The Role of e-Commerce Awareness on Increasing Electronic Trust

Issa Najafi

PhD Candidate, IT & E-commerce
ARMENIAN STATE AGRARIAN UNIVERSITY (ASAU)
E-mail: issa.najafi@gmail.com / najafy@um.ac.ir

Abstract: It is not long ago that e-commerce service has turned to be one of the most important applications of the Internet and www. In all aspects of human life, especially in business activity, the application of ICT is so strong that in near future, the world will witness inevitability of this technology in most of the daily issues. Regardless of its technological advantages in the areas of increasing speed, accuracy, ease and dramatic reduction of transaction or processing costs, many challenges and application barriers are continuously faced by its users. Concerns such as users' privacy breaches, ensuring the accuracy, original identification of the buyers and sellers, confidentiality provision cause discomfort and distress an individual during cyberspace transaction or deal. And the achievement of the desired level of confidence in the abilities and capabilities of the other side and performance endanger the system. The increased level of awareness and the security culture of the cyberspace application enhance relative peace of an individual while being in the virtual space or in the process of e-commerce. The resulting comfort helps a person to identify and belief in the capabilities of the opposite side or system and their adherence to the commercial, behavioral, legal and technical principles connected to right deals. In cyberspace under discussion, this identification or situation is corresponding with electronic trust. E-Trust is the pillar of E-commerce. This article will discuss the role of e-commerce awareness in increasing the electronic trust.
[Issa Najafi. **The Role of e-Commerce Awareness on Increasing Electronic Trust.** *Life Sci J* 2012;9(4):1487-1494] (ISSN:1097-8135). http://www.lifesciencesite.com. 226

Keywords: Trust, E-commerce Awareness, Privacy, Security, Risk, e-Trust

1. Introduction

Digitally enabled commercial transactions between and among organizations and individuals, also known as e-commerce, involve the exchange of value across organizational or individual boundaries in return for products and/or services. Due to this, IT usage in present times has become a common practice. B2C transactions, B2B transactions, C2B and B2B2C are commonly used in the market. Chen and Dhillon have defined ecommerce as "the transaction of goods and services over the internet". It is also described as the "sharing, transferring and exchanging of information". In order to survive in the highly competitive global economy, businesses must leverage technologies such as data warehousing and data mining to collect customer information, analyze their characteristics and behaviors, build relationships with existing customers, and draw potential ones. As such, gathering information about customers is a necessary task for managers to gain a better understanding of consumer preferences. Despite its exponential growth, e-commerce is faced with the predicament of an increasing number of users and their corresponding apprehension. The purpose of e-commerce is to perform B2B as well as B2C online transactions, and to exchange goods and services from a distance by any electronic and networked device that can use the Internet. E-commerce entails the exchange of information by EDI. The success of e-Commerce will continue to be an important part of business growth if it can overcome the concerns businesses and consumers have with stolen identity, secure banking, payments, and transactions. One way to overcome these concerns (and secure e-Commerce) is to use cryptography. The Internet is not known for its secure environment. In fact, the Internet is not safe for e-Commerce unless it involves using cryptography and making users aware of the concerns with e-Commerce. PC users need to know how to improve e-Commerce security. Both PGP and SSL encryption provide cryptography; they can form the basis of a secure e-Commerce infrastructure. Another aspect of confidence and trust is linked to the capability to evaluate and assess the security levels/features of components, systems, services, etc.

2. E-Business and Internet Marketing

Customer and Merchant trust is really important because without that there is no business. E-commerce leans to trust. Internet is good way how to make money and also good way how to spend them, but this is also quite insecure place! Every day peoples suffer from identity thief and lost money, identity and reputation. Because it is so important make a place, where people-customer can feel safe and be sure that information which he hand over here, will never be use to make damage him! The trust is really hard to get and if you lose it once then it is big possibility that you

lose it forever! E-commerce application includes the use of many different types of online facilities to do business: order registration, electronic advertising, electronic billing system, electronic marketing, online delivery status and tracking and customer services support. E-business applications also include the use of many different types of online facilities to communicate and coordinate: production planning, JIT management, scheduling, outsourcing and other business operation process. In the Internet, Make the most of your online presence by ensuring that your website is working effectively for your business. Everything you do to promote your business online is Internet marketing. For example, Internet marketing strategies include (but are not limited to) website design and content, search engine optimization, directory submissions, reciprocal linking strategies, online advertising, and email marketing. Internet marketing is a fast-changing industry that readily adapts to improvements in technology. There are always new marketing tools available to small businesses. Some of these tools are listed below (Website development & search engine optimization / Online advertising models / Publishing on third-party websites / Permission marketing using email / Corporate blogs / Affiliate/referral programs. It is not so hard, make webpage, and find something what to sell and starting make e-commerce! In these days it is really easy, but much harder is find customers and get trust from them, because any business plan, even the most perfect, can totally fail without trust. How to get this trust? How make webpage safe? How to known, that this webpage is dependable? When a merchant or companies want to setup and use the new e-commerce website, before all of them, they should find the correct answer for above questions. In the e-commerce models (main categories: B2C, C2C, B2B,...) enhancing online presence Items is one of the important factors. This is some considerable factors for enhancing online presence involves: The basics of developing your website (Learn how to create a website so you can attract more customers to your business) / Internet search tools (Find out how you can improve the chances of having your business found on the Web)/ Domain names(e-shop or E-commerce Portals names on the Internet) /Website visibility(Find tips to help you improve the way your website is found and displayed by search engines)/Getting hits(Find out how to attract customers to your website and keep them coming back). By offering products and services on the Web, businesses can gain unique benefits: (New customers, Cost-effective delivery channel, Stream lined enrollment, Better marketing through better customer knowledge.

3. Trust, Risk, Privacy and Security

The concepts, Trust, Risk, Privacy and Security, are widely used in various studies done by multiple disciplines, and they are often incorrectly referred to almost as synonyms. The aim is to clarify the concepts from the consumer viewpoint in e-commerce. E-business has issues that you are less likely to find with more traditional means of doing business. Entire relationships are built in e-business without any kind of face-to-face communication. However, e-business does expose you and your customers to risks, such as theft of your customer lists and customer credit card information, fraudulent purchases, misunderstanding with suppliers and customers due to lack of personal communications, and loss of customer or Consumer trust. For consumers to trust a transaction partner, they must have a degree of knowledge about them. This knowledge can be gained through previous experiences or by gaining information from a third party. Needham (1998) agrees that one way vendors can win the trust of potential customers is to secure recommendations and referrals from credible third parties. This is particularly important in online environments. Since time and experience are needed to deepen trust and the Internet is still relatively new, online transactions require very explicit guarantees up front. Clearly, the degree to which a consumer's opinions and purchasing behavior is influenced by a referee is directly dependent on the consumer-perceived reliability and trust of that referee. We classify four types of referees (word-of-mouth; watchdogs; certificate authorities; seals-of-approval) (Head, et al).

Consumer trust may be even more important in electronic, "cyber" transactions than it is in traditional, "real world" transactions. This is because of some of the characteristics of Internet cyber transactions they are blind, borderless, can occur 24x7,and are non-instantaneous (payment may occur days or weeks before delivery is completed) can cause consumers to be concerned that the seller won't adhere to its transactional obligations. In the electronic transactions, the key to success in Internet business is the establishment of trusted transaction processes where e-sellers create an environment in which a prospective consumer can be relaxed and confident about any prospective transactions. In other words, parties to a transaction in the online environment, should be on safe and secure environment, with minimal risk, maximal trust attempt to deal do so. After its transactions, its remain previous level of risk and trust in good status. If in the Cyber space, there are good policy and privacy, suitable trust and confidence, the risks will be negligible. Electronic transaction or e-commerce, the parties to the transaction, would be satisfactory and profitable. Since trust is likely to play an essential role in online transactions, it is important

to identify the antecedents of a consumer's trust in the context of an Internet transaction. In e-commerce development security is a critical and key factor. It is one of the pivotal success factors of e-commerce. Security is defined as "The protection of data against accidental or intentional disclosure to unauthorized persons, or unauthorized modifications or destruction". It usually refers to the provision of access control, privacy, confidentiality, integrity, authentication, non-repudiation, availability and effectiveness. Surveys conducted and compiled recently shows increasing concerns on security risks and have become a global issue. When customers lose Trust in a systems ability to protect sensitive and confidential data such as credit card information its feasibility will be compromised.

Since personal computers and web servers possess the ability to gather and process large amounts of data and the ability of the internet to provide and make available such on a global scale the need and concern for better security has also arisen. In turn consumers, legislators and even privacy advocates have pressed for broader and improved privacy protocols on the internet. Grandinetti 1996 and Martin 1973 define Privacy as "The rights of individuals and organizations to determine for themselves when, how and to what extent information about them is to be transmitted to others". Privacy can be understood as a legal concept and as the right to be let alone. Privacy can also mean "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". There is wide acceptance that trust is an important factor in nurturing or constraining the growth of e-commerce. The concept of trust has been heterogeneously defined by many authors in the fields of economics, social psychology, sociology, management, marketing, and information systems. One of the most accepted definitions of trust is stated as follows: "the willingness of a party to be vulnerable to the actions of another party, based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party. For online consumer's, Trust is defined as "a consumer's subjective belief that the selling party or entity will fulfill its transactional obligations as the consumer understands them". From a privacy standpoint, trust can be viewed as the customer's expectation that an online business will treat the customer's information fairly. The aim of building consumer trust in e-commerce is twofold: to encourage potential buyers to purchase for the first time and to encourage those who have already bought once to continue to do so. But, risk is defined as a consumer's subjective experience of uncertain consequences regarding an action the consumer took. A consumers' perceived risk is an important barrier for online consumers who are considering whether to make an online purchase. The perceived risk (RISK) means as a consumer's belief about the potential uncertain negative outcomes from the online transaction. There are strategies and methods that can help you reduce the risks to yourself and your customers. Be aware of the risks and take steps to deal with them before they become problems. Since the concept of perceived risk appeared in the marketing literature, various types of risk have been identified. For example, Jacoby and Kaplan identified seven types of risks: financial, performance, physical, psychological, social, time, and opportunity cost risk. In the case of Web shopping, three types of risk are said to be predominant: financial risk, product risk, and information risk (security and privacy). Product risk is associated with the product itself; for example the product may turn out to be defective. Financial risk, including opportunity cost and time, is related not to the product but to the marketing channel (the Internet); for example the online transaction may be duplicated because of technological error or unintended double-click the purchase button. Information risk is associated with transaction security and privacy; for example, the requirement that a consumer submits credit card information through the Internet can evoke apprehension due to the possibility of credit card fraud.

4. Trust and E-commerce

E-commerce and the Internet are usually defined as equivalent to each other. In fact, E-commerce is an integrated part of the Internet. They are commonly but mistakenly utilised as synonyms. While e-commerce is the utilisation of electronic means in making business transactions, the Internet is what has given e-commerce a greater outreach by providing a faster transmission media. E-commerce was used long before the Internet. E. Boyd and I. C. Bilegan shows electronic data usage to engage in purchasing and selling behavior is not new. They argue that the travel and hospitality business were pioneers in the sharing of information through electronic media for more than three decades. An example of this is the booking of reservations by airlines. As part of the airline Revenue Management System, transmission of data by electronic means was established to enable sales through a central reservation system in the early 60's. E-Commerce covers a wide variety of perspectives. The technological enabler is the Web, including the globally connected networks, the universal networking interface and transmitting standard (based on TCP/IP), and the WWW infrastructure that facilitates information storage, browsing, and retrieval. The Internet is the tool which makes e-commerce grows at a geometrical rate. As a

global system of connected computer networks, the Internet gives the opportunity to reach global markets with a broad audience and rapid transmission of information. According to the World Bank's World Development Indicators, in a very recent report (September, 2011), 27 percent of the world's population are internet users. E-commerce has created very specific benefits and some that were even unimaginable during the pre-internet era. It has become a basic instrument for successful commerce and more than a strategic issue, it has transformed into a tactical essential for effective business transactions. The Internet has developed as a media for transmitting information to everyone, but e-commerce needs to limit the distribution of information. This leads to several failures when it comes to transactions and information sharing. In the e-commerce literature, researchers have encountered many areas of concern. However, from the customer's perspective, trust and security are the two biggest concerns, and repeatedly studied by researchers.

The basic definition of trust is the reliance on the integrity, ability, etc. of a person or thing. The concept of trust has been widely analysed in different areas of study. Psychologists, sociologists and economists among others define trust from different perspectives. Trust is viewed as a personal characteristic by psychologists, as a social framework by sociologists, and as an economic mechanism for selection by economists. There are diverse definitions of trust, but all point in the same direction. In addition trust is a very complex construct, which has many definitions. For example, there seems to be a distinction between interpersonal trust and organizational trust. Interpersonal trust is trust in which the trustee is another individual. The target of trust is the person, which is not based on their position, title, or because they represent an organization. Organizational trust is when the trustee is an organization. Example includes that an employee trusts his or her company. Another aspect of organizational trust is that the trustee could be the representative of an organization. Key characteristic of trust include that, without it, it is hard to transfer knowledge, since the risk and uncertainty is high for the exchange of intellectual capital. There seems general agreement that risk is essential in understanding trust, whether it is interpersonal or organizational. For instance, Boon and Holmes define trust as "positive expectations about another's motives with respect to oneself in situations entailing risk ". Trust is a method of dealing with uncertainty; when dealing with independent agents, institutions or providers of resources (including knowledge), one trusts them if one accepts their characterization of what they will do. Trust can be a moral notion (X trusts Y to act in X's interests), or not (X trusts Y to perform some task T). Adopting the attitude of trust towards others means that one can plan and cooperate more efficiently, at the cost of greater risk of wasting resources when trust is misplaced.

To succeed in the fiercely competitive e-commerce marketplace, businesses must become fully aware of Internet security threats, take advantage of the technology that overcomes them, and win customers' trust. The process of addressing these general security questions (about customer concerns) determine the fundamental goals of establishing an e-commerce trust infrastructure: (Authentication, Confidentiality, Data integrity, Nonrepudiation).

The cyber world of e-commerce, there are always concerns. The solution for meeting the goal status less concerns includes two essential components:

- Digital certificates for Web servers, to provide authentication, privacy and data integrity through encryption
- A secure online payment management system, to allow e-commerce Web sites to securely and automatically accept, process, and manage payments online.

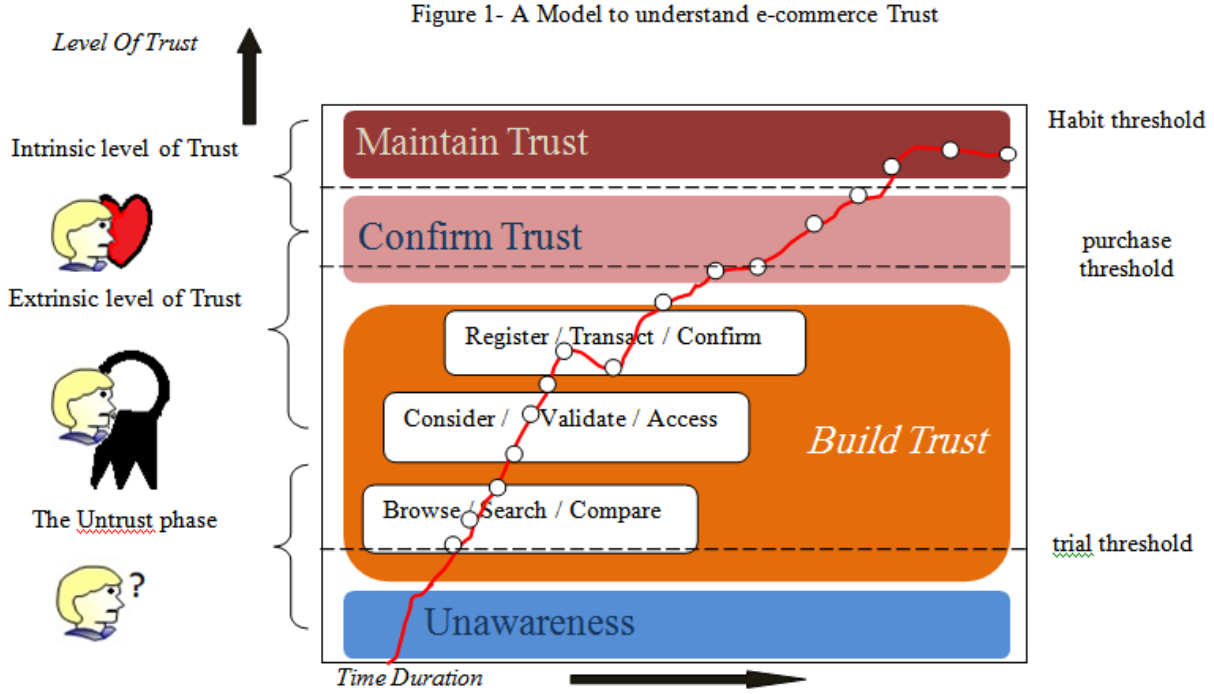
Together, these technologies form the essential trust infrastructure for any business that wants to take full advantage of the Internet. There is background technical information on cryptographic systems, including Public Key Cryptography, the system underlying SSL the basis for every e-commerce trust infrastructure. Encryption is the process of transforming information before communicating it to make it unintelligible to all but the intended recipient. Encryption employs mathematical formulas called cryptographic algorithms, or ciphers, and numbers called keys, to encrypt or decrypt information. There are some of secure solutions for reduce concerns on using e-commerce include : Symmetric Cryptography, Public-Key Cryptography, Modern Cryptography Systems (A Hybrid Approach), The Key Management Problem, Digital Signatures, Digital Certificates. A secure awareness of the packages listed in the e-commerce consumer confidence helps.

Web design is the process of developing a Web site, consisting of five main phases. Web design is 1-dimensional and N-dimensional as opposed to the 2-dimensionality of print design. Trust is one of the most important issues e-commerce Web sites have to consider. The issue of trust is of major importance for e-commerce Web sites. Visitors new to e-commerce are usually very reluctant and careful. The Web is often considered as a medium where information is vulnerable to hackers, where technology is unreliable, and where good intentions may lead to unpredictable results. These uncertain perceptions lead to a desire of control, protecting one's personal information. For current e-commerce users, control is still a

fundamental concern, but does not result in an non-buying attitude anymore. These users feel sufficiently assured, to their satisfaction, that they retain some control over their own personal information.

A model to understand e-commerce trust is provided below (model developed by Cheskin and Archetype Studio). Four phases can be distinguished: unawareness, building trust, confirming trust, and maintaining trust. Obviously, the aim of every e-commerce Web site is to arrive at the latest phase, which will be called lock-in in this thesis. Although the last phase is the most interesting one to an e-commerce Web site, the second phase, building trust, is the most important one. By completion of this phase, one travels from the trial threshold to the purchase threshold. As the figure shows, building trust is a long process of several Web site specific activities: browsing, searching, comparing, considering, validating, assessing, registering, transacting, and confirming. As will be discussed and investigated, building trust in e-commerce Web sites is primarily achieved by pursuing several good Web design strategies. Building trust in a Web site is not only a matter of using an appropriate Web design strategy. There are some factors, which we call extraneous factors that have a great impact on trust but cannot be influenced by the developer of an e-commerce Web site. Lack of consumer trust in e-commerce merchants, e-commerce technology, and the social, financial and legal infrastructures of the e-commerce environment, poses a major challenge to the large-scale uptake of business to consumer e-commerce.

Figure 1- A Model to understand e-commerce Trust



Four extraneous factors can be distinguished that have an impact on trustworthiness in an e-commerce Web site: increased experience with using the Internet, higher numbers of hours online at home, use of the Web for financial services, and a significant reliance on e-mail. Note that these factors not only increase trustworthiness, but also result in an increase of online spending. Trust is built on a foundation with a multitude of influential elements. If the e-commerce website cannot attractive the consumer or visitor, the greater the likelihood the visitor will go elsewhere, like a competitor's site. By following the above recommendations, you are all but guaranteeing an increase in trust and online sales. Trust plays an important role in customers' willingness to proceed with a transaction. The major concern of many users not buying goods and services on the Internet involves security reasons. It is clear that users who use the Web for financial services are not preoccupied with security concerns, and hence put a high degree of trust in e-commerce Web sites.

5. E-Trust

Trust is often understood as a relation between an agent (the trustor) and another agent or

object (the trustee) and this is a complex concept that has been studied from varying views and disciplines. The relation is supposed to be grounded on the trustor's beliefs about the trustee's capabilities and about the context in which the relation occurs. This is a generalization of the definition of trust provided by (Gambetta, 1998). Trust is a catalyst for human cooperation. It allows people to interact spontaneously and helps the economy to operate smoothly. Lack of trust on the other hand is like sand in the social machinery. It makes us waste time and resources on protecting ourselves against possible harm and thereby clogs up the economy. From a business perspective, trust has been defined as the willingness to depend on an exchanging partner in whom one has confidence, the willingness to be vulnerable to the actions of another party, and the expectation of ethically justifiable behavior, among others. Geyskens et al. provide a concise and meaningful view, where trust is described as the belief or expectation that the vendor's word or promise can be relied upon and the vendor will not take advantage of the consumer's vulnerability. The establishment of consumer trust is highly desirable for vendors, as it facilitates long-term relationships and encourages repeat interactions/purchases. In order to identify the antecedents of on-line trust needed to develop a model, we first have to define on-line trust. While this may appear to be a relatively straightforward task, defining on-line trust is inherently difficult. The on-line trust can emerge in numerous trustor / trustee relationships. However, it is not obvious that all forms of on-line trust relationships can be understood through one definition. For exploration of online trust can be start by discussing the several combinations of trustor / trustee relationships occurring both offline and online. Psychologists, sociologists and others have discussed several forms of trustor / trustee relationships as they occur in the offline world. Trustors and trustees, that is, objects of trust, can be individual people or groups. Groups may be families, neighbors, organizations or even societies. In the online world, there are two approaches to defining relationships between trustors and objects of trust. Computer-mediated communication researchers study individual-to-individual trust relationships mediated through technology. In contrast, other researchers focus on technology as the object of trust. E-trust occurs in environments where direct and physical contacts do not take place, where moral and social pressures can be differently perceived, and where interactions are mediated by digital devices. All these differences from the traditional form of trust give rise to a major problem that any theory of e-trust must solve: whether trust is affected by environmental features in such a way that it can only occur in non-digital environments, or it is mainly affected by features of the agents and their abilities, so that trust is viable even in digital contexts.

6. E-Commerce awareness and Trust

The survey and studying about e-commerce awareness and readiness users and companies is very important, because the e-commerce awareness can be reducing the all online consumers and customers concern. This study also identifies the enabling factors, the bottlenecks and, forecasts the future growth of e-commerce in scope of using e-commerce. Now, Awareness of e-commerce among the companies is very high but investment to develop an e-commerce application is very poor according to the survey. Awareness is the state or ability to perceive, to feel, or to be conscious of events, objects, or sensory patterns. In this level of consciousness, sense data can be confirmed by an observer without necessarily implying understanding. More broadly, it is the state or quality of being aware of something. In biological psychology, awareness is defined as a human's or an animal's perception and cognitive reaction to a condition or event. Awareness is a relative concept. Awareness is also a concept used in CSCW. Its definition has not yet reached a consensus in the scientific community in this general expression. However, context awareness and location awareness are concepts of large importance especially for AAA applications. The term "Customer Awareness" has found many uses in commerce. The understanding by an individual of their rights as a consumer concerning available products and services being marketed and sold. The concept involves four categories including safety, choice, information, and the right to be heard. The process of development along with the expanding globalization and liberalization process has increased the number of consumer related issues. Consumer protection has earned an important place in the political, economic and social agendas of many nations. Consumer education is an important part of this process and is a basic consumer right that must be introduced at the school level. Consumers by definition include all citizens who are, by and large the biggest group, who are affected by almost all government, public or private decisions. The most important step in consumer education is awareness of consumer rights.

Consumer awareness, which refers to a buyer's knowledge of a particular product or company, allows the buyer to get the most from what he buys. Consumers know more about their choices when they have product information and benefit from knowing their rights, hearing about alerts and warnings and finding out about safety issues.

On the one hand, the Awareness word is connected to the Security. On the other hand, security

and trust are the foundation of e-commerce and customer awareness on e-business is a necessity. In other words, awareness and security in e-commerce are related to each other. Therefore, in the e-commerce ISMS play a role. Security awareness is one of the main activities in design and implementation of information security management system in any organization.

Information security (IS) has always been looked upon as a necessary evil by business people and management. One of the biggest challenges for IS professionals has been to sell security to management. IS is a process and not a product. The process is intended to identify and minimize risk to acceptable levels. It should be iterative and should be managed. An ISMS is a set of policies concerned with IS management or IT related risks. The governing principle behind an ISMS is that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of IS risk. As with all management processes, an ISMS must remain effective and efficient in the long term, adapting to changes in the internal organization and external environment. ISMS is a proactive approach to continuously and effectively manage, at a high level, IS including people, infrastructure and businesses. The goal is to reduce risks to manageable level, while taking into perspective both business goals and customer expectations.

7. Security Awareness and Trust

These concepts of trust, risk, privacy, and security are used for many purposes and with many meanings. It is important to understand that these concepts serve different purposes: trust and risk are human-related concepts, while security is mainly used in a technical way. Security in that sense is the means to achieve and support consumer privacy. Security could also mean a consumer's feeling of being secure, safe. Studies concerning consumer trust, privacy, and security are often theoretical in nature. Two phrase "insecurity of financial transactions" and "loss of privacy" are among the major impediments to e-commerce. But in fact most users have only ague ideas about the threats and risks (lack awareness), and a very limited understanding of the technical and legal options for minimizing their risk. For instance, the cardholder's risk in sending his or her credit card number over the Internet is typically over estimated. At least as of this writing payments over the Internet are treated like mail-order / telephone-order transactions, which means that the cardholder is not liable at all. All risk is with the merchant. Strategies, products and services to enhance trust can be evaluated along five dimensions, each having different implications on trust and privacy: (participation, depth, publication, payer and price). Understanding each is important in developing guidelines and policies for evaluating, monitoring, comparing and developing different approaches and products to deal with specific trust-enhancement goals. When examining barriers to the adoption of e-commerce, numerous studies have singled out consumers' lack of trust as a major factor. Some people reduce the trust problem to one of security, arguing that, if security issues are resolved, people will be happy to transact online. However, when the trust problem is broken down into its constituents, privacy, ease-of-use or the credibility of information on the web are revealed to be as important to consumers as security. In other words, in all cases to achieve proper awareness of the consequences of any decision to reduce the risks of e-commerce. Lack of awareness of e-commerce system performance (privacy, security, risk), Technical items, required skills, Laws, regulations, legal considerations will be in creating is understandings. The mutual confidence and trust in the system or is reduced. The mismatch between consumer risk on online activities perception and the real risks has already been pointed out. (One of the illustrations the auction market) This lack of consumer awareness of the actual level of risks, of risk reduction measures and of available protection mechanisms is a major target of consumer protection. The security awareness goal is twofold: first, to provide information on trust and risk to businesses that are developing e-commerce systems; and second, to help consumers understand the risks in using the Internet for purchases and show them how to protect themselves.

8. Conclusion

Since the commercial events in cyberspace or virtual reality, unlike the traditional trade, are done online, thus every attempt of an individual: be it the buyer or the seller, may cause and bear damaging consequences for one of the parties or both of them, or their supporters such as the intermediaries, insurance agencies and banks. The decision for approving the electronic transaction is one the challenging steps in the e-commerce environment. These challenges can be discussed in relation to the security, validity and credibility of measures. For a safe business in cyberspace, the desirable level of trust and confidence is necessary for the actual beneficiaries of the e-commerce application. Even though for detection of unusual events in the electronic process, the contemporary electronic trading systems have advanced and intelligent mechanisms, but still in these systems most of the transactions are done under the impact of human factor. Among the key and influential issues in establishing a level of trust in e-commerce, the following are of importance:

Knowledge, skills, expertise and experience of an individual in making decision to acquire the necessary information regarding the deal, choosing a product or service, purchase decision and post purchase behavior, or

A deal together with the certain feeling of reliability toward system performance at the application layer and other layers of infrastructure under use, as well as

The integrity of the identities of the parties, accuracy of the product or service, assurance of a proper time for shipping and delivery.

Elimination or alleviation of security concerns requires the basics knowledge of security in e-commerce. One of the key factors affecting implementation and stability of the security solutions is knowledge: the awareness and scientific level of the users of e-commerce. Security awareness means training and cultural enhancement to achieve the desired level of security and mitigate the risks and threats against users in cyberspace. Since the users of cyberspace are concerned about issues like breach of privacy, confidentiality of information, dissemination of personal information, or responses to the inquiries and spam messages and the professional methods used by cyberspace robbers to steal, he increases in the e-commerce awareness level cause the enhanced level of e-trust.

References:

[1] Anil Gurung, Xin Luo, M.K Raja, 2008, “An Empirical Investigation on Customer's Privacy Perceptions, Trust and Security Awareness in E-commerce Environment”.

[2]- Atul Gupta and Rex Hammond, Information systems security issues and decisions for small businesses. IS security issues and decisions 2003

[3]- Balasundram Maniam, Lily Naranjo, and Geetha Subramaniam, Member, IEDRC, “ E-Commerce Best Practices“, August 2012, International Journal of Innovation, Management and Technology, Vol. 3, No. 4.

[4]- Clara CENTENO,European Commission, DG JRC, IPTS, Sevilla,2004,”Soft Measures to Build Security in e-Commerce Payments and Consumer Trust”.

[5]- Dan J. Kim, Donald L. Ferrin, H. Raghav Rao, 2007, “A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents”, Elsevier Godwin. J. Udo, Privacy and Security. Information management and computer security, 2001.

[6]- E. Boyd and I. C. Bilegan, “Revenue management and e-commerce,” Management Science, vol. 49, no. 10, pp.1363-1386, 2003.

[7]- I.Najafi,2011, “The Role of Electronic Readiness of Countries in Increasing Reliance on Electronic Transactions in the Context of E-Government and E-Commerce”, INTERNATIONAL SCIENTIFIC JOURNAL BULLETIN OF STATE AGRARIAN UNIVERCITY OF ARMENIA.

[8]- Kyösti Pennanen; Taina Kaapu; Minna-Kristiina Paakki,2006, “Trust, Risk, Privacy, and Security in e-Commerce”, FRONTIERS OF E-BUSINESS RESEARCH.

[9]- Needham, P. (1998). Developing trust and credibility, TICG Newsletter, http://www.intercongroup.com/aug98news.html, Accessed July 2000.

[10]- Gambetta, D. (1998). Can We Trust Trust? In D. Gambetta (Ed.), Trust: Making and Breaking Cooperative Relations (pp. 213–238). Oxford: Basil Blackwell

[11]- Geyskens, J. Steenkamp, L. K. Scheer, and N. Kumar, "The effects of trust and interdependence on relationship commitment: A transatlantic study," International Journal of Research in Marketing, vol. 13, pp. 303-317, 1996.

[12]- Head, M., and Hassanein, K. (2002). “Trust in e-Commerce: Evaluating the Impact of Third-Party Seals”, Quarterly Journal of E-commerce, 3(3), 307-325.

[13]- Rashad Yazdanifard, Noor Al-Huda Edres and Arash Pour Seyedi,2011, International Conference on Information Communication and Management IPCSIT vol.16 (2011) © (2011) IACSIT Press, Singapore.

[14]- V. Shankar, G. L. Urban, & F. Sultan, “Online Trust: a Stakeholder Perspective, Concepts, Implications, and Future Directions” Journal of Strategic Information Systems, vol. 11, 2002. pp. 325-344.

[15]-http://www.canadabusiness.ca/eng/145/148/4326/

[16]http://www.nicolasdeproft.be/pages/ecommercetrust/index.html.

[17]-http://www.verisign.com/.

10/2/2012