Security threats on e-Business

Taking into consideration the logical relation in the chain of business, beginning from consumer to e-business server, e-business related concerns can be analyzed. Many things which should be kept on alert for secured e-Business are the web and e-business servers (including hardware/software), the computers of the clients, and the communicating messages in that transaction channel during process or activity. If the communications links secured only without putting any control measure of security on the above said components or e-business or web services, then there will be full or partial security failure which ultimately will collapse a business. In our study we found three types of security threats on e-business, namely- Server threats, Client threats, Communication link threats. See fig1:

![Diagram: Security Threats in e-Business]

**Fig1:** Types of security threats on e-business
1. The Threats on Server

In any customer and business environment on the server, the server is the important element which provides the e-business links between the users and the e-Business server. The e-business servers have vulnerabilities which can be exploited by anyone planned to cause destruction or acquiring information illegally.

These server threats are again can be mainly of any of the following five types.

**Fig2:** Server Security Threats

1. **Database Security threats:** Most of the business databases contain username/user passwords without keeping in view the security. In any situation some intruder or hacker may get user’s personal important information to misuse the secured data imposing as the authorized user and keeps the private information. It is a fact that user data are kept in e-Business systems from where they and get the beneficial data from their databases. These databases are linked with the web-server. These databases connected to the Internet or web services if mishandled or misused then they may damage or give loss to the companies by changing the information/data or getting important information from them only for their personnel use.
1. **Common gateway interface (CGI) security threats:** These are the programs which on misuse may generate a security problem. These programs can be triggered to fire with their characteristics to obtain their target associated with them. These programs set the changes of all data from server connected to some other program of a database program. These programs put the data or change in data to the web pages they are associated with. Defective or malicious CGI with free access to resources disable the system. CGI can call privileged original programs of the system to finish files, or find confidential data or information which may be passwords or highly secured data.

1. **Security threats to password hacking:** These are the most common and the simplest security threat against a password-based system is to guess passwords. Guessing of passwords requires –

   a) Access to the complement

   b) The complementation functions

   c) And the authentication functions.

   If no one of these three are changed by the passing of time the password is guessed. In that case the hacker uses the password to access the system information.

1. **Internet-server security threats:** The HTTP requests made by the customers are obtained by the Internet-server software which give response and reply on internet web. The web services are attached with these Internet-server software keeping in view the risks. If the software is quite complex, there is maximum possibility of getting coding errors or bugs which are the security weakness holes to provide entry for the malicious attacker.

1. **e-Business server security threats:** The business server/ web-server, responds to requests from web browsers through the HTTP protocol and CGI. The e-business server software suitability with FTP server, mail server, far ends login server and OS. These operating systems (OS) may have security issues.

2. **Client security threats**
Too much applicable advantage and use of active material of internet pages has altered the idea that internet pages can update than display content and give connection to connected pages with desired information.

The content, malicious code and server side attack may leak out the credit card numbers, passwords and customers identities which are generally kept in stored files or cookies. The internet is stateless which never learn a reaction from one web page view to another web page, cookies support in finding the solutions of the problems of learning customer order or passwords and names. The malicious code like torjons, virus can create havoc to security files.

3 Communication linked security threats

The Internet messages pass from a source point to the destination node. Just before arriving the destination node the messages travel into several interlinking computers on the network of that business.

So every computer on the internet through which messages are passed is not safe, secured, and without hostility. There are the three security threats named CIA (Confidentiality, Integrity and Availability).