Solving the Security issues with e-Business characteristics: Impact of security Threats on e-Business

ABSTRACT:

The access to any information is enforced by physical and procedural controls. Making business information accessible through electronic medium greatly enhances the customers’ numbers that can be capable to receive that data using internet. When money is transferred to the web, the surrounding is totally altered. In an office environment, the access to any sensitive information of business is frequently through employees of that business. Companies may very little know or nothing about the users accessing their systems. Our research shows that there is a need for a well-resourced, formal organizational e-business security infrastructure. It required featuring a comprehensive, holistic e-business security management program containing a range of coordinated elements, including an e-business security policy. It is important that featuring an Internet acceptable usage policy is must. Virtualization, Integrated with safety measures with dependability, Interpretability of database- providing information and Security enabled system working automatically are the key factors which can solve the effects of safety concerns in businesses. There is the need for the awareness sessions; monitoring; and a formal compliance process to handle instances of non-compliance.

Key Words:

Survey method, basic advanced technologies, CIA, ten stage security management model, security provision

Introduction:

First IBM in1990’s started a research work on electronic business. Now a day’s big companies are again working on their businesses on electronic or web world. Organizations are working on the Internet to purchase tools and offers from outside organizations, to join on ventures of sales
they are combined to do research. Some trade should not hope for the full success in safety to meet with its requirements. There are the people who will interact with the trade might self impose themselves as other one. It needs for organizations to be better secured and safe in response to fast global shifts with the application and implementation of IT with concerned actions. A design structure change like changed business scenario should be combined with specific safety measurements which shall guarantee the security concerns happening in these should be lowered and finished.

The globalization and slow economy growth has been the main driving factors to give complexities and many methodologies have changed the ever growing business world environment. The commerce surrounding has ever seen spontaneous transforms each time and some specific changes are introduced here. The business process changed the world with the help of advanced technologies. The gain on money expenses may not ever as assumed, and the machines keep aside. This is because knowledge is important in deploying the company shift while going towards an on-demand business in real sense. The on-demand commerce is the way of shifting the trend one see on new researching the commerce from the perspective view of company and its associates, the vendor’s and the workers of the company [1].

In an office environment, the access to any sensitive information of business is frequently through employees of that business. The employees are not always reliable, so the receiving of crucial information is restricted by the work responsibilities given to them. Workers who steal the sensitive data outside the organization should be punished on working against the E-BSP action.

The threat of punishment helps in preventing the unauthorized access of sensitive information. The access to any information is enforced by physical and procedural controls. Making business information accessible through electronic medium greatly enhances the clients’ population that may receive the data through electronic medium.

As the commerce is transferred to the web, the surrounding can completely altered. The organizations can have small knowledge of the customers receiving the information. Our research shows that there is a need for a well-resourced, formal organizational e-business security infrastructure. It required featuring a comprehensive, holistic e-business security
management program containing a range of coordinated elements, including the e-business security policy.

It is important that featuring an Internet acceptable usage policy is must. There is the need for the awareness sessions; monitoring; and a formal compliance process to handle instances of non-compliance.

**Objective and Scope:**

The objective of this paper is to look into various aspects and behaviors of the web users doing businesses and money/fund dealings through Internet, then to analyze reports and security concerns with its effects on Trade/Business.

There is no perfect security or perfect counter solution to the electronic business concerns. Security concerns are the main objectives of any e-Business while using the applications allotted for these security concerns.

The users doing e-Business faces new challenges which he/she wants to fix while dealing with them. His/her main concern is to counter with these challenges and odd situations to get total success in e-Business transactions or processes in changed scenario.

We find that there is no full proof or full perfect security while doing e-Business on Internet in its environment.

The person/corporate to which the user is dealing can be the fake one or replicating itself.

In the changing or rapid processes the IT processes and technologies are the prime responsibilities of the Corporate/Persons so that no failure may take place.

This paper discusses various methods of concerns that systems take in the e-businesses. The IT functioning and security systems of e-Business are required to counter with all related problems or security threats otherwise the corporate or user may lose important or confidential data/information.
This may put them on stake of reputation. Today the Threats have affected the every aspect of e-business. This paper looks into maximum security concerns to the users doing e-Business.

As Internet business is growing day by day its challenges i.e. threats are also growing with it. So the main aim of this study is to know up to which extent it has impact on users and how they are controlled or reduced.

Thus the specific objectives are:

- Recognize different type of security threats and its negative effects to the user doing e-Business. To find out the application style on Web.
- How web jobs and their applications work and take place.
- The users doing e-Business may deal with all or maximum security concerns and may able to counter with these problems/hackers.
- Recognize the friendly environment and be ready to deal the fake one.

**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 security requirements can be studied.

In our study we found three types of security threats on e-business, namely- Server threats, Client threats, Communication link threats. See fig37:
1. **Considering the Threats on Server**

It may be the basic chain on any server-user-web relation employing E-business chain among clients with the computing machine of e-business. 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.
1.(i) Database Security threats:

A few warehouses contain customer-ID/user passwords with very unsafe manner. When some intruder or hacker gets user authentication information, then he can misuse the secured data imposing as the authorized client/user and reveal private and information. E-business machines contain clients’ information and get valuable data through information pools that are linked to the Internet server. Rather business data, information pools linked to the Internet has important and safe data which can spontaneously destroy a corporate as they are destroyed, obtained and changed.

1.(ii) Common gateway interface(CGI) security threats:

CGIs are programs; they can create a security threat if misused. CGI scripts can established for working having the safety to run standard controls. The graphics deploy the changes of all data from web-server to other program. Defective or malicious graphics with free access on resources disable the system. CGI can call privileged root computing works which spoil folders and looking into important data, like- customer ID, and secure words.

1.(iii) Secure word hacking security threats:

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) Complementation functions

c) Authentication functions.

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

1.(iv) Internet-server security threats:
Internet-program is structured to give network sheets answering the hypertext transferred protocols queries asked on net. Internet-server software is not inherently high-risk and is designed with web service. 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.(v) e-Business server security threats:

The business server/web-server, responds to requests from web browsers through the HTTP protocol and CGI. Software has the e-business programs for the server files having full transfer protocols on server which have security holes in them.

2. Client security threats

The widespread use of active content of internet pages has changed the perception that internet pages can work smaller than showing matter giving connections to concerned sheets along with extra data. Content, malicious code and server side attack may open the secured numbers, ID’s, A/C numbers and secured words which are available in cookies-files. Malicious code like torjons, virus can create havoc to security files.

3 Communication linked security threats

Messages in the web pass from one destination to another node. The message travels by many linking systems on the web early to arriving the destination. So every computer on the internet through which messages are passed is not safe, secure, and non-hostile. There are the three security threats named CIA i.e. Confidentiality, Integrity and Availability

Review of Literature:

Any researcher to be able to take this step should be adequately prepared for it i.e. he/she must be amply knowledgeable about the domain of his/her research field/area/topic. Skill of known knowledge, in the field of searching the technologies and processes for the information, is very useful and advantageous. Gathering the net findings of the studies done put the finder in right
track and keep in its own venture. Hence, the theme of concerned literature is always helpful and exiting step.

A.C. & A. Roy[2] have established that frauds doing persons are getting latest or better methods for finding the entry to user’s bank A/C data. Phishing etc are general methods which misguide user to false site.

The CISCO [3] found that little and some greater industries apply the Web and Internet usages to go to some unknown clients as customers and give them something new in better mode successfully. Micro levels corporate utilize their connections to increase the customer approach to them and to have contact with them sharply and in price cutting manner.

As the change and trend in corporate has changed, the meeting of corporate for business can be risky and expansive safety threats. To keep a more trusted, safe, and connected framework is very crucial. It depicted that safety was the largest threat in front of these little or some greater industries. Five safety concerns are worms or viruses, data stealing, trade present, the strange and safety of rule.

A de ter. [4] revealed a group of rules for Safe E-Banking that should be accepted by western Banks. The main purpose of the discussion is to support corporate to deploy safety measurements in their networking tunes depending upon better work in contest to particular threats types. This is clear in stating that dissimilar bank works and exchanges form various threats to them and hence they should meet the same fate. In this note 5 various e-banking services are recognized having 5 threats covers. It highlighted the particular threat cover for their clients fund exchanges. Few clients prefer to the representative the right to arrange the bank activities to another person or aggregators. These provided an attack node to be taken in these 5 risk study. The paper presented a few notes to cover the extra problems.

Vendor A. [5] inspected the upper level of ten safety concerns posing threats to the web trades which were Phising, kernel attacks, worms, aimed folder, and others.

D.A.S. & C.T. U. [6] established that data machines and methods, primarily hoped for supplying trades, with benefits in decision making, were presently directives.
Web process and receiving massages and mails are general matter in SME’s, these are growingly accepting Electronic Data Interchange (EDI).

SME’s were not presently dealing data safety properly. Virus defense and information backups were general in SME.s.

**Methodology:**

We applied Survey method in this study of research. For getting this aim of gathering the connected matter with information of our research, we had to prepared a questionnaire ed using criterion test. These tests were employed in the information gathered applying last questioning for getting the safety concerns lying on the facts associated with the true reactions and results of the users answers to our test.

E-Business Security Threats concerns cover each industry. The companies had chests with locks/keys when the computers were not there. These terms are utilized to elaborate e-Business safety cautions. Web usages for business were limited in mid of last decade of 19th century. Then the business usage of the web was unlocked which started the golden episode of the initiating e-commerce or E-Business. WWW and graphic usages grew immediately with browsing [7][8].

This can be tough to industries to forbid or abolish clients from granting data against the business logics even if they know who their users are. It is crucial that companies manage access to sensitive information by preventing unauthorized access to that information before it occurs. This all occurs through any use of e-Business characteristics. The e-Business Policies of the company should be implemented via firewalls and other technical security mechanisms. These should be supported by other components of the advanced technological programs. We based our review and research on these basic issues and focused on the following four e-Business characteristics:


To minimize complexity for users and making the best use of technology resources, the e-business prefers networks for using the combined strength of calculating machines in the
network available to the clients, corporate and the vendors in the grid. Running information systems way has been changed totally by Virtualization of Database Layer and Desktop Virtualization Solution through the permission of flexibility of hardware and software for the industry. The resources timely expansion of mostly available servers, the optimal utilization must be enabled without problems. There is a need of IT infrastructures to improve manageability and ownership cost reductions at all levels. To adapt rapidly to business demands the enterprises will be empowered. Clearly the database servers will run havoc inside the virtual machines in such environments.

2. Integrated with Safety and Dependability [10]-

Network computers are connected endlessly throughout the company & to all of the customers, companies, and suppliers. Critical software must be safe, secure, and dependable. Confidentiality and availability constitute part for measurement of quality consideration along with integrity. Security and most important dependability are particularly the essential part of qualities while dealing with threats in e-business. Designing usages and support system to the decisions increased the era for the safety tendencies on them.

3. Interpretability of Database- providing information [11]-

Different systems should run in association linking to machines & running various works throughout the global business and regional barriers. Interpretability of databases using data sources for application at the internet traffic disorders provide information for the web jobs and works in helping the recovery of information residing on various places in different resources and files creation. It helps in self generation of folder works. This freelance habit of the active information source is kept safe and generation of the network is permitted by entering and deleting information pool. Additionally, the design helps the technological and architectural difficulties done through the widespread application of various methods and application rules on web and modifies the problem of representing one method in the whole architecture. It is due to data abstraction property of database.

4. Security Enabled system working automatically [12]-
Advanced technology controls and manage the complete management itself. Like the human autonomic nervous system, the advanced technology work automatically by auto-adjustment, auto-curing, auto-performing, and auto-defensing from various attacks.

**Answer for the safety:**

In web related Businesses, safety is seen as main trade initiator [13]. Trade’s safety is useful only in the case of its top priority maintenance as full and complete company threats control rule. ABAS [14] are a system methodology that applies 2 groups of agents: 1.“Network” 2.“Hacker”

Decide business safety attacks by auto-checking and external accounting. Identify the owner of the security plan and action before initiating.

Evaluate- which element is on threat border, what’s the cost to it, and what’s the expense budget to control this. Find whose risk is on verge of loss by whom via connection.

Calculate IT techniques & methods for removing the drawbacks and engage the cure steps.

The advanced technologies respond automatically and work around problems, security threats, and system failures.

The advanced technologies manage software upgradation, balance optimized workload of the overall system performance.

These security enabled systems work automatically, they take action against malicious viruses attack and they can issue denial-of-service attacks on system are:

**Artificial Intelligent Network Attack Detection System (AIN-ADS)**

**Multi agent approach [15]**
Database Security from Malicious Attack [16]

Nullify effects of safety concerns [12]

e-Business Policies and safety measures[10]

Firewalls [17]

Ten Stage Security Management Strategy Model [18]

A few safety concerned fields like works of advertising, need the application of limited, safety measurements, on the other hand others, as client enrolment, need specific better restrictions, to make sure the guarantee with fund and client’s needs. There are various kinds of threats a customer must keep in mind and give an opportunity to see into a few of the safety methods.

CONCLUSION:

Security threat in e-Business can be a method for treating it like battle to look into the attacks and understand their results to create harm. This all is needed before getting some control measurement. While considering the control management, one has to consider the standardization of policies and regulations of rule with action plan. These are to be considered taken together and passed to the industries. This is the tactic that using only chosen methodology that is designed for this purpose and modified spontaneously. Safety is the defense to the requirement of initiating the company to the large volume of the Web connected anyhow to the industry. This specific methodology of work might not be successful to give confidence and restricting threats due which the businesses and the associated customers indulging with the business may get advantages of threat control methods. Multi agent attack detection system, Database Security, firewall and safety control plan work taking some new specific latest methods
and many more are good for solving the impact of security threats. A more efficient approach with more advanced technologies is taken into consideration. So there is some hope for invitation from industries to feel its need and apply these in business.

**FURTHER STEPS:**

These latest and more specific methods with technologies are great advantageous in different kinds of people using the Web network to offend and taking data causing the sincere effects of safety risks on companies. Finding the attacker’s recognition could support deciding the optimizing method to put these away. Legal authorities and the state agencies indulged in electronic businesses are getting the advantages of the available methods and latest modern techniques with advanced usages in limiting the inverse effects of safety concerns internally as well as externally. This is also a fact on social humanity ground that safety rules and processes joined to a better type of knowledge are always the effective control counter to the society habits and technology. Safety in electronic trades coupled with restrictions should be treated through action. There is one root rule - make security standards. It becomes more specific when we talk about the safety controls associated with electronic business. In other case it could be more serious position of keeping the safety of our trades. Nil harm action to make nil the effects of safety concerns in electronic industry applying controls and above said advanced methods of technology is the important implementation to the development of the business. This will finish errors in the very starting levels to enlarge the procedure. The companies need essentially some controlling and restrictive methods to counter with the safety concerns and attacks on businesses. There is an urgent need of finding and prepare the architecture of protecting and error acceptance system in industries.

**ACKNOWLEDGEMENT**

We are heartily thankful to all who contributed their valuable contribution and help in this paper.
REFERENCES:

National conference Proceedings at BVICAM, Paschim vihar, New Delhi (26-27th Feb 2010)

[17] Search Security.com, Firewall
www.progress.com/webspeed/whitepapers/securing_firewall.htm