Chapter -1

Introduction

E-business implies the two aspects by way of electronic and the second is commercial activity. E-Business means transaction on networks such as internet which offers fast and effectively solution for realizing various kinds of businesses. In more general sense, we can say any business that uses computer. But today it is mostly done using World Wide Web, Internet, Intranet, Extranet or any combination of these. Businesses also have been engaging in a form of e-business known as electronic data interchange (EDI) for many years. EDI occurs when one business transmits computer readable data in standard format to another business. A good definition mentions the use of electronic data transmission to enhance a business process. IBM has defined Electronic business to be “the transformation of key business processes through the use of Internet technologies”. Today major corporations are rethinking their businesses in term of the internet and its new culture and capabilities. A concept of paperless business is emerging.

As the time plays its own role in growth the end of 20th century made a great deal of business by inventing e-business. The latest technological developments are also playing a vital role in today’s business. Due to this aspect the growth in use of technology is exponential. With the invention of technology wide range of e-emerged such as – e-mail, e-cash, e-return, e-commerce, e-business, e-banking, e-ticket, e-governance, e-learning, e-auctions, e-process, e-network etc. As every coin has two phases similarly the advent of the technology is misused by the hackers and cyber criminals by playing their role too.

E-business needs to provide safe services for participants. It is the main concern of electronic transactions. Safety regards to the risk security and trust associated by the participants in e-business. Requirement of development of trust, confidentiality and privacy are key concern to e-business. 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. This becomes even more difficult when dealing with e-business specifically. Protection of any electronic file or record from unauthorized access and ensuring safe transmission and data storage of such information is key concern. Computer and networks originally were built to ease the exchange of information.

What will information security be like in the 21st century? Networks are designed to sharing and distribution of data and information. Controlling access to these resources can become a problem because we need to balance the requirement for access to free information with the value of the content of that information.
Early information technology infrastructures were built around central computers or mainframe solutions while others were deployed around the personal computer. What some thought impossible became reality and today businesses are driven by the power of the personal computer with new possibilities for crime by stealing access to information and create disastrous effect on computers, networks or information. Keeping this fact in view the need for security arises to counter the security threats on business entities. A security plan is an absolute must for companies that are serious about protecting their assets while doing e-business. E-business security plans are unique and must be developed through a series of steps. While the plans are unique the steps taken by companies can be very similar. E-business can be defined as the use of the internet to network and empower business processes, electronic commerce, organizational communication and collaboration within a company and with its customers, suppliers, and other stakeholders. E-commerce is the buying and selling, marketing and servicing of products and services via computer networks. Since e-business includes the process of transacting with suppliers and customers there is an overlap in activities with e-commerce. Although the terms ‘e-business’ and ‘e-commerce’ are often used synonymously, the distinction between them lies in the broader range of processes in e-business that incorporates internal transactions within an organization. These include transactions relating to procurement, logistics, supply chain management, payments, stock control and order tracking. As Chaffey (2004) [51] notes, e-commerce can best be conceived as a subset of e-business. Where the two concepts overlap is in the buying and selling of products and services.

“The very idea of a public communications network as a global market is commercially appealing. Indeed, even from a security point of view, it makes more sense that we do our transactions on the same communications network than that we drive on the same roads” [25].

Continuous development of technology and its use in business security has become a major concern of business community wants to take edge over their competitor. Criminal attacks and intrusions into computer and information systems are spreading quickly and they can come from anywhere and everywhere. Intrusion prevention measures, such as user authentication, firewalls and cryptography have been used as the primarily protection to protect computer and information systems from intrusions. As intrusion prevention alone may not be sufficient in a highly dynamic environment, such as the internet, intrusion detection has been used as the secondary protection intrusions. However, existing cryptography-based intrusion prevention measures implemented in software, have problems with the protection of long-term private keys and the degradation of system performance. Moreover, the security of these software-based intrusion prevention measures depends on the security of the underlying operating system, and therefore they are vulnerable to threats caused by security flaws of the underlying operating system. On the other hand, existing
anomaly intrusion detection approaches usually produce excessive false alarms. They also lack in efficiency due to high construction and maintenance costs.

Popularity of the Internet and the World Wide Web, computer and information systems have increasingly become the targets of criminal attacks and intrusions. Attacks spread very quickly and they can come from anywhere on the globe. The reported number of computer and network attacks rises sharply every year. Therefore, finding the best possible ways to protect valuable information and computer systems against intrusions is crucial. An attack, or intrusion, on a system is a security policy breach. Most attacks cause security policy breaches in very specific ways. For example, certain attacks may enable an attacker to read specific files, but they do not allow the attacker to modify any system components. Another attack may cause a system service disruption to authorized users, but it does not allow the attacker to access any files. Although computer and network attacks vary in types and capabilities, they usually cause breaches of four different security properties of the system:

- **Confidentiality:** An attack causes a confidentiality breach if it allows unauthorized access to data.
- **Integrity:** An attack causes an integrity breach if it allows unauthorized modification to the system state or data.
- **Availability:** An attack causes an availability breach if it keeps authorized users from accessing a particular system resource when they need it.
- **Control:** An attack grants an attacker privilege to interfere with system operation in violation of the access control policy of the system. This can lead to a subsequent confidentiality

“Secure flow of information in e-business is hard”, says Anderson, in an article with a similar title [5] and continue that management of e-business security is a much deeper and more political problem than is usually realized; solutions are bound to be understated and incomplete, while many simplistic approaches are bound to be fail. The main key to understand the problems that exists in e-business security argues Bishop [153] that the problem involved are not new but growing exponentially. Problems are long-standing but the reality has changed primarily because of advances in technology and its use in modern business. Development of www and other communication technology has been central issue in organizational business theory, says Orlikowski [279].

With the arrival of e-commerce and e-business in late 1990s and their growth in 21st century the issue of security has becomes acute, as these new models of doing business necessitate the use of information technology and give very large number of people access to an organization’s network.
Network level security is widely practiced in order to protect organizational internal resources, and the dominant security management approach called perimeter security. This approach is designed to protect organization by limiting connectivity between the external world and the organization’s network resources.

Perimeter security implies the existence of a logical defensive boundary around specific resources. The goal of securing the perimeter is to prevent malicious or unauthorized users and applications from accessing the company’s resources and the various business functions that they support.

1.1 Challenges
Research illustrated in this thesis brings together two disciplines - e-business and information security. With the significant increase in adoption of the e-business mode [220], the importance of security as a major factor in e-business success has been widely recognized and commonly shared [21,241].

The challenges addressed here is to develop a model for e-business security that provides an alternative approach to both the way security is viewed and the way it is designed and managed, while keeping in mind that organizations and information technology systems are complex dynamic systems. This means that the various elements of these systems must be analyzed separately and the selection of security safeguards must be appropriate to the individual elements.

This challenge is addressed here by the definition of new security model together with a model and methodology for the design and management of e-business information security.

1.2 Research purpose and objectives
The existing perimeter security model, as discussed in chapter 4, is no longer relevant for modern e-business environments. Therefore, there is a strong need for an alternative approach. The purpose of the research described in this thesis is to develop a security design model for e-business organizational information systems, based on a new model. The objectives of the research described in this thesis, as derived from this purpose, are:

- To introduce a new model for e-business information systems security design.
- To develop a working methodology for e-business information security management based on this narrative approach.

1.3 The Proposed Model
The new model for e-business security proposed here is Electronic Business Security Model (EBSM). The selection is based on the core characteristics of an e-business performing business process by means of electronic information flow. Using this new security model, a methodology for its implementation is presented in the form of an EBSM.

1.4 Research Approach
The research described in this thesis complies with the principles of qualitative interpretive research in these disciplines of information systems and information system security. A mixed approach to research methods namely using design theory/design science methods and the case study method has been used to perform this research.

1.5 Contribution

The suggested model and the associated methodology provide e-business organizations with a tool that enables the design of a rational information security plan for organizational information security which is effective, efficient and comprehensive. This work provides an example and verification of widely discussed research methodologies and methods and as research in e-business security design and management, the thesis provide new knowledge regarding e-business security which can cover future research on this topic.

1.6 Contents

The structure of the thesis reflects the way in which the research was performed. The first step, after defining the purpose and goals, was to decide on the research methods, which are described in chapter 2. Given the fact that the described research falls within the field of Information Systems, the research methods from this discipline were reviewed in order to determine which fit best to the specific research goals. The selection of an appropriate research approach for conducting-business security research is even more challenging, since information system security research is relatively new, and the research theory is constantly being enriched. The selection of the research methodologies and methods must take into account the unique characteristics of this discipline. A review of approaches and methodologies used in research is presented, together with an analysis of their appropriateness to the focus of the challenge addressed by this thesis. Chapter 4 is dedicated to a discussion of the e-business mode of doing business. The subject is approached from both organisational and technological perspectives, as a comprehensive understanding of the subject is needed in order to identify and formulate the security requirements for an e-business organisation. The model which is presented in chapter 8 must provide a means of meeting and addressing these requirements, in order to ensure that e-business information systems are secure. This chapter explains basic business and organisation concepts, and discusses the integration of information technology within a business environment. The notion of an e-business is defined, and models for e-business are described. The information system security domain is presented in chapter 3. This review makes it possible to identify the problems that need a solution. To help structure the discussion, an information system security conceptual framework is also presented. Such a framework enables us to present a comprehensive picture of the subject in a systematic way; it is also helpful because of the wide variety of definitions and interpretations of commonly used terms.
in information security practice and research. This is followed by a discussion of security issues for an e-business. In today's business environment, organisations can perform critical business operations via Internet-based e-processes, and hence the correct execution of such e-processes is of critical importance.

The next chapter (chapter 5) discusses the characteristics and properties of an e-process, and looks in particular at the specification of an e-process. The structure of an e-process is identified here primarily in terms of information flows based on business logic. Information flows are discussed in chapter 6, which introduces the concept of an information flow as it is used in this thesis. A case study is presented in order to illustrate information flows in practice. Previous relevant work on information security issues is presented in chapter 7. The review includes research on issues with perimeter security, business process security, and information flow security. The newly suggested model is presented in chapter 8. In this chapter a new security model, the Electronic Business Security Model (EBSM), is presented. This model proposes that the security of an e-business organisation should be designed and implemented according to the security requirements of individual e-processes. A new security septet is proposed, and a methodology to meet the requirements produced by applying the EBSM is presented, i.e. the Electronic Business Security Model (EBSM). Chapter 9 demonstrates the practical implementation of the newly suggested security model, methodology and model using a case study analysis. The focus of this case study is an airline company that practices the e-business mode in its business activities. Chapter 10 provides a summary of the main contributions of the thesis, together with a brief review of possible directions for future research.

1.7 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.

1.7.1 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.[269]

1.7.2 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 [74].

1.7.3 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 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 [88].

1.7.4 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 [105].

1.7.5 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 [66].

1.7.6 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 [23].

1.7.7 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 [152].

1.7.8 So W.C and Sculli D. (2002) - This paper sated internet technology and business trust, consumer’s 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 [257].

1.7.9 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 with a password protected site since they worried that other people will see their records [75].

1.7.10 Winch G 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 [289].

1.7.11 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 [182].

1.7.12 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 [250].

1.7.13 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 and need security and maintenance of data privacy is the part of trust building [179].

1.7.14 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 [204].

1.7.15 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 results of the study support for all the dimensions being strongly significant[273].