Electronic Business Security Model (EBSM)

Bijender Singh Yadav
Research Scholar, JJT University Chudela (Jhunjhunu)

Abstract

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. The development and improvement of technologies have brought success towards e-business. High technologies attracted people misuse the technologies such as hackers and cybercrime which they can access to e-business privacy easily. This article examines the issues related to the security of the assets and transactions in the e-business components and activities. Since a large business community is involved and public money at large invested in business, role of information security and privacy is not blown up in this kind of business. This article identifies the need of security, essential components of security and their importance to protect e-business from threats. Thus e-business companies should built security circle around business entity. Company should built security and trust to protect e-business customers which in turn will improve e-business prospective. This paper undertake descriptive study on security threats determining the quantum of risk of security threats on e-business and develop a model of total security for secure business transaction using e-business platform.

Introduction to e-business

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.

E-business implies the two aspects by way of electronic and secondly a 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.

With the fast growth of the Internet and the World Wide Web, security has become a major concern of many organizations, enterprises and users. 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.

The latest technological developments are playing 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 the time plays vital role in growth the end of 20th century made a great deal of business by inventing e-business. 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.

Security overview.

E-business security is the protection of e-business assets from unauthorized access use alteration or destruction. A secure system accomplishes its task without any side effect. Any unprocessed weakness in an e-business system is loss of vital information we can say that the e-business should have all the characteristics that follows. Any organization dealing with e-business system has to be able for assuring these characteristics otherwise massive loss of information can be noticed. Keeping track on what has happened and providing the following characteristics an e-business community can do its desired business activity without concerning too much for the e-business safety.

Privacy- Provision of data control and disclosure.

Authenticity and Availability- –
Authentication of data source and Prevention against data delays or removal

Non-repudiation- Prevention against anyone party involved in a transaction denies having taken part. This is totally a trust issue. The e-business can only establish whenever and wherever trust between two parties establishes.

Integrity – Prevention against unauthorized data modification.

Confidentiality- Protection against unauthorized data disclosure

PAIN - Security requirements – Any secure e-business system must meet four integral requirements (a) Privacy, (b) Authentication (c) Integrity (d) Non-repudiation

Privacy (Confidentiality of data) – It means e-business information is accessed and changed only by authorized parties. This is achieved by encryption of data before transmitting over an open channel of communication such as Internet. Encrypted data may be interpreted by the hackers but cannot be decrypted within a short span of time. For extra security data can be stored long term in an encrypted format.

Authentication - In online business the best defense against being misled by an imposter is provided by unforgivable digital certificates from a trusted authority, Although anyone can generate digital certificate for themselves, a trusted authority demands real world proof of identity and checks its validity before issuing a digital certificate. Only certificates from trusted authorities will be automatically recognized and trusted by the major web browser and e-mail client software. Authentication can also be provided by physical property of a person, physical token such as PIN only known to the person involved.

Integrity (Integrity of data) – Integrity of information means that an information received has not been altered or tampered with. If someone is receiving sensitive information online, he not only wants to ensure that it is coming from who he expects it to, but also that it has not been intercepted by a hacker while in transit and its contents altered.

Non-repudiation – It is the ability to guarantee that once someone has requested a service or approved an action, they cannot turn around and say "I didn't do that!" This characteristic allows one to legally prove that a person has sent a specific request for a service or made purchase approval from a website. In e-business non-repudiation is achieved by using digital signature.

Authorization – It allows a person or a computer system to determine if someone has the authority to request or approve an action or information. Authorization is tied with authentication. If a system can securely verify that a request for information or a service has come from a known individual, the system can then check against its internal rules to see that person has sufficient authority for the request to proceed. Online authorization can be achieved by an executive sending a digitally signed e-mail. Such an e-mail once checked and verified by the recipient, is a legal binding request for a service.

Threats to e-business Security – The threats relevant to the life cycle of a business entity covers the following –

- Client computer threats – The main threats caused the concern of today's e-business community is spray of bundled viruses, active contents, Trojan horse etc.

- Communication channel threats – The threats on the data/information during transition of information from one end to the other through communication channel are sniffer program, denial of service, spoofing and backdoor.

- Server threats – Spamming, privilege setting, common gateway interface etc

Minimize security threats – Any procedure that is employed to recognizes, reduces or eliminate a threat is called a countermeasure to the e-business threats. This includes intellectual property protection, client computer protection, communication channel protection and server protection. Steps to minimize security threats-

- Carry out a risk assessment
- Build up a security policy
- Create an implementation plan for security policy
- Develop Disaster recovery plan
- Build a security institute
- Perform a security appraisal.

The e-business industry faces a challenging future in terms of security threats and it must avert the same to explore the possibilities of 21st century global market. Increased technical awareness and wide spread availability of internet, misuse of invent of technology has geared up and attracted the criminal to be more sophisticated in the deception and attack they can perform. Attacking plans and vulnerabilities get exposed once a perpetrator has exploited them. There are multiple security strategies which any e-business community can instigate to reduce the risk of attack and not to compromise significantly awareness of the risks and implement multi layered security procedure

Proposed secure model – In an e-business architect security model deals with the Clint Security. Sever Security and Communication Channel security.

E-Business Security Model (E-BSM). The method and model are built on the assumptions such as :

- Complex system.
- Single Process Stage Management.
- Parts of an e-process
  - Business logic
  - Information flows
- Security design e-business security must be designed to meet the requirement of business logic as well as information flow.

These basic ethics, together with the defined building blocks, helped us to prepare the new e-business security model, which is discussed next.

E-Business Security Model should be designed to secure business logic and information flow of individual processes. To achieve this we need to adopt –

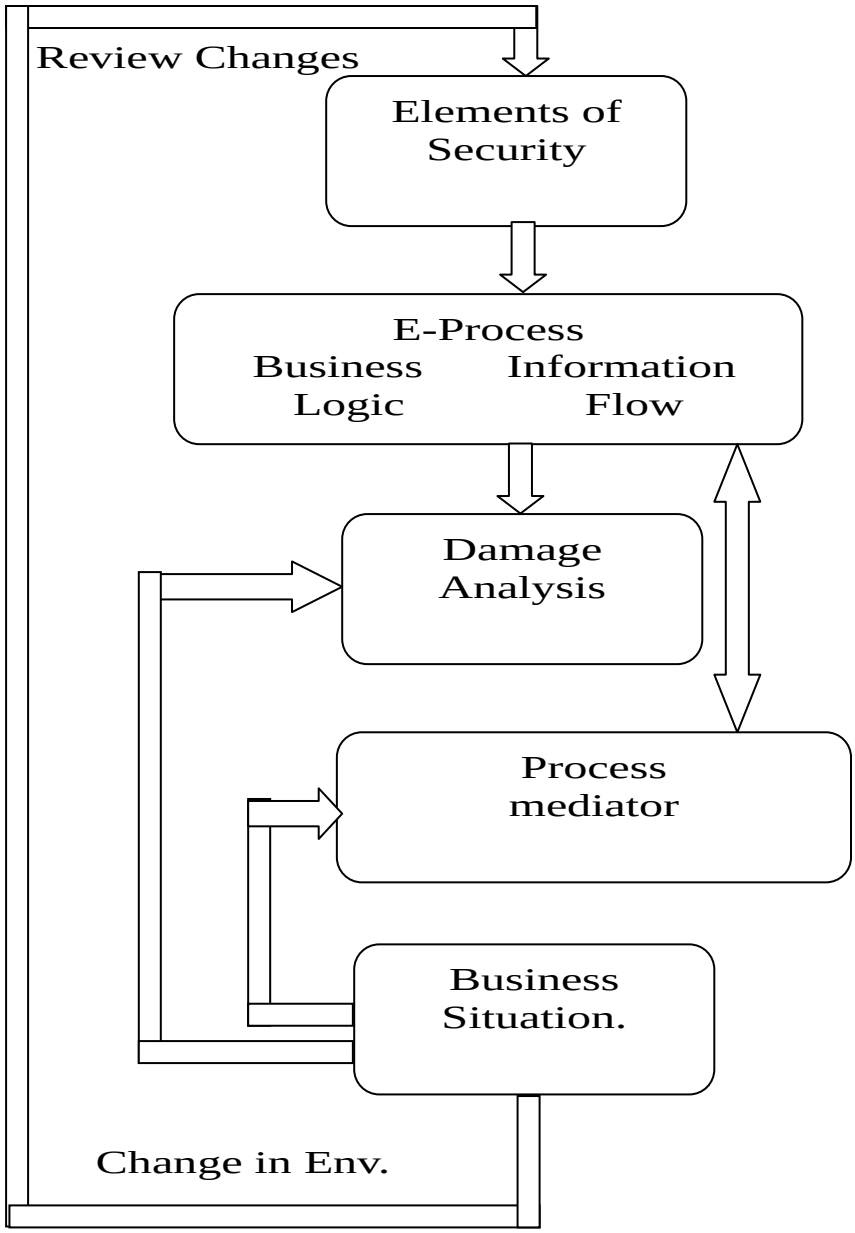
- Damage analysis
- Process agent analysis

Change in e-business circumstances such as (one amongst the following or the combination of these)

- People
- Technology
- Organization

Resulted in need of an updated e-process security

Figure 1 Proposed New Model



Conclusion

E-business is growing exponentially. Technological development facilitated the growth in every aspect of life. The advancement in computer technology and communication

technology changed the way of business. With the change of style of business laid the road map of change in security requirement. It is a continuous process.
Security requirement depends upon the business environment as the business environment gets altered by means of change in any one or combination of people, technology or organization. Any moderate change in aforesaid elements will need an alteration in security policy. The requirement of security is a continuously changing aspect of business. What is up to date today is going to be obsolete tomorrow.
The E-BSM model manages the e-business information security. It is a management tool designed for use in the design, implementation and maintenance phases of information security in an e-business organization.

References :

[1]B. Dahlbom, Postface, Oxford University Press, 2001.

[2] Burns S 2002 Unique Characteristic of e-commerce and their effect upon payment system Ver. 1.3

[3] Computer Insecurity Springer Verlag, London 2005

[4] Majumdar C Barik MS, Das S 2003 Final technical report for project development.

[5] N. Jarvis, E-commerce and encryption: Barriers to growth, Computers & Security 18 (1999), no. 5, 429-431.

[6] P. Jungck and S. Shim, Issues in high speed Internet security, Computer 37 (2004), no. 7, 36-42.

[7] S. Katsikas, J. Lopez, and G. Pernul, Trust, privacy and security in e-business: Requirements and solutions, Lecture Notes in Computer Science 3746 (2005),548-558.