Review of Literatures

Since the days of the invention of computer the research continued for safe and secure data transfer from one end to other. This dynamic with the help of network started playing a vital role in business. Critical research in this field are the foundation pillars on which the future research work continue its journey and research conclude to the new unknown to emerge as known and serve to the society. If we ignore the previously done research work put in the form of literatures our work is likely to emerge as duplicate work. E-business is a powerful tool for business transformation to 21st century that allows companies to enhance their supply chain operation reach new market and improve services for customers as well as for providers.

**US GAO Security Certification Authority (1999a,b) -** This aspect of security policy is where vulnerability are handled. Vulnerability is often the first thing to address that is where the organization and the system administrator tend to have the most control. This is the area of security risk management that is principally a technology issue. At the moment, businesses are using various proxies for best practices as substitute for overall security strategy. Security Certification Authority that will certify that best practices procedures have been effectively deployed.

**Eben Otuteye, Faculty of administration, University of Brunswick, Canada (June 2000) -** This paper is in two parts. The first part presents an outline of the significance and impact of information security for e-business with emphasis 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. The consequence of each type of security breach is discussed and various technological solutions...
are presented. The present approach is inadequate primarily because the solution tends to be threat-specific, technology centered.

**Greg Shanton (2000)** - There is almost an uncountable numbers 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. From a business perspective Denial of Service attacks appear to be be most serious threats. Effective information security policy must have the following six objectives: Confidentiality; Integrity; Availability; Legitimate use (Identification, Authentication and Authorization); Auditing or Traceability; and non repudiation. If these objectives could be achieved. It will alleviate most of the security concern.

**InformationWeek Research's Global information Security Survey(2000)** - It is relatively easy in today's internet world to create alter and transmit information. The advancement in computing capacity and inter connectivity has presented a situation where small efforts can cause potentially large losses. Both accidental and incidental breaches are easier and more likely. This is a major challenge to businesses that want to take advantage of the current information technology.

**Davidson M.A. (2001)** - Davidson proposed that having business on internet offers potentially opportunities for increasing efficiency and reducing costs but it also offers unlimited risks. The much greater access to data will attract hackers and criminals. The author identified the importance of business security will bring benefits to e-business. The examples of security systems are virtual private database, which provides a set of tools to enforce fine gained access control within the database and oracle label security which is useful for hosting environments in
which access to information can be formalized. The limitation of this article is that author has not explained details about the impact of security in e-business.

**Alan D.S. and William T.R. (2002)-** They stated that one of the most important issues in e-business 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 are not familiar with the lender, it stated that borrower will not proceed to exchanging personal information without a sufficient level of confidence and the impact is the customers will not pursue 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 customs informed through web presence and shared database where the paper was not included.

**Lord P. and Marry A. and Kristey B. 2002 -** This paper discussed the e-business is essential to reduce the cost resulting from less overhead, greater economies of scales and increased of efficiency. The author examined that the Internet provides greater access to data, not only to legitimate users, but also hackers, disgruntled employees criminals and corporate spies. But making business information accessible via the internet increases the number of users who may be able to access the information. Internet creates challenges in terms of scalability of security mechanism, management of those mechanism and the need to make them standard and interoperable. It is essential to have security for e-business but one of the limitation the author did not focused is it needs highly cost to develop and maintain it. Besides it is costly to hire an expert to develop and manage it especially if the company is only a small or medium enterprise.
**So W.C and Sculli D. (2002)** - This paper sated internet technology and business trust, consumers privacy and security. Trust must exist at all levels for the maintenance of cooperation fundamental for any exchange and most routine of everyday interaction. Now a days in uncertain and uncontrollable future trust has become an important factor in needed in buyer-seller relationship in order to facilitate the transaction. The limitation of this paper is that it did not state about the problems may occur when applying trust in business transactions.

**Eben O. (2003)** - There is uncountable of ways of ways that an 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 this paper 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 center. The recent surveys reported by Georgetown University Institute for health care research policy contain statics regarding to the people's concern for the confidentiality. There were about 63% of internet health seekers are 60% of all internet users oppose the ideas of keeping medical record online even with a secure password protected site since they worried that other people will see their records.

**Winch G and and Joyee P (2006)** - This paper mentioned that the dynamic nature in building and losing trust in business to customer (B2C). E-business is 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. This work helps to give a new understanding of trust building and maintenance as a dynamic process within what is, in significant part a closed
loop system. The paper has therefore stock-flow diagramming approach from business dynamics modeling to reflect the structure of the trust building systems.

**Mukherjee A. and Nath P. (2007)** - This paper deals with 'Role of Electronic Trust in online Retailing. Trust and commitment are the central tenets in building successful long term relationship in e-business. 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. The limitation the paper has not discovered is fraud may increase since customers might not received the goods they had ordered; sometimes the goods are not reached to the customers.

**Salo J. and Karjaluoto H. (2007)** - This paper deals with "A conceptual model of trust" in the online business environment. Trust being the first and foremost requirement to establish electronic data transfer. If business partner could not trust each other a business entity could not be established.

**Manivannan Senthil Velmurugan (2009)** - Electronic business is revolutionizing the way of communication between internal and external stakeholders in an organization. E-business can lead to a competitive advantage and at the same time increase profitability. There are several factors resulting on the success of secure e-business. One of the most important factor is 'Trust'. Acquiring customers' trust depends on many things that an e-business controls. Some relating factor for gaining customers' are: Appeal of website, service offering, quality of service, branding through transaction, information contents, product, technology, and institution very little. There are huge numbers of impact on the way businesses think about designing,
developing, and deploying web based application. 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 the security in e-business and also addressed security concern in web service. This paper focused on trust from transaction perspective and discussed on the role of trust and what business could do in building customer trust. It is between the end operators but when data on net also need security and maintenance of data privacy is the part of trust building.

**Pandey Dherander and Dr. Rastogi A. (2010)** - The paper mainly concerned with the study in which how we can make our electronic transaction more safely and protective and also concerned with research of the security technology, key technology and current application protocol of payment transaction on network and give useful suggestions and counter measures for the development of protective payment transactions.

**Venkat Vijay K Dhurbhakula and J Kim (2011)** - This paper propose a Country-Business-Technology-Government based e-business frame work for nation. Research model include for dimensions for development of e-business in a nation. They analyzed proposed model empirically with a set of data. The result of the study support for all the dimensions being strongly significant. Country administration and policy makers can use the proposed model as guide for e-business development for the country.

Both accidental and incidental breaches are easier and more likely. This is a major challenge to businesses that want to take advantage of the current information technology. [HREF 1]

Effective information security policy must have the following six objectives-[HREF 2]

- Confidentiality
Integrity
Availability
Legitimate use
Traceability
Non repudiation.

A overwhelming majority of internet users are worried about others finding out about their activities: eighty-nine percent of internet users are worried that internet companies might give away or sell information, and eighty five percent fear that insurance companies might change their coverage after finding out what online information they accessed.[HREF3]

Availability means that systems, data, and other resources are usable when needed despite subsystem outages and environmental disruption. Lack of availability is essential loss of use.[HREF4]
Conclusion

The development and improvement of technologies have brought success 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 built security circle around business entity. Companies should built security and trust to protect e-business customers. Benefits of application security and trust includes-

- Improved customer service.
- Built customers trust.
- Avoid the misuse of technology.
- Protect customers privacy.
- Maintain reputation of organization.
- Create effective infrastructure for securing e-business.

It requires a comprehensive development of of several elements including-

- Laws
- Policies
- Industry self regulation
- Technical standards
- Law enforcement

These elements provide positive environment and infrastructure to support the growth of e-business and relation with the customers.