The role of e commerce in the era of globalization

E commerce is the electronic commerce where business starts with electronically. For using the e commerce transaction must be happen via electronic system. For example someone wants to sell his product then he needs to get the order of that product and also needs to get payment so that he can send the product. In this case the buyer can buy that product through the electronic payment system. But there is some problem for this case such as security issue. If the third party involve on the e payment system then it will be harmful for both buyer and sellers. So the security of e payment system should be strong to protect from third party. Here third party is internet expert hacker.

Aim & objective: To secure and monitor of the e payment will be increase in the business sector day by day. More than one browser needs to be user friendly. Maintain a good customer service.

Different section: Blaise j.(2004)said that Though the Internet has increased the speed and number of victims a fraudster can reach in one attempt, the actual types and techniques of the Internet scams follow the same patterns as scams previously conducted by mail or telephone. As with pre-cyber scams, the number of scams and the subsequent variations make it impossible to mention them all. The primary intent of the fraudster is to befriend the victim, gain their trust, and then obtain money or enough personal information to access financial accounts. Becoming aware of and informed about some of the different types of Internet scams should make consumers more mindful of their on- line actions and transactions.

According to the Adi m alwaked.(2008). some questions arisen like: Do the electronic payments securely exist in the Business to Business transactions within the country? What are the governmental security criteria for the e-business transactions? And do I as a work owner and a government have professionals and graduates who can manage e-business departments and projects using the new e-business methodologies as knowledge management and expert systems? And if the e-business pillars are not yet completed or initiated, to what level should the users deal with e-business? Do we have any alternatives? Many of these critical enquiries should be answered when reviewing e-government and e-readiness situations. Failing to answer and solve this ambiguity can result in two unwanted situations: the work owners will not adopt e-business, or the e-business will be initiated based on ambiguous visions that will not achieve the expected propositions and therefore will fail.

All the e-business revenues are part of the whole business revenues and they will be part of the final financial statements of the enterprises, and if the governments decided to give these taxation supports to motivate e-business inside the different enterprises, it is recommended that good policies and frameworks applied against frauds that take advantage of the financial facilitations, for instance the fake online contracts and payments in order to delude the authorities and to create an impression that the e-business in a particular company was the main reason for the revenues, and therefore there should be some efficient procedures against these kinds of frauds.

The e-business field has become the first target for the e-hackers today, many kinds of frauds in credit cards, stealing identities, and different kinds of frauds are evolving every day, but actually the solution is not always within the responsibility of the governments, but can the governments support the e-business adopters here?

Traditionally, this is found in e-business pillars and e-readiness, as the secure e-payment methods in e-billing, and the good regulations to fight the net crimes, and the e-business awareness programmes as mentioned.

But as a part of a new strategic e-business policy that keeps and increase the advantages of the e-service and limits the weaknesses, calls for defined e-security criteria in the DNs might be a solution, such criteria that specifies strict standards for e-commerce websites, including all the security aspects, as authentications, IP viewers for more identifications of customers, a strong insist on the ecommerce website owners to include the security awareness issues in the main pages of their websites and to keep reminding their users about them, all these procedures can increase the customer’s confident about security and solve the ambiguity of these issues.

National payment systems are the backbone of a financial sector. Standard protocols for check and electronic payments will facilitate the adoption of electronic payments by banks, retailers, government agencies, and others in the payments chain. Access to electronic payments settlement can be contentious, as banks typically control or influence payment systems and may resist opening access to other financial service providers and retailers (Isern, Deshpande & van Doorn, 2005).

Avshalom Aderet et al(2007). said security and privacy assesses the degree of customer exposure to the risks involved in the e-shopping process and the likelihood of a product or service not meeting consumer expectations (Dillon and Reif, 2006). The variables discussed in this factor are: the means used to assure data security, the privacy of personal information, and the security guarantee that pertains to each transaction (Chung-Hoon and Young-Gul, 2003). We group “ privacy” and “ security” together following Flavián and Guinalíu (2006) who, having reviewed the privacy and security literature, suggest that, although these concepts are often researched as separate variables, there is a close relationship between them in the mind of the consumer and they should therefore be considered as a single variable. Furthermore, in practice, e-vendors tend to handle the protection of privacy and security together. Finally, in public policy these concepts run side by side.

Globalization has brought in many changes in the business scenario with the whole world inching towards one big market place. Communication between the buyers and sellers has

become critical as each can opt to explore a greater number of alternatives than ever before.

E-commerce through Internet, e-mails, websites, and other facilities, enables a businessman to be linked with every corner of the world, and thus opens up greater opportunities in the world market.

Important factor is the time required for completing a business transaction. As markets are becoming competitive and information is more readily

available, a quick, reliable and replicable transaction implies availing of prevailing opportunities. On the contrary, delays in processing a transaction might become synonymous to wasting an opportunity.

Therefore, a fast and alternative mechanism of communication, contract, and payment is an Integral part of a globally competitive business organization.

Wasting the customer’s time — Time is the most important commodity in online shopping. You want your customers to be able to find what they want and buy it as quickly as possible. Dynamic pages with changing content may look interesting, but they also make pages take longer to load. When customers have to wait for pages to load, they often give up and go to a faster-moving site. Additionally, some e-commerce sites make the mistake of wasting a customer’s time during the checkout process by requiring registration or asking for unnecessary info. Once a customer decides to buy from your site you should make the checkout processes as fast as possible with as few clicks as possible. Otherwise, the customer may fail to complete the sale out of frustration.

Lack of compatibility with more than one browser — While 80% of the market uses Microsoft Internet Explorer, failing to design your e-commerce site to work with other browsers is passing up a huge opportunity. You immediately knock out at least 20% of your potential customer pool, maybe more. Making your website work with a variety of browsers usually only requires a few minor tweaks, but it can make a big difference in the amount of traffic you receive.

Poor overall web design -When a website is not well organized or looks unprofessional, many customers will immediately look elsewhere. Online shoppers have high standards these days when it comes to how your e-commerce site looks and functions. Your products should be easy to find and displayed nicely. Customers should be able to search for what they want and find it. Likewise shopping cart use should be a streamlined process. Any hitches in the buying process from start to finish will cost you customers.

Poor customer service -All e-commerce sites should make it easy to get questions about products and purchases answered. Too many sites make finding contact information and accessing company policies challenging for the customer. If customers can’t find the information they need to feel comfortable about a sale, they will probably abandon the sale. Make sure all of your merchant policies and contact information are prominently displayed on multiple pages of your website.

Conclusion: Internet fraud can evidently be defined as an electronic deception and theft. However, as technology advances, the tactics and skills used by fraudsters to commit these crimes will also advance. In 2002, over $14. 6 million in losses were reported in the U. S. alone, due to Internet fraud; while it is expected, several million more went unreported. Local, state and federal agencies are actively tracking, investigating, and prosecuting fraud offenders. However, with the limitless capabilities of the Internet, it’s often difficult to determine if the con artist is in the next apartment, next state, or in a completely different country. These cyber swindles and dot-cons present new challenges to governments. The

Internet enables criminals to cloak themselves in anonymity, making it imperative that governments act more quickly to stop newly emerging schemes before the perpetrators can disappear in the World Wide Web. Online consumers need to execute added precaution when surfing, reading e-mail, making purchases, and considering online opportunities. The great thing about the Internet is it is easy to find other information, and consumers should do crosscheck before they become a victim. Legitimate online retailers and credit card companies will also have to make continued efforts to reassure consumers that their Internet activities will be secure.

The global nature of the Internet, and law enforcement experience in conducting Internet fraud investigations, have made it increasingly clear that law enforcement authorities need to coordinate their efforts to have a substantial effect on all forms of Internet fraud.

- Reference: Blaise J(2004), internet fraud: a global perspective, vol4, pp1-9.

  Anguelov, C., Hilgert, M. & Hogarth, J. (2004). US consumers and electronic banking, 1995-2003. Federal Reserve Bulletin, Winter 2004. Retrieved December 10, 2005 from: http://www. federalreserve. gov/pubs/bulletin/2004/winter04_ca. pdf

  BIS. (2004). Survey of developments in electronic money and internet and mobile payments. Committee on Payment and Settlement Systems (CPSS). Basle: Bank for International Settlements.

BIS. (2003). Risk management principles for electronic banking. Electronic Banking Group of the Basel Committee on Banking Supervision. Basel: Bank for International Settlements.

Bézard, G. (2005). Low-value payments: Looking for the code cracker. Boston: Aite Group, LLC.

Journal of E-Business: Volume VII, No 2 (2007) 45 the United States, Federal Reserve Bulletin, Spring, 180-201.

Isern, J. (2007). Launching electronic banking in developing countries: What can be learned from experience in developed countries? E-Business Review, 7.

Isern, J., Deshpande, R. & van Doorn, J. (2005). Crafting a money transfers strategy: Guidance for pro-poor financial service providers. CGAP Occasional Paper 10. Washington: The World Bank.

Lafferty Group. (2005c, November 14). US consumers and corporates reduce cheque usage. Electronic Payments International Newsletter. London: Author.

NetBank, Inc. (2004). Annual report. Retrieved December 29, 2005 from: http://www. netbankinc. com/ir_reports. htm

Pennathur, A. (2001). “ Clicks and bricks”: E-risk management for banks in the age of the internet. Journal of Banking and Finance (25), 2103-2123.

Rombel, A. (2005). The world’s best internet banks 2005. Global Finance 19(8), 31-36.

Adi m alwaked.(2008). encouraging e-business investments in the developing nations and the ambiguous road: a proposed vision. vol8, pp12-18,

Avshalom Aderet et al(2007). taking customer perceptions of the ethical commitments of e-vendors seriously, vol6 pp12-15