International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 06, 2020
ISSN: 1475-7192

"E-BUSINESS SYSTEMS - APPLICATIONS AND SECURITY MEASURES"

B.Karthiga, Dr. Mrs. V.Sujatha,

Research scholar in Department of Commerce,Cauvery College For Women (Autonomous), Affiliated to Bharathidasan University,Tiruchirappalli-18.

Principal& Research Advisor, Cauvery College For Women (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli-18.

Abstract

Electronic Business commonly referred to as "e-Business" or "e-business", or an internet business, may be defined as the application of information and communication technologies (ICT) in support of all the activities of business. Commerce constitutes the exchange of products and services between businesses, groups and individuals and can be seen as one of the essential activities of any business. Electronic commerce focuses on the use of ICT to enable the external activities and relationships of the business with individuals, groups and other businesses. The term "e-business" was coined by IBM's marketing and Internet teams in 1996.

Keywords: e-Business, information and communication technologies (ICT), Internet

I. INTRODUCTION

Electronic business methods enable companies to link their internal and external data processing systems more efficiently and flexibly, to work more closely with suppliers and partners, and to better satisfy the needs and expectations of their customers. In practice, e-business is more than just e-commerce. While e-business refers to more strategic focus with an emphasis on the functions that occurs using electronic capabilities, e-commerce is a subset of an overall e-business strategy. E-commerce seeks to add revenue streams using the World Wide Web or the Internet to build and enhance relationships with clients and partners and to improve efficiency using the Empty Vessel strategy.

E-business involves business processes spanning the entire value chain, electronic purchasing and supply chain management, processing orders electronically, handling customer service, and cooperating with business partners. Special technical standards for e-business facilitate the exchange of data between companies. E-business software solutions allow the integration of intra and inter firm business processes. E-business can be conducted using the Web, the Internet, intranets, extranets, or some combination of these.

Basically, electronic commerce (EC) is the process of buying, transferring, or exchanging products, services, and/or information via computer networks, including the internet. EC can also be beneficial from many perspectives including business process, service, learning, collaborative, community. EC is often confused with e-business.

II. SUBSETS OR APPLICATIONS OF E – BUSINESS:

Applications can be divided into three categories:

1. Internal business systems:
   - customer relationship management
   - enterprise resource planning
   - document management systems
   - human resources management
2. Enterprise communication and collaboration:
   - Voice over Internet Protocol
   - content management system
   - e-mail
   - voice mail
   - Web conferencing
   - Digital work flows or business process management
3. electronic commerce - business-to-business electronic commerce (B2B) or business-to-consumer electronic commerce (B2C):
   - internet shop
   - supply chain management
   - online marketing
   - offline marketing

Received: 10 Apr 2020 | Revised: 20 May 2020 | Accepted: 02 Jun 2020

MODELS

When organizations go online, they have to decide which e-business models best suit their goals. A business model is defined as the organization of product, service and information flows, and the source of revenues and benefits for suppliers and customers. The concept of e-business model is the same but used in the online presence. The following is a list of the currently most adopted e-business models:

- E-shops
- E-commerce
- E-procurement
- E-malls
- E-auctions
- Virtual Communities
- Collaboration Platforms
- Third-party Marketplaces
- Value-chain Integrators
- Value-chain Service Providers
- Information Brokerage
- Telecommunication
- Customer relationship

III. CLASSIFICATION BY PROVIDER AND CONSUMER

Roughly dividing the world into providers/producers and consumers/clients, one can classify e-businesses into the following categories:

- business-to-business (B2B)
- business-to-consumer (B2C)
- business-to-employee (B2E)
- business-to-government (B2G)
- government-to-business (G2B)
- government-to-government (G2G)
- government-to-citizen (G2C)
- consumer-to-consumer (C2C)
- consumer-to-business (C2B)

It is notable that there are comparably less connections pointing "upwards" than "downwards" (few employee/consumer/citizen-to-X models).

ELECTRONIC BUSINESS SECURITY

E-Business systems naturally have greater security risks than traditional business systems, therefore it is important for e-business systems to be fully protected against these risks. A far greater number of people have access to e-businesses through the internet than would have access to a traditional business. Customers, suppliers, employees, and numerous other people use any particular e-business system daily and expect their confidential information to stay secure. Hackers are one of the great threats to the security of e-businesses. Some common security concerns for e-Businesses include keeping business and customer information private and confidential, authenticity of data, and data integrity. Some of the methods of protecting e-business security and keeping information secure include physical security measures as well as data storage, data transmission, anti-virus software, firewalls, and encryption to list a few.

IV. KEY SECURITY CONCERNS WITHIN E-BUSINESS

PRIVACY AND CONFIDENTIALITY

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. However, this becomes even more difficult when dealing with e-businesses specifically. To keep such information secure means protecting any electronic records and files from unauthorized access, as well as ensuring safe transmission and data storage of such information. Tools such as encryption and firewalls manage this specific concern within e-business.

AUTHENTICITY

E-business transactions pose greater challenges for establishing authenticity due to the ease with which electronic information may be altered and copied. Both parties in an e-business transaction want to have the assurance that the other party is who they claim to be, especially when a customer places an order and then submits a payment electronically. One common way to ensure this is to limit access to a network or trusted parties by using a

virtual private network (VPN) technology. The establishment of authenticity is even greater when a combination of techniques are used, and such techniques involve checking "something you know" (i.e. password or PIN), "something you have" (i.e. credit card), or "something you are" (i.e. digital signatures or voice recognition methods). Many times in e-business, however, "something you are" is pretty strongly verified by checking the purchaser's "something you have" (i.e. credit card) and "something you know" (i.e. card number).

DATA INTEGRITY

Data integrity answers the question "Can the information be changed or corrupted in any way?" This leads to the assurance that the message received is identical to the message sent. A business needs to be confident that data is not changed in transit, whether deliberately or by accident. To help with data integrity, firewalls protect stored data against unauthorized access, while simply backing up data allows recovery should the data or equipment be damaged.

NON-REPUDIATION

This concern deals with the existence of proof in a transaction. A business must have assurance that the receiving party or purchaser cannot deny that a transaction has occurred, and this means having sufficient evidence to prove the transaction. One way to address non-repudiation is using digital signatures. A digital signature not only ensures that a message or document has been electronically signed by the person, but since a digital signature can only be created by one person, it also ensures that this person cannot later deny that they provided their signature.

ACCESS CONTROL

When certain electronic resources and information is limited to only a few authorized individuals, a business and its customers must have the assurance that no one else can access the systems or information. Fortunately, there are a variety of techniques to address this concern including firewalls, access privileges, user identification and authentication techniques (such as passwords and digital certificates), Virtual Private Networks (VPN), and much more.

AVAILABILITY

This concern is specifically pertinent to a business' customers as certain information must be available when customers need it. Messages must be delivered in a reliable and timely fashion, and information must be stored and retrieved as required. Because availability of service is important for all e-business websites, steps must be taken to prevent disruption of service by events such as power outages and damage to physical infrastructure. Examples to address this include data backup, fire-suppression systems, Uninterrupted Power Supply (UPS) systems, virus protection, as well as making sure that there is sufficient capacity to handle the demands posed by heavy network traffic.

V. COMMON SECURITY MEASURES FOR E-BUSINESS SYSTEMS

Many different forms of security exist for e-businesses. Some general security guidelines include areas in physical security, data storage, data transmission, application development, and system administration.

PHYSICAL SECURITY

Despite e-business being business done online, there are still physical security measures that can be taken to protect the business as a whole. Even though business is done online, the building that houses the servers and computers must be protected and have limited access to employees and other persons. For example, this room should only allow authorized users to enter, and should ensure that "windows, dropped ceilings, large air ducts, and raised floors" do not allow easy access to unauthorized persons. Preferably these important items would be kept in an air-conditioned room without any windows.

Protecting against the environment is equally important in physical security as protecting against unauthorized users. The room may protect the equipment against flooding by keeping all equipment raised off of the floor. In addition, the room should contain a fire extinguisher in case of fire. The organization should have a fire plan in case this situation arises. In addition to keeping the servers and computers safe, physical security of confidential information is important. This includes client information such as credit card numbers, checks, phone numbers, etc. It also includes any of the organization's private information. Locking physical and electronic copies of this data in a drawer or cabinet is one additional measure of security. Doors and windows leading into this area should also be securely locked. Only employees that need to use this information as part of their job should be given keys.

Received: 10 Apr 2020 | Revised: 20 May 2020 | Accepted: 02 Jun 2020

Important information can also be kept secure by keeping backups of files and updating them on a regular basis. It is best to keep these backups in a separate secure location in case there is a natural disaster or breach of security at the main location. “Failover sites” can be built in case there is a problem with the main location. This site should be just like the main location in terms of hardware, software, and security features. This site can be used in case of fire or natural disaster at the original site. It is also important to test the “failover site” to ensure it will actually work if the need arises.

State of the art security systems, such as the one used at Tide point's headquarters, might include access control, alarm systems, and closed-circuit television. One form of access control is face (or another feature) recognition systems. This allows only authorized personnel to enter, and also serves the purpose of convenience for employees who don't have to carry keys or cards. Cameras can also be placed throughout the building and at all points of entry. Alarm systems also serve as an added measure of protection against theft.

DATA STORAGE

Storing data in a secure manner is very important to all businesses, but especially to e-businesses where most of the data is stored in an electronic manner. Data that is confidential should not be stored on the e-business' server, but instead moved to another physical machine to be stored. If possible this machine should not be directly connected to the internet, and should also be stored in a safe location. The information should be stored in an encrypted format.

Any highly sensitive information should not be stored if it is possible. If it does need to be stored, it should be kept on only a few reliable machines to prevent easy access. Extra security measures should be taken to protect this information (such as private keys) if possible. Additionally, information should only be kept for a short period of time, and once it is no longer necessary it should be deleted to prevent it from falling into the wrong hands. Similarly, backups and copies of information should be kept secure with the same security measures as the original information. Once a backup is no longer needed, it should be carefully but thoroughly destroyed.

DATA TRANSMISSION AND APPLICATION DEVELOPMENT

All sensitive information being transmitted should be encrypted. Businesses can opt to refuse clients who can't accept this level of encryption. Confidential and sensitive information should also never be sent through e-mail. If it must be, then it should also be encrypted.

Transferring and displaying secure information should be kept to a minimum. This can be done by never displaying a full credit card number for example. Only a few of the numbers may be shown, and changes to this information can be done without displaying the full number. It should also be impossible to retrieve this information online. Source code should also be kept in a secure location. It should not be visible to the public. Applications and changes should be tested before they are placed online for reliability and compatibility.

SYSTEM ADMINISTRATION

Security on default operating systems should be increased immediately. Patches and software updates should be applied in a timely manner. All system configuration changes should be kept in a log and promptly updated. System administrators should keep watch for suspicious activity within the business by inspecting log files and researching repeated logon failures. They can also audit their e-business system and look for any holes in the security measures. It is important to make sure plans for security are in place but also to test the security measures to make sure they actually work. With the use of social engineering, the wrong people can get a hold of confidential information. To protect against this, staff can be made aware of social engineering and trained to properly deal with sensitive information.

E-businesses may use passwords for employee logons, accessing secure information, or by customers. Passwords should be made impossible to guess. They should consist of both letters and numbers, and be at least seven to eight digits long. They should not contain any names, birth dates, etc. Passwords should be changed frequently and should be unique each time. Only the password's user should know the password and it should never be written down or stored anywhere. Users should also be locked out of the system after a certain number of failed logon attempts to prevent guessing of passwords.

VI. SECURITY SOLUTIONS

When it comes to security solutions, there are some main goals that are to be met. These goals are data integrity, strong authentication, and privacy.

Received: 10 Apr 2020 | Revised: 20 May 2020 | Accepted: 02 Jun 2020

ACCESS AND DATA INTEGRITY

There are several different ways to prevent access to the data that is kept online. One way is to use anti-virus software. This is something that most people use to protect their networks regardless of the data they have. E-businesses should use this because they can then be sure that the information sent and received to their system is clean. A second way to protect the data is to use firewalls and network protection. A firewall is used to restrict access to private networks, as well as public networks that a company may use. The firewall also has the ability to log attempts into the network and provide warnings as it is happening. They are very beneficial to keep third-parties out of the network. Businesses that use Wi-Fi need to consider different forms of protection because these networks are easier for someone to access. They should look into protected access, virtual private networks, or internet protocol security. Another option they have is an intrusion detection system. This system alerts when there are possible intrusions. Some companies set up traps or "hot spots" to attract people and are then able to know when someone is trying to hack into that area.

ENCRYPTION

Encryption, which is actually a part of cryptography, involves transforming texts or messages into a code which is unreadable. These messages have to be decrypted in order to be understandable or usable for someone. There is a key that identifies the data to a certain person or company. With public key encryption, there are actually two keys used. One is public and one is private. The public one is used for encryption, and the private for decryption. The level of the actual encryption can be adjusted and should be based on the information. The key can be just a simple slide of letters or a completely random mix-up of letters. This is relatively easy to implement because there is software that a company can purchase. A company needs to be sure that their keys are registered with a certificate authority.

DIGITAL CERTIFICATES

The point of a digital certificate is to identify the owner of a document. This way the receiver knows that it is an authentic document. Companies can use these certificates in several different ways. They can be used as a replacement for user names and passwords. Each employee can be given these to access the documents that they need from wherever they are. These certificates also use encryption. They are a little more complicated than normal encryption however. They actually used important information within the code. They do this in order to assure authenticity of the documents as well as confidentiality and data integrity which always accompany encryption. Digital certificates are not commonly used because they are confusing for people to implement. There can be complications when using different browsers, which mean they need to use multiple certificates. The process is being adjusted so that it is easier to use.

DIGITAL SIGNATURES

A final way to secure information online would be to use a digital signature. If a document has a digital signature on it, no one else is able to edit the information without being detected. That way if it is edited, it may be adjusted for reliability after the fact. In order to use a digital signature, one must use a combination of cryptography and a message digest. A message digest is used to give the document a unique value. That value is then encrypted with the sender's private key.

KEYS TO E-BUSINESS SUCCESS

1. Think big, start small
2. Be end-user centric
3. Content is king
4. Channels must be integrated
5. Develop applications iteratively
6. Communicate with stakeholders before, during and after
7. It's not a one-shot project, it's an ongoing process

VII. CONCLUSION

E-Business trends are very interesting and useful in ones career because of the importance it embraces in today's business world. The aspect of e-commerce has changed a lot lately to in the beginning of the 1990s be about being present on the Internet with a web site, to being about transactions, meaning to buy or sell through digital media at the end of the 1990s, to today be about being used to make profitability – an era that can be called e-business, because it is now that e-business finally gets its big breakthrough an starts to be recognized as a necessity for companies to survive. As long as e-business has existed so have trends in the same matter. What will be the

trends of e-business in the future? Impossible to say of course, but by taking today's major trends into consideration, and to look at what drives these trends might have, will make it possible to get a glimpse of the future of this relatively new business phenomenon called e-business. Two major trends namely, customer orientation and service digitization have been focused on. Customer oriented trends are trends which have their focus towards customers such as customer service, offering more product choices and to have integrated solutions. Service digitization is the transformation of paper-based transactions into the new integrated multi-channel processes. Customers are important as drivers since they have adopted a new role in the business process. With the help of blogs, social networks and wikis over the Internet they can express their feelings and suggestions about products as well as companies and have so to say gained a more active role as customers to also taking part of the development. This voice of the customers is highly essential to listen to if a company wants to survive in a business world where customers get more and more power. The importance of service and especially customer service as well of personalization and customization (to personalize the shopping experience for the customer) is to be concentrated. Another important conclusion is the importance of customers, both as trends to focus on, as well as drivers behind these trends.

REFERENCES

[1] www.wisegeek.com/what-is-ebusiness.htm
[2] www.ecommercetimes.com/
[3] en.wikipedia.org/wiki/Electronic business
[4] www.apdip.net/publications/iespprimers/eprimer-ecom
[5] searchcio.techtarget.com/definition/e-business

Received: 10 Apr 2020 | Revised: 20 May 2020 | Accepted: 02 Jun 2020