

SECURITY AND TRUST IN E-BUSINESS: PROBLEMS AND FEATURES

Dr. M.S. Chakravarthy

Asst Professor, Department of MBA, KBN College, Vijayawada, A.P., India

Abstract— Electronic Business (e-Business) is revolutionizing the way of communication between internal and external stakeholders in an organization. E-business can lead to competitive advantage and at the same time, increase profitability. There are several factors resulting on the success of e-business. One of the most important factors is trust. Acquiring customers' trust depends on many things that an e-business controls. Some relating factors for gaining customers' trust are: appeal of the website, product/service offering, branding, quality of service, and trusted seals. Actually, trust can be viewed from many angles such a transaction, information content, product, technology, and institution. There are huge numbers of impact on the way businesses think about designing, developing, and deploying Web-based applications. Web services may be an evolutionary step in designing distributed applications; however, they are not without problems. Therefore, we have to concern on the issue which is relating to the security in web-services of e-business. This paper discusses the issues relating to problems and prospects rose of the trust and security in e-business and also addressed security concerns in web services. It also discusses on the role of trust from the transaction perspective and analyses the things that what business could do in building customer trust.

Index Terms— e-Business, Security, Trust, Problems and Prospects

I. INTRODUCTION

Electronic Business which is commonly referred to as e-business, which is the utilization of information and communication technology (ICT) in conduct business on the internet, not only buying and selling but also servicing customers and collaborating with business partner. Electronic 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. Trust is the key to the success of e-business and lack of trust is the significant problem on the way to e-business success. During every business transaction, the parties involved should feel trust with the people and the companies. It must be established and managed continuously in business transaction activities.

Security services offering protection from security threats are: identification, authentication, confidentiality, integrity,

access control, and non-reputation. Today, e-business applications are doing more than ever to increase efficiency and improve relationships with partners and customers. In relation to trust and internet technologies, consumers are concerns about two main things which are privacy and security. This study is focusing on the issues relating to e-business, such as its importance, issues and the solutions in order to overcome related to the security and trust in e-business.

II. RESEARCH PROBLEM

E-business is very widely implemented by many companies in order to simplify purchasing processes by customers. There is almost an uncountable number of ways that an e-business setup could be attacked by hackers, crackers and disgruntled insiders. Common threats include hacking, cracking, masquerading, eavesdropping, spoofing, sniffing, Trojan horses, viruses, bombs, wiretaps, etc.

The research problems are:

- Lack of understanding on how e-business operation works.
- Lack of awareness regarding the security involved in e-business.
- Lack of understanding relating the trust involved in e-business.

III. OBJECTIVES OF STUDY

- The objectives of this research are as follows:
- To learn about e-business and how its business operation works.
 - To analyze and increase the awareness regarding security involved in e-business. To analyze the understanding relating the trust involved in e-business.
 - The increase the confidentiality of trust and security relating to e-business.

IV. LITERATURE REVIEW

Alan and William have stated that one of the most important issues in E-lending is security. In the paper, there was a statement from Richard Biell of Tower Group: "it's one

thing to submit a credit card number online to buy a product. It's quite another thing to put your entire personal dossier online and hope that no one intercepts it, particularly if you're not familiar with the lender." It stated that a borrower will not proceed to exchanging personal information without a sufficient level of confidence, and the impact is the customers will not peruse other products and services without being familiar with the vendor and the process. In order to improve the trust among the customers, the suggestions given are keeping the customers informed through web presences and shared database where the paper was not included. Mukherjee and Nath stated that trust and commitment are the central tenets in building successful long-term relationships in the online retailing context.

This paper aims to re-examine the Commitment-Trust Theory (CTT) of relationship marketing in the online retailing context. The electronic hypermedia environment posed new challenges for relationship retailing, where it is in the interest of retailers to establish and maintain long-term bonds with customers. This new marketing medium and channel is now an integral part of the multi-channel strategy for most retailers. The limitation the paper has not discovered is fraud may increase since customers might not receive the goods they had ordered, and sometimes the goods are not reached to the customers. Eben presented and reviewed the impact of information security for e-business with emphasize on the security threats and potential losses that could arise from those vulnerabilities. E-business security is analyzed as consisting of six dimensions: confidentiality, integrity, availability, legitimate use, auditing and non-repudiation.

This paper has proposed that designing a comprehensive and systematic security policy is a need for implementing Ebusiness security. The main thesis of this paper was that e-business security can only be effective if it is regarded as part of an overall corporate information security risk management policy. The author proposed a six-stage security management strategy in this paper. The limitations of this paper are that implementing the framework were lack of building blocks in place and it was very costly for a company to developing software regarding to the increasing of the security. Winch and Joyce mentioned that the dynamic nature in building and losing trust in business to consumer (B2C) EBusiness in an effort to better understand the casual nature of trust.

The purpose of this paper is not to present yet another model, but to suggest how to move from the information and knowledge those models provide into a better understanding of the problem of trust in B2C. Past models are largely descriptive and static in nature. This work helps to give a new understanding of trust building and maintenance as a dynamic process within what is, in significant part, a closedloop system. The paper has, therefore, taken the stock-flow diagramming approach from business dynamics modelling to reflect the structure of the trust building systems. This emphasized that the management of system levels, such as trust, has to be through the control of the in and outflows - if a company

needs to build trust it has to work through the flows resulting from consumers' beliefs about how and whether problems might arise. The limitations of this paper are that it did not mention that how can they reduce actual risks in the company and its process and in etransactions itself, and how can they ensure perceived risks close to reality. Sharon discovered that business applications provide critical linkage between customers, suppliers, and partners. Enterprises today have realized that their success will necessitate considerable attention to the security and privacy of their application software, and particularly their e-business applications. Vulnerabilities and threats related to ebusiness application programs can be seen as occurring at all the different levels of the application system. All of these vulnerabilities and threats result in loss of confidentiality, integrity and authenticity. This paper highlighted the methods and recommendations that can be utilized by organizations working through the complex maze of application security.

V. DISCUSSION, ANALYSIS AND FINDINGS

Problem: Lack of trust

It is known that e-commerce has becoming one of the most important elements in running business successfully particularly for small business. Managers have realized on how e-commerce can benefits their business and thus, many organizations have started their business online. Internet is becoming more and more powerful tools for a firm to run their business as internet helps to connect the stakeholders from all over the world which has improved the efficiency of an organization. The customers who are buying their products online will face another risky problem on dealing with the vendors where the vendors cannot be observed, and sometimes they are unknown.

Besides, customers not only have to receive the products which are unacceptable in quality, but they have to face the risks of not receiving the items they had ordered at all after they made their payment through online. Moreover, personal information and credit card numbers of customers might disclosed to other people during or after their online trades when the vendors are incapable to protect the customers' data. Due to the reason stated above, it in impossible for customers to do their online trades safely and because of those cases happened before, it caused the customers to lost their confident in buying through online and it does make customers lost their trust towards online trading.

Solution: Confidence of trust To solve this major problem of trusting in E-Business, a large amount of trust will be very important to prove to the users that the certain website which the users are accessing are trust worthy.

The trust makes a website in a good condition and all the users who are using it will feel comfortable dealing any type of business with them. As the issue of trust occurs in everything in the internet and E Business, it is very important that the value of trust is big and it is able to gain the trust and the loyalty of the users and making sure that they stay loyal to

the particular website. This trust can be achieved by taking few steps which can help gain this trust. The steps are making sure that all private data about the user are kept safe, well maintained and kept updated. By doing this we can prevent the lack of trust a user's puts towards the particular website. When we have enough trust amongst the users, an E-Biz website can perform well and at full speed and makes sure that all the information are kept safe and making sure that no hackers go through the website and steal users information.

Problem: Unaware of How e-Business

Transactions Take Place E-business has made an organization to run their business more efficient where the customers can get their products just in time. Through e-business like by using extranet, the suppliers are able to access to an organization's database on when the want to receive what they have ordered and that enable them to make the products available to the particular company just in time. Besides, with the co-operation from suppliers, a company can try to have their products sent to clients' house on the time.

Solution: Being aware of e-business transaction

The issue of being unaware of not knowing about how online transaction works can lead to a lot of issues as stated above. This problem is a threat to users who don't seem to understand that their money can be blacked out if hackers hacks their account. To prevent this problem, the E-Biz has to make sure that they have enhanced versions of security and good transaction system for the users to cash in their money. By making this transaction system secure, we can no longer be afraid of hackers. In the meantime, E-Biz needs to teach the users about the online transaction system.

By teaching them how the system functions, users can learn and they too can be aware of the system's processes. All this learning will alert the users to be more caution on their online transaction. E-Biz websites with online transaction systems should list down all the possibilities of doing online transaction and all the misuses possible.

Problem: Degree of Confidentiality Involves

There is uncountable of ways that and e-business set up will be attacking by hackers, crackers, and disgruntled insiders. These have immediately decreased the degree of confidentiality of clients towards e-business. According to confidentiality is defined as making information accessible to authorized users, and prevents the access from unauthorized users towards information. The problem of degree of confidentiality is always taken place in health centre. The recent surveys reported by Georgetown University Institute for Health Care Research and Policy contain statistics regarding to the people's concern for the confidentiality, there were about 63 per cent of internet "health seekers" and 60 per cent of all internet users oppose the ideas of keeping medical records online, even with a secure, password protected site since they worried that other people will see the detail of their records.

Majority of internet users are worried about others finding out about their online activities where 89 percent fear that

internet companies might sell or give away and 85 per cent fear that insurance companies might change their coverage after finding out what online information they accessed.

Solution: Making sure that degree of confidential is reached

Organizations have to keep secured of clients' personal information and stored in a way that it is unable to be accessed by other unauthorized users. In order to build the confidence of users, the system has to be secured and tight so that no bugs or viruses could enter the website or the transaction system.

This prevention of this system can enlarge the safety and can ensure the safety of the users using the system and this confidentiality is essential because of the fear towards forgery and hacking. Confidential are privacy of data and safety of an individual's property and assets. In E-Biz, hackers always are on the wait for any loophole to enter the system and hack information about the user's confidential folders. In these folders, there may be a lot of important information which can be useful and harmful to others. By using this powerful system, hackers will find it difficult to hack the system, and due to this users will have more confident on the EBiz website and they will certainly cash in their money and deal their businesses thru the internet.

Problem: Out-dated Law and Regulation

Internet enables people to find new opportunities in running their business but at the same time, criminals have find their new ways to crime others and criminals nowadays tend to use cyberspace for crime. There are several factors that had been recognized to be the potential factor in the growth of crimes where one of those factors is outdated law and regulation.

New technologies are changing frequently and the changes of new technology is much advanced and faster enough till the criminal laws of some jurisdiction have not caught up with the challenge of new technologies (Tan, 2004). Some countries may have address the threat , and some of these laws are already in need of amendment to address the new kinds of cyber-crimes, but there are still several countries especially those from developing and less develop areas are under the condition of not seeing cyber-crimes as an important issue that must be addressed (Tan, 2004) and there are only several countries that have attempted to address the issue of prosecuting cybercrimes committed by criminals from another jurisdiction. Therefore, it is not hard to find out that some of the countries cannot even recognized the types of crimes occurred and the criminals who are conducting the crimes.

Solution: Updating the law & regulation

Cyber-crime is a serious issue and hackers are a real threat to E-Biz. All this threats can give severe break down on E-Biz websites if proper care is not given. And sometimes users may think that the law and regulation in the internet are lousy. We have to prove them wrong by giving updated law & regulations which will help keep an E-Biz safe and secure. Laws & Regulation are very important to prevent the users to miss use their priority and their freedom and to not do useless

things such as hacking to others account and getting away with it. Frauds in E-Biz can be punished and jailed if all this laws & regulation are kept well and updated regularly. These laws must be strict and the people who misuse the system. Any misuse and misconduct of the system have to pay the penalty.

VI. RECOMMENDATION

In my opinion, the concepts and theories on e-business trust and security can guide the managers and companies to develop their own unique customer retention strategies. While developing trust between companies and customers in e-business, managers should understand that different service qualities might lead to different level of customer buying behaviour and customer retention. The security systems are strongly needed to handle the process of developing the customer retention strategies in e-business transaction process in an attempt to capture the relationship within organization and with the customers. The benefits of applying trust and build up security in e-business is quite obvious. To develop a better relationship between customers and e-business, there are certain steps that could be considered for future preferences such as the attitudes of employees towards the customers, the usage of technologies in developing security in e-business transaction, and protect customers during business transactions. Researchers have caused executives to think on what do exactly customers want? And it was concluded that companies have to find best solutions in improving service quality and develop trust in relation between e-business and customers.

VII. CONCLUSION

The development and improvement of technologies have brought successful towards e-business. High technologies have attracted people misuse the technologies such as hackers and cybercrime which they can access to e-business privacy easily. Thus, e-business companies should build trust and using security during the business transaction. To provide value to the customers through service and goods provided, research found that companies should build up trust and security to protect their customers. Benefits of application trust and security include improved customer service, build customers trust, avoid the misuse of technologies, protect customer's privacy and maintain the companies' reputation. In order to create an effective infrastructure for securing E-business, it requires a comprehensive development of several elements including laws, policies, industry self-regulation, technical standards and law enforcement. These elements may provide positive environment and infrastructure to support the growth of ebusiness and relation with customers.

Therefore, Governments and businesses need to work together to improve consumer trust and security are attempt to increase transactional efficiency and effectiveness in all aspects of the design, production, marketing and sales of products or services for existing and developing good relation

through the utilization of current and emerging electronic technologies, which will gain the more confidence in e-business. Additionally, the government itself needs to re-examine existing regulations to ensure protection for the e-business.

VIII. REFERENCES

- [1] Alan, D. S. and William, T. R., 2002 "E-Lending: Foundations of financial and consumer marketing in an information intensive society," *Journal of e-Business and Information Technology*, Vol. 3, No. 1, pp. 5-19.
- [2] Lord, P., Mary, A. and Kristy, B., 2002, *Managing e-Business Security Challenges*, an Oracle White Paper, U.S.A.: Oracle Corporation.
- [3] Mukherjee, A. and Nath, P., 2007, "Role of electronic trust in online retailing: A re-examination of the commitment-trust theory," *European Journal of Marketing*, Vol. 41, No. 9/10, pp. 1173-1202.
- [4] Salo, J. and Karjaluoto, H., 2007, "A conceptual model of trust in the online environment," *Online Information Review*, Vol. 31, No. 5, pp. 604-621.
- [5] Shalhoub, Z. K., 2006, "Trust, privacy, and security in electronic business: The case of the GCC countries," *Information Management and Computer Security*, Vol. 14, No. 3, pp. 270-283.
- [6] Sharon, H., 2005, *Engineering eBusiness Applications for Security*, Symposium on Information Systems Assurance Integrity, Canada: Privacy.
- [7] W. C. and Sculli, D., 2002, "The role of trust, quality, value and risk in conducting e-Business," *Industrial Management and Data Systems*, Vol. 102, No. 9, pp. 503-512.
- [8] Srinivasan, S., 2004, "Role of trust in e-Business success," *Information Management and Computer Security*, Vol. 12, No. 1, pp. 66-72.
- [9] Tan, S. K. 2004, "Current challenges of developing a legal infrastructure for securing e-Commerce," *Proceedings of the Unescap Regional Experts Conference*, pp.149-158.