping processes among the various social stakeholders of these concerns. So, the perspective of the e-governance is "the use of the technologies that both help governing and have to be governed".[3]

E-Governance is the future; many countries are looking forward to for a corruption free government. E-government is one-way communication protocol whereas E-governance is two-way communication protocol. The essence of E-governance is to reach the beneficiary and ensure that the services intended to reach the desired individual has been met with. There should be an auto-response system to support the essence of E-governance, whereby the Government realizes the efficacy of its governance. E-governance is by the governed, for the governed and of the governed.[4]

---

2 Larry Freed, (2010),"Annual E-Commerce Report, ForeSeeResults", Available at: http://www.a-nei.org/blog/wpcontent/uploads/2010/02/ACSI_Ecommerce_2010.pdf

3 Agarwal, Devendra et al, "E-Commerce: True Indian Picture", *Journal of Advance in Information Technology,* Vol. 3, No. 4, 2012

4 Starting a Business (2012),"Small Businesses and E-Commerce in India", Available at: http://smallbusinessindia.intuit.in/starting-business/small-businesses-e-commerce-india/

Establishing the identity of the end beneficiary is a true challenge in all citizen-centric services. Statistical information published by governments and world bodies do not always reveal the facts. Best form of E-governance cuts down on unwanted interference of too many layers while delivering governmental services. It depends on good infrastructural setup with the support of local processes and parameters for governments to reach their citizens or end beneficiaries. Budget for planning, development and growth can be derived from well laid out E-governance systems.

Need for E-Commerce and E-Governance

While much has been written of the economic advantages of Internet-enabled commerce, there is also evidence that some aspects of the internet such as maps and location-aware services may serve to reinforce economic inequality and the digital divide. Electronic commerce may be responsible for consolidation and the decline of mom-and-pop, brick and mortar businesses resulting in increases in income inequality.[5]

1. Security

E-Business systems naturally have greater security risks than traditional business systems, therefore it is important for e-business systems to be fully protected against these risks. A far greater number of people have access to e-businesses through the internet than would have access to a traditional business. Customers, suppliers, employees, and numerous other people use any particular e-business system daily and expect their confidential information to stay secure. Hackers are one of the great threats to the security of e-businesses. Some common security concerns for e-Businesses include keeping business and customer information private and confidential, authenticity of data, and data integrity. Some of the methods of protecting e-business security and keeping information secure include physical security measures as well as data storage, data transmission, anti-virus software, firewalls, and encryption to list a few.

2. Privacy and confidentiality

Confidentiality is the extent to which businesses makes personal information available to other businesses and individuals. With any business, confidential information must remain secure and only be accessible to the intended recipient. However, this becomes even more difficult when dealing with e-businesses specifically. To keep such

5 Rastogi, Rajiv, "India Country Report on E-Commerce Initiatives", Director Department of Information Technology, Ministry of Communication and Information Technology India available at: http://www.unescap.orgtidpublicationpart_three2261_ind.pdf

information secure means protecting any electronic records and files from unauthorized access, as well as ensuring safe transmission and data storage of such information. Tools such as encryption and firewalls manage this specific concern within e-business.

3. Authenticity

E-business transactions pose greater challenges for establishing authenticity due to the ease with which electronic information may be altered and copied. Both parties in an e-business transaction want to have the assurance that the other party is who they claim to be, especially when a customer places an order and then submits a payment electronically. One common way to ensure this is to limit access to a network or trusted parties by using a virtual private network (VPN) technology. The establishment of authenticity is even greater when a combination of techniques are used, and such techniques involve checking "something you know" (i.e. password or PIN), "something you need" (i.e. credit card), or "something you are" (i.e. digital signatures or voice recognition methods). Many times in e-business, however, "something you are" is pretty strongly verified by checking the purchaser's "something you have" (i.e. credit card) and "something you know" (i.e. card number).[6]

4. Data integrity

Data integrity answers the question "Can the information be changed or corrupted in any way?" This leads to the assurance that the message received is identical to the message sent. A business needs to be confident that data is not changed in transit, whether deliberately or by accident. To help with data integrity, firewalls protect stored data against unauthorized access, while simply backing up data allows recovery should the data or equipment be damaged.

5. Non-repudiation

This concern deals with the existence of proof in a transaction. A business must have assurance that the receiving party or purchaser cannot deny that a transaction has occurred, and this means having sufficient evidence to prove the transaction. One way to address non-repudiation is using digital signatures. A digital signature not only ensures that a message or document has been electronically signed by the person, but since a digital signature can only be created by one person, it also ensures that this person cannot later deny that they provided their signature.

6 Khan, Abdul Gaffar, "Electronic Commerce: A Study on Benefits and Challenges in an Emerging Economy", *Global Journal of Management and Business Research,* Vol. 16, Iss.1, 2016

6. Access control

When certain electronic resources and information is limited to only a few authorized individuals, a business and its customers must have the assurance that no one else can access the systems or information. Fortunately, there are a variety of techniques to address this concern including firewalls, access privileges, user identification and authentication techniques (such as passwords and digital certificates), Virtual Private Networks (VPN), and much more.

7. Availability

This concern is specifically pertinent to a business' customers as certain information must be available when customers need it. Messages must be delivered in a reliable and timely fashion, and information must be stored and retrieved as required. Because availability of service is important for all e-business websites, steps must be taken to prevent disruption of service by events such as power outages and damage to physical infrastructure. Examples to address this include data backup, fire-suppression systems, Uninterrupted Power Supply (UPS) systems, virus protection, as well as making sure that there is sufficient capacity to handle the demands posed by heavy network traffic.

8. Common security measures

Many different forms of security exist for e-businesses. Some general security guidelines include areas in physical security, data storage, data transmission, application development, and system administration.

9. Physical security

Despite e-business being business done online, there are still physical security measures that can be taken to protect the business as a whole. Even though business is done online, the building that houses the servers and computers must be protected and have limited access to employees and other persons. For example, this room should only allow authorized users to enter, and should ensure that "windows, dropped ceilings, large air ducts, and raised floors" do not allow easy access to unauthorized persons. Preferably these important items would be kept in an air-conditioned room without any windows.

Protecting against the environment is equally important in physical security as protecting against unauthorized users. The room may protect the equipment against flooding by keeping all equipment raised off of the floor. In addition, the room should contain a fire extinguisher in case of fire. The organization should have a fire plan in case this situation arises.

In addition to keeping the servers and computers safe, physical security of confidential information is important. This includes client information such as credit card numbers, checks, phone numbers, etc. It also includes any of the organization's private information. Locking physical and electronic copies of this data in a drawer or cabinet is one additional measure of security. Doors and windows leading into this area should also be securely locked. Only employees that need to use this information as part of their job should be given keys.

Important information can also be kept secure by keeping backups of files and updating them on a regular basis. It is best to keep these backups in a separate secure location in case there is a natural disaster or breach of security at the main location.

"Failover sites" can be built in case there is a problem with the main location. This site should be just like the main location in terms of hardware, software, and security features. This site can be used in case of fire or natural disaster at the original site. It is also important to test the "failover site" to ensure it will actually work if the need arises.[7]

State of the art security systems, such as the one used at Tidepoint's headquarters, might include access control, alarm systems, and closed-circuit television. One form of access control is face (or another feature) recognition systems. This allows only authorized personnel to enter, and also serves the purpose of convenience for employees who don't have to carry keys or cards. Cameras can also be placed throughout the building and at all points of entry. Alarm systems also serve as an added measure of protection against theft.[8]

10. Data storage

Storing data in a secure manner is very important to all businesses, but especially to e-businesses where most of the data is stored in an electronic manner. Data that is confidential should not be stored on the e-business' server, but instead moved to another physical machine to be stored. If possible this machine should not be directly connected to the internet, and should also be stored in a safe location. The information should be stored in an encrypted format.

7 Wang, Yidan, "Research on E-commerce Platform of Online Shopping Consumers", *Advances in Economics, Business and Management Research,* Vol 203, 2021

8 Shweta Sharma, Sugandha Mittal, "Prospects of E-Commerce in India", Available at: http://www.rimtengg.com/iscet/proceedings/pdfs/adv_nw_tech/43.pdf

Any highly sensitive information should not be stored if it is possible. If it does need to be stored, it should be kept on only a few reliable machines to prevent easy access. Extra security measures should be taken to protect this information (such as private keys) if possible. Additionally, information should only be kept for a short period of time, and once it is no longer necessary it should be deleted to prevent it from falling into the wrong hands. Similarly, backups and copies of information should be kept secure with the same security measures as the original information. Once a backup is no longer needed, it should be carefully but thoroughly destroyed.

11. Data transmission and application development

a) All sensitive information being transmitted should be encrypted. Businesses can opt to refuse clients who can't accept this level of encryption. Confidential and sensitive information should also never be sent through e-mail. If it must be, then it should also be encrypted.

b) Transferring and displaying secure information should be kept to a minimum. This can be done by never displaying a full credit card number for example. Only a few of the numbers may be shown, and changes to this information can be done without displaying the full number. It should also be impossible to retrieve this information online.

c) Source code should also be kept in a secure location. It should not be visible to the public.

d) Applications and changes should be tested before they are placed online for reliability and compatibility.

12. System administration

Security on default operating systems should be increased immediately. Patches and software updates should be applied in a timely manner. All system configuration changes should be kept in a log and promptly updated.

System administrators should keep watch for suspicious activity within the business by inspecting log files and researching repeated logon failures. They can also audit their e-business system and look for any holes in the security measures. It is important to make sure plans for security are in place but also to test the security measures to make sure they actually work. With the use of social engineering, the wrong people can get a hold of confidential information. To protect against this, staff can be made aware of social engineering and trained to properly deal with sensitive information.

E-businesses may use passwords for employee logons, accessing secure information, or by customers. Passwords should be made impossible to guess. They should consist of both letters and numbers, and be at least seven to eight digits long. They should not contain any names, birth dates, etc. Passwords should be changed frequently and should be unique each time. Only the password's user should know the password and it should never be written down or stored anywhere. Users should also be locked out of the system after a certain number of failed logon attempts to prevent guessing of passwords.

13. Security solutions

When it comes to security solutions, there are some main goals that are to be met. These goals are data integrity, strong authentication, and privacy.

14. Access and data integrity

There are several different ways to prevent access to the data that is kept online. One way is to use anti-virus software. This is something that most people use to protect their networks regardless of the data they have. E-businesses should use this because they can then be sure that the information sent and received to their system is clean. A second way to protect the data is to use firewalls and network protection. A firewall is used to restrict access to private networks, as well as public networks that a company may use. The firewall also has the ability to log attempts into the network and provide warnings as it is happening. They are very beneficial to keep third-parties out of the network. Businesses that use Wi-Fi need to consider different forms of protection because these networks are easier for someone to access. They should look into protected access, virtual private networks, or internet protocol security. Another option they have is an intrusion detection system. This system alerts when there are possible intrusions. Some companies set up traps or "hot spots" to attract people and are then able to know when someone is trying to hack into that area.[9]

15. Encryption

Encryption, which is actually a part of cryptography, involves transforming texts or messages into a code which is unreadable. These messages have to be decrypted in order to be understandable or usable for someone. There is a key that identifies the data to a certain person or company. With public key encryption, there are actually two keys used.

9 Kumar Dhananjay, Senthilkumar, "Effectiveness of E-Marketing in the success of Digital Entrepreneurship: A Conceptual Model", *JETIR*, May 2019, Volume 6, Issue 5, 2019

One is public and one is private. The public one is used for encryption, and the private for decryption. The level of the actual encryption can be adjusted and should be based on the information. The key can be just a simple slide of letters or a completely random mix-up of letters. This is relatively easy to implement because there is software that a company can purchase. A company needs to be sure that their keys are registered with a certificate authority.

16. Digital certificates

The point of a digital certificate is to identify the owner of a document. This way the receiver knows that it is an authentic document. Companies can use these certificates in several different ways. They can be used as a replacement for user names and passwords. Each employee can be given these to access the documents that they need from wherever they are. These certificates also use encryption. They are a little more complicated than normal encryption however. They actually used important information within the code. They do this in order to assure authenticity of the documents as well as confidentiality and data integrity which always accompany encryption. Digital certificates are not commonly used because they are confusing for people to implement. There can be complications when using different browsers, which means they need to use multiple certificates. The process is being adjusted so that it is easier to use.

17. Digital signatures

A final way to secure information online would be to use a digital signature. If a document has a digital signature on it, no one else is able to edit the information without being detected. That way if it is edited, it may be adjusted for reliability after the fact. In order to use a digital signature, one must use a combination of cryptography and a message digest. A message digest is used to give the document a unique value. That value is then encrypted with the sender's private key.[10]

The Information Technology Act, 2000

As early as the middle of 1997, Dell computers reported orders of a million dollars a day. By early 1999, projected E-commerce revenues for business wherein the billions of dollars and the stocks of companies deemed most adept at E-commerce were skyrocketing. Although many so-called dotcom retailers disappeared in the economic shakeout of 2000, Web retailing

10 Rajon, S A Ahsan, Nahid, Abdullah-Al, Arif, Abu, "A Generic Framework for Implementing Electronic Commerce in developing Countries", *IJCIT,* Online, Vol.1 Iss. 2, 2011

at sites such as Amazon.com, CDNow.com, and Comp data online.com continues to grow. International Data Corp (IDC) estimates the value of global E-commerce in2000 at US$350.38 billion. This is projected to climb to as high as US$7.14 trillion by 2007. IDC also predicts an increase in Asia's percentage share in worldwide e-commerce revenue from5% in 2000 to 18% in 2007. Asia-Pacific e-commerce revenues are projected to increase from $76.8 billion at year-end of 2001to $438.5 billion by the end of 2007.[11] Fig. 1, shows the growth of E-commerce in India over last few years.

Challenges

While we have a lot of advantages of E-commerce, we have a major disadvantage of reduced privacy. In order to better understand the impact of data mining on privacy, consider the following example of its potential application in the telecommunication industry. A cellular phone service provider has the technological ability to determine the location of any switched on cell phone in its coverage area.

The cell phone service provider collects information about all its subscribers during the sale of a contract. Typical subscriber information that would be collected may include the following:[12]

- Age
- Occupation.
- Income
- Banking Details

The ability of the cell phone service provider to track the location of the cell phone, and therefore its owner, might yield the following information:

- The route typically traveled to and from work by the subscriber.
- Whether the subscriber travels during business hours, or spends most of the day in the office.
- Which shopping centers the subscriber visits over weekends or after hours. cell phone service provider could make use of the collected information to position its own advertising billboards more strategically, or to situate its different branches at the correct shopping centers. At the same time however, the organization might decide to

11 Yue, Hongqiang, "Research on E-Commerce Data Standard System in the Era of Digital Economy From the Perspective of Organizational Psychology", DOI: https://doi.org/10.3389/fpsyg.2022.900698

12 Ahmad, Vasim, Ghai, Divya Negi, "Challenges and Prospects of E-commerce – A Review (2015-2022)", IJFANS, Vol. 11, Iss. 11, 2022.

benefit from this knowledge by selling it off to other organizations. The information could for instance be sold to other organizations who also want to be able to position their billboard more effectively, or a fast food chain could send out advertising messages to subscribers as soon as they come into close proximity of one of their outlets. One potential application of the above information could be the use of the information by marketers selling billboard advertising on the side of the road.[13]

Knowing the age, income and occupation of the people who travel a specific route could improve the effectiveness of such marketing campaigns even further. This example highlights an interesting application of data mining, but it also shows the potential threats that data mining pose to privacy. The main areas of concern with regard to data mining and privacy are therefore found in the followings:[14]

- What kind of information do you collect about your customer?
- Who is ultimately in control of that information?

It is up to the organization employing data mining to ensure that their actions result in neither of the negative effects, namely, incurring legal liability or obtaining bas press as a result of privacy violations associated with their data mining effort. Awareness project aimed at applying data mining to commercial databases for information on potential terrorists, due to a lack of consideration that was shown for privacy issues. The consumers might for instance be aware of the fact that collected information about them is used for billing purposes, but that they did not necessarily implicitly agree to allow the organization to use the data in a data mining scenario, thereby exceeding the original intent of the data collection. To this end it is important to pay particular attention to how the data used in data mining was obtained in the first place, and whether it's used could result in a violation of privacy.

13 Rajput, Vidhu, E-Business and E-Governance: "A case study of web portal Punarbhava and accessibility features", *International Journal of Educational Planning & Administration,* Vol 7 Iss. 1, 2017

14 Santos, Vasco, Augusto, Tatiana, et al, "E-Commerce: Issues, Opportunities, Challenges, and Trends", DOI: 10.4018/978-1-6684-5523-4.ch012

Compensation for Computer Frauds

Consisting of sections 43 to 47 of the Information Technology Act, 2000, provides provisions for compensation for the loss arising out from computer frauds and provision for making appeals against such compensation. Section 43 deals with penalty for damage to computer, computer system etc. by any of the following methods.[15]

1. Securing access to the computer, computer system, or computer network.
2. Downloading or extracting any data, computer database, or information from such computer system or those stored in any removable storage medium.
3. Introducing any computer contaminant or computer virus into any computer, computer system or network.
4. Damaging any computer, computer system, or network or any computer data, database or program.
5. Disrupting any computer, computer system and network.
6. Denying access to any person authorized to access any computer, computer system, or network.
7. Providing assistance to any person to access any computer, computer system, or network in contravention of any provision of this act or its rules.
8. Changing the services availed of by any person to the account of another person by tampering with or manipulating any computer, computer system or network.

Section 46 confers power to adjudicated contravention under this Act to an officer not below the rank of a director to the government of India or an equivalent officer of a state government. The adjudicating officer shall hold an enquiry in the prescribed manner after giving reasonable opportunity of being heard and, thereafter, impose penalty where required.

Section 47 provides that while deciding upon the quantum of compensation the adjudicating officer shall have due regard to the amount of gain of unfair advantage and the amount of loss caused to any person as well as the respective nature of default.

15 For a more detailed discussion please see : Aashit Shah, Parveen Nagree, et. al., "Legal Issues in E-Commerce," available at: http://www.nishithdesai.comResearch-PapersLegal_issues_ecom.pdf

Conclusion

E-Commerce has unleashed yet another revolution, which is changing the way businesses buy and sell products and services-Commerce is the future of shopping. Thus, is would be apt to quote "The future is here. It's just not widely distributed yet"-William Gibson. With the deployment of 3G and 4G wireless communication technologies, the Internet economy will continue to grow robustly? These technologies will prove to be a catalyst in the growth of E-commerce and internet users would buy more products and buy more frequently online; both new and established companies will reap profits online. Information technology leads to enhancement of customer service which can give customer control over all aspects of their interaction with a company through a user-friendly website.