Security in e-business

Business

The Issue of Security in e-business Introduction: Security plays an important role in e-business solutions. Be it removal or sabotage of valuable information, infiltration of spam or unsolicited mail, or distribution of other illegal activities over the Internet, security is very much essential as practical and technical solution to online business enterprises. The main objective of a security plan in e-business is to “ protect the privacy of the people with whom you do business and safeguard your IT and other information assets.” (Rapalus, 2001)

Safeguarding your business:

Information is a significant business asset for any online enterprise. Therefore, protecting it from other competitors in the market is relevant for a business organization. Security for e-business can suitably protect information from a number of threats while focusing on the following perspectives (“ Protecting”, 2008),

Ensuring business continuity

Minimize business damage

Maximize return on investments and business opportunities

In the age of Internet, it is quite easy to create, alter and transmit information. Besides, “ the advancement in computing capacity and interconnectivity has presented a situation where small efforts can cause potentially large losses” (Otuteye, 2003). That is why concern for information security is a must for all small and big e-business organizations.

e-business security objectives:

There are numerous ways to attack an e-business setup by various hackers, competitors and even displeased insiders. e-business enterprisers should conduct evaluation processes on their technological capabilities including multiple areas (“ Approach to e-business security”, 2007),

Core authentication and authorization functions

Security policy setting

Support for existing enterprise software

Manageability

Scalability and reliability

Privacy

Software quality

Above all, protection of information or data focuses on three core elements as pointed out in E-business guide (“ Protecting”, 2008)

Confidentiality: Assuring sensitive data is disclosed only to authorized individuals.

Integrity: Protecting data from improper modification done by annoyed employees.

Availability: Accessibility of IT network, desktop and data resources when authorized users need such access.

Concluding remarks:

Security in e-business is an ongoing process that has to deal with both existing and new threats. A good security program always ensures continuous improvement. It is without doubt that security does add to the cost of business at initial phases. But in the long run, it can do tremendously well in saving money, earning good reputation as well as customers for the company. After all, what matters most in the end of e-business or generally any business enterprise is the trust and credibility one builds and maintains with customers and business partners.

References:

(2007). Approach to e-business security. eCommerce Program. Retrieved from http://www. ecommerceprogram. com/ecommerce/Ebusiness-Approach. asp.

Otuteye, Eben (2003). A systematic approach to e-business security. University of New Brunswick. Retrieved from http://ausweb. scu. edu. au/aw03/papers/otuteye/paper. html.

(2008). Protecting. E-business guide. Retrieved July 17, 2008 from http://www. e-businessguide. gov. au/protecting/about.

Rapalus, Patrice (2001). Guiding you toward secure e-business. 2001 Computer Crime and Security Survey IBM. Retrieved 2002 from http://www-935. ibm. com/services/in/bcs/pdf/g510-3073-guiding-you-toward-secure-e-business. pdf.