THE IMPORTANCE OF E-EDUCATION IN TODAY'S BUSINESS WORLD AND SOME RECENT EXPERIENCE

Lakavath Deshya
Master of Education
Kakatiya University
Warangal
Telangana- 506009
dsnaik1477@gmail.com

Abstract

It is possible to describe electronic business, also known as e-business, as the application of information and communication technologies (ICT) in support of all of the activities that are associated with running a business. One of the most important things that any company does is engage in commerce, which is the buying and selling of goods and services between other companies, organisations, and private individuals. The use of information and communication technologies (ICT) to facilitate a company's external activities and interactions with individuals, groups, and other enterprises is the primary focus of electronic commerce. To engage in industry, trade, or commerce through the use of computer networks is an example of what is referred to as "e-business." In 1996, IBM's marketing and Internet teams came up with the concept that would later be known as "e-business." Electronic business processes allow businesses to link their internal and external data processing systems in a way that is more efficient and flexible, to collaborate more closely with their partners and suppliers, and to better meet the requirements and expectations of their consumers. A public thoroughfare is represented by the internet. The management of an organization's internal operations can be made more effective and efficient by the use of more private networks, which are also more secure.

Introduction

In its most basic form, e-business encompasses more than just online shopping. E-commerce is a part of an entire e-business plan, whereas the term "e-business" refers to a more strategic approach with an emphasis on the functions that occur as a result of the use of electronic capabilities. The goal of e-commerce is to increase productivity by using the Empty Vessel strategy in order to generate additional revenue streams through the use of the World Wide Web (WWW) or the Internet (Internet), as well as to establish and strengthen relationships with customers and business partners. Knowledge management systems are frequently utilised in the course of conducting business online. E-business entails conducting business operations that span the entirety of the value chain. These operations include electronic purchasing and administration of the supply chain, electronic order processing, the provision of customer support, and collaboration with business partners. The sharing of data between businesses is made easier by the application of specialised technical standards for e-business. The use of e-business software solutions enables the integration of business activities both within and across companies. The World Wide Web, the Internet, private intranets and extranets, or any combination of these can all be used to do business online. In its most fundamental form, electronic commerce (EC) refers to the act of acquiring, transferring, or exchanging goods, services, and/or information through the use of computer networks such as the internet. EC may also be useful from a variety of viewpoints, including

those of corporate processes, customer service, learning, collaborative efforts, and communities. The term "e-business" is frequently confused with "e-commerce."

Classification according to the provider and the customer

One can classify e-businesses into the following categories by roughly dividing the world into providers/producers and consumers/clients. These categories include

- 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 (C2B).

Potential concerns

While much has been written about the economic benefits of internet-enabled commerce, there is also evidence that certain aspects of the internet, such as maps and location-aware services, may serve to reinforce economic inequality and the digital divide. This is despite the fact that much has been written about the economic benefits of internet-enabled commerce.

It is possible that the rise of electronic commerce is to blame for the consolidation of firms and the collapse of mom-and-pop, brick-and-mortar shops, which has led to an increase in income disparity.

Security

It should come as no surprise that the potential dangers to data security posed by e-business systems are higher than those posed by traditional business systems. For this reason, it is critical that e-business systems be adequately safeguarded against all potential dangers. E-businesses, which are conducted online and are accessible to customers via the internet, are accessible to a significantly larger number of individuals than conventional businesses are. Any given e-business system is used on a regular basis by customers, suppliers, employees, and a wide variety of other people, all of whom anticipate that the confidentiality of their information will be maintained. Hackers represent one of the most significant challenges to the safety of online enterprises. Keeping business and consumer information private and discreet, verifying the authenticity of data, and maintaining the integrity of data are some of the most typical security challenges for online businesses. Physical security measures, data storage, data transmission, anti-virus software, firewalls, and encryption are just a few of the many approaches that can be utilised to ensure the security of an online business and maintain the confidentiality of its customers' information.

Protection of one's privacy and secrecy

A company's level of confidentiality can be measured by the amount to which it shares personally identifiable information with other companies and individuals. In any company, it is imperative that sensitive information be kept confidential and only available to

those who are authorised to receive it. Having said that, this challenge multiplies when it comes to dealing specifically with e-commerce companies. To ensure the safety of the transmission and data storage of such information, as well as the protection of any electronic records and files against unauthorised access, maintaining the security of such information is necessary to keep it private. Tools within the realm of e-business, such as encryption and firewalls, are used to manage this particular risk.

Authenticity

Due to the simplicity with which electronic information can be manipulated and copied, authenticating e-business transactions presents a larger problem than traditional commercial transactions. When conducting an online business transaction, both parties involved want to have the assurance that the other party is who they claim to be. This is especially important when a client puts an order and then sends an electronic payment for the product. Utilizing a technology known as a virtual private network (VPN) is one typical method that may be used to achieve this, as it restricts access to a network or trusted people. When multiple ways are employed, it is even easier to verify authenticity. These approaches include checking "something you know" (such as a password or PIN), "something you need" (such as a credit card), or "something you are," respectively (i.e. digital signatures or voice recognition methods). When conducting business online, however, it is common practise to check the purchaser's "something you have" (i.e. credit card) as well as their "something you know" in order to establish that they are who they say they are (i.e. card number).

Data integrity

The answer to the question "Can the information be modified or corrupted in any way?" is determined by the data's integrity. The confidence that the message received is the same as the one sent can be gained as a result of this. A company must have complete faith that the data they send over the internet will not be altered in any way, whether on purpose or by mistake. Firewalls prevent unwanted access to data that has been saved, which helps maintain data integrity. Merely backing up data enables for its retrieval in the event that either the data or the equipment suffers harm.

Non-repudiation

This issue is concerned with the availability of proof in a transaction. A company is required to have the assurance that the receiving party or purchaser cannot deny that a transaction has taken place, and this requires the company to have sufficient proof to verify that a transaction took place. Utilizing digital signatures is one approach that can be taken to address the issue of non-repudiation. A digital signature not only verifies that a message or document has been digitally signed by the person, but also, given that only one person can create a digital signature, it ensures that the person cannot later deny that they provided their signature by preventing them from denying that they created the digital signature in the first place.

Access control

When access to specific electronic resources and information is restricted to only a small number of authorised individuals, a company and its customers need to have the peace of mind that no one else can use the systems or view the information. Firewalls, access

privileges, user identification and authentication techniques (such as passwords and digital certificates), Virtual Private Networks (VPN), and a great deal more are just some of the methods that can be used to address this concern. Fortunately, there are many other methods as well.

Availability

This topic is especially relevant to a company's consumers since specialised information must be made available to customers at the precise moment they require it. It is necessary that messages be delivered in a dependable and timely manner, and that information be saved and retrieved according to the requirements. Because the availability of service is critical to the success of online businesses, it is imperative that measures be made to mitigate the risk of service interruptions caused by problems such as loss of power and damage to physical infrastructure. Data backup, fire-suppression systems, Uninterrupted Power Supply (UPS) systems, virus protection, and ensuring that there is sufficient capacity to handle the demands posed by heavy network traffic are a few examples of ways to deal with this issue. Another option is to ensure that there is sufficient capacity.

Standard precautions taken for safety

E-commerce sites can take advantage of a wide variety of different security measures. Physical security, data storage, data transfer, application development, and system management are just few of the fundamental domains covered by these generic security rules. Physical security Despite e-business being business done online, there are still physical security measures that may be taken to secure the business as a whole. Even though commerce 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 space should only enable authorised individuals to enter, and should guarantee that "windows, dropped ceilings, huge air ducts, and high floors" do not allow simple access to unauthorised personnel. Preferably these precious artefacts would be housed in an air-conditioned chamber without any windows. Defending against the environment is equally vital in physical security as protecting against unwanted people. The chamber may safeguard the equipment against floods by keeping all equipment raised off of the floor. In addition, the room should contain a fire extinguisher in case of fire. **The organisation should have a fire plan in case this event develops**

In addition to keeping the servers and computers safe, physical security of critical information is crucial. 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 material in a drawer or cabinet is one further measure of protection. It is also important to ensure that any doors or windows that lead into this space are properly locked. The keys should be restricted to only those workers who, as part of their duties, are required to make use of this information. Keeping regular backups of files and making sure they are always up to date are both great ways to ensure the safety of important information. It is in everyone's best interest to store these backups in a different secure place in the event that the primary location suffers from a natural disaster or a security breach of some kind.

It is possible to construct "failover sites" in the event that there is an issue at the primary location. In terms of the hardware, software, and safety measures, this location should be identical to the primary one. This location serves as a backup in the event that the primary location is destroyed by a fire or another natural disaster. In order to verify that the "failover site" will function properly in the event that it is required, it is essential to test it. Access control, alarm systems, and closed-circuit television are all examples of components that might be found in cutting-edge security systems like the one installed at the headquarters of Tidepoint. Face recognition systems, along with other types of biometric authentication, are one method for controlling access. This not only ensures that only authorised workers are able to enter, but it also makes it more convenient for staff, who no longer need to carry about keys or access cards. Additionally, cameras may be installed at any and all points of entry as well as everywhere in the structure. Alarm systems offer an additional layer of security against theft in addition to their primary function.

Data storage

It is vitally important for businesses of any kind to store data in a secure manner, but this is of utmost significance for online firms, since the vast majority of data is kept in an electronic format. The server of the online business should not be used to keep data that is considered sensitive; instead, the data should be relocated to another physical machine and stored there. This computer should, if at all possible, not be directly linked to the internet, and it should also be kept in a secure location. It is recommended that the information be saved in an encrypted format. If it is at all possible to avoid doing so, extremely sensitive information should never be saved. In the event that it is necessary to keep data, however, it need to be done so on no more than a handful of dependable computers in order to avoid unauthorised access. If at all practicable, further security precautions, such as the use of private keys, should be implemented to protect sensitive information. In addition, information should only be stored for a short amount of time, and once it is no longer required, it should be removed so that it does not get up in the wrong hands. This is done to avoid it from being misused. In a similar vein, information backups and copies should be protected using the same security methods as the original information. When a backup is no longer required, it should be disposed of in a manner that is both meticulous and comprehensive.

Data transmission and application development

Encryption should be used for any sensitive information that is being transferred. Clients who are unable to comply with this level of encryption can be turned away from companies if they so want. It is imperative that private and sensitive information never be transmitted over email under any circumstances. If it really must be, then it need to be encrypted as well. The amount of protected information that is both transferred and shown should be limited to a minimum. This can be accomplished by, for instance, never revealing the complete number of a credit card. It is possible that only some of the numbers will be displayed, and modifications to this information can be made without the whole number being presented. Additionally, it should not be feasible to get this information via the internet. Additionally, the source code ought to be stored in a safe area. It should not be out in the

open for anyone to see. Applications and updates ought to be put through their paces in terms of dependability and compatibility before being published online.

System administration

Immediate action is required to strengthen the security of operating systems by default. It is important to install software patches and updates as soon as they become available. Every alteration made to the configuration of the system ought to be recorded in a log and promptly brought up to date. System administrators should be on the lookout for suspicious activity within the company by reviewing log files and investigating instances of failed logon attempts that occur frequently. They can also conduct an audit of their e-business system to search for vulnerabilities in the protection protocols. It is essential to not only ensure that plans for security are in place, but also to conduct tests on the security measures to determine whether or not they are effective. It is possible for the wrong people to obtain confidential information through the use of a technique called social engineering. Staff members can be educated about social engineering and taught the appropriate way to handle sensitive information so that they are better protected against this threat. Passwords may be required for logging in as a customer or employee at an online business, as well as for accessing confidential information. It is important to ensure that passwords cannot be guessed. They should be at least seven to eight digits long, include both letters and numbers, and include both uppercase and lowercase characters. They must not include any identifying information, such as names, birth dates, etc. It is important to regularly change your password and make sure it is different each time. The user of the password should be the only person who is aware of the password, and it should never be written down or saved in any way. In order to prevent a user's password from being guessed, the system ought to lock the user out after a predetermined number of unsuccessful attempts to log in.

Options for ensuring safety

When it comes to implementing security measures, there are a few primary objectives that need to be accomplished. The integrity of the data, a robust authentication system, and complete confidentiality are these goals.

Access and the reliability of data

There are a variety of different approaches that can be taken to restrict access to the data that is stored online. Utilizing anti-virus software is one approach that can be taken. Regardless of the types of data that are stored on their networks, the vast majority of users safeguard them using this method. E-commerce companies should make use of this since it will allow them to verify the validity of the data that is transmitted to and received by their system. Utilizing firewalls and other forms of network protection is an additional method for data security. Access to private networks as well as any public networks that may be used by an organisation can be restricted with the help of a firewall. Additionally, the firewall is able to log any efforts made to enter the network and issue alerts as these attempts are made. They are highly helpful in preventing unauthorised third parties from accessing the network. Because it is simpler for unauthorised users to connect to wireless networks, businesses that rely on Wi-Fi should give careful consideration to the usage of additional layers of security. Protected access, virtual private networks, and internet protocol security are all options they

need to investigate. An intrusion detection system is yet another alternative that is available to them. When there is a possibility of an incursion, this system will sound an alarm. Some businesses lure potential hackers in by setting up "hot spots" or other lures, and they are then in a position to detect whenever someone attempts to breach security in that region.

Encryption

Encryption, which is a subset of cryptography, is the process of converting plaintext documents, such as communications or text messages, into an unintelligible code. Deciphering these communications is necessary for anyone to be able to read them or make use of the information they contain. There is a key that can identify the data as belonging to a specific individual or business. In the case of encryption using public keys, there are in fact two keys in use. One of them is open to the public while the other is not. The public key is the one that is used for encryption, while the private key is the one that is used for decryption. The actual encryption can have its degree changed, and this change should be made dependent on the information being protected. It's possible that the key is nothing more than a straightforward slide of letters, or it may be an entirely random combination of letters. Because it is possible for a corporation to acquire the necessary software, this can be put into action with only a moderate amount of difficulty. A corporation must make certain that their keys are registered with a certificate authority before they may use them.

Conclusion

The purpose of a digital certificate is to verify the identity of the person who is in possession of a particular document. This ensures that the recipient is aware that they are in possession of a genuine document. These certificates have a wide variety of applications for businesses and can be used in a variety of ways. They are an alternative to user names and passwords and can be used in their place. These can be provided to every employee so that they can access the documents they require whenever and wherever they are. In addition, encryption is used by these certificates. On the other hand, they are somewhat more difficult to decipher than standard encryption. They did make advantage of vital information that was contained within the code. They do this in order to ensure that the papers are authentic in addition to maintaining the security and integrity of the data, which are always maintained when encryption is used. Digital certificates are not widely used because the process of implementing them can be difficult for people to understand. There is the potential for complications when utilising different browsers, which results in the requirement that they use multiple certificates.

Using a digital signature is the third and final method for protecting information that is stored online. If a document contains a digital signature, it is impossible for anyone else to make changes to the information contained within it without being discovered. In this manner, if it is edited, the accuracy of it can be adjusted after the fact if necessary. Combining cryptography with a message digest is required in order to use a digital signature. Otherwise, the signature will not be valid. A message digest is used to give the document a unique value. Following that step, the value is encrypted using the sender's private key. The type of web browser that a customer uses can be ascertained by online retailers thanks to the

rise of e-commerce. Some retailers provide varying prices for their products, which they decide based on the type of web browser that the buyer is employing.

References

1. *Beynon-Davies P. (2004). E-Business. Palgrave, Basingstoke. ISBN 1-4039-1348-X*
2. *Gerstner, L. (2002). Who says Elephants Can't Dance? Inside IBM's Historic Turnaround. pg 172. ISBN 0-06-052379-4.*
3. *Paul Timmers, (2000), Electronic Commerce - strategies & models for business-to-business trading, pp.31, John Wiley & Sons, Ltd, ISBN 0-471-72029-1*
4. *Badger, Emily (6 February 2013). "How the Internet Reinforces Inequality in the Real World". The Atlantic. Retrieved 2013-02-13.*
5. *"E-commerce will make the shopping mall a retail wasteland" ZDNet, January 17, 2013*
6. *"'Free Shipping Day' Promotion Spurs Late-Season Online Spending Surge, Improving Season-to-Date Growth Rate to 16 Percent vs. Year Ago" Comscore, December 23, 2012*
7. *"The Death of the American Shopping Mall" The Atlantic — Cities, December 26, 2012*
8. *Westfall, Joseph. "Privacy: Electronic Information and the Individual." Santa Clara University. Markkula Center for Applied Ethics, 2010. Web. 30 Nov. 2010. http://www.scu.edu/ethics/publications/submitted/westfall/privacy.html>.*
9. *"What Is Nonrepudiation? - Definition." Information Security: Covering Today's Security Topics. TechTarget, 4 Sept. 2008. Web. 30 Nov. 2010.*