Volume 2, Issue 7, July 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Study of Ethical and Social Issues in E-Commerce

Himani Grewal
Management Dept, SSIM, Moradabad
SSIM, Moradabad, India

Shivani
Dept. of CSE
SNGI, Meerut, India

Abstract- ***The web environment is quite different from that of the traditional brick and mortar businesses. The very nature of e-business necessitates the need for things to be viewed from a different perspective. An important contemplation is whether ethics needs to be considered, and if so, the development and implementation of policies that would support that need should be explored. The rapid spread of e-commerce has created tremendous opportunities for economic efficiency and customer choice. Use of the global Internet computer network for ecommerce activities provides some advantages to the consumers on their daily life. On the other hand Internet represents a new environment for unethical behaviour. While e-commerce has witnessed extensive growth in last decade, consumers concerns regarding ethical issues also continue to increase. Even many consumers and businesses are revelling in e-commerce; consumer problems related to online selling and purchasing become the dark side of the issue.***

Keywords- ***e-commerce, business ethics, security, threats.***

I. INTRODUCTION

A) What Is E-Commerce?

E-Commerce is the ability of a company to have a dynamic presence on the Internet which allowed the company to conduct its business electronically, in essence having an electronic shop. Products can be advertised, sold and paid for all electronically without the need for it to be processed by a human being. Due to the vastness of the internet advertising and the website can be exposed to hundreds of people around the world for almost nil cost and with information being able to be changed almost instantly the site can always be kept up to date with all the latest products to match with consumers demands. The biggest advantage of E-Commerce is the ability to provide secure shopping transactions via the internet and coupled with almost instant verification and validation of credit card transactions. This has caused E-Commerce sites to explode as they cost much less than a store front in a town and has the ability to serve many more customers. In the broad meaning electronic commerce (E-Commerce) is a means of conducting business using one of many electronic methods, usually involving telephones, computers (or both). E-Commerce is not about the technology itself, it is about doing business using the technology.

B) What is Business Ethics?

Ethics is the branch of philosophy that studies what's right and wrong. Ethical rules are rules to follow in our interactions with other people and in our actions that affect other people. They apply to all of us and are intended to achieve good results for people in general, and for situations in general; not just for ourselves, and not just for one situation. Business ethics is concerned with the numerous ethical questions that managers must confront as part of their daily business decision-making. Managers use several important alternatives when confronted with making ethical decisions on business issues. These include:

1) *Stockholder Theory* – Holds that managers are agents of the stockholders, and their only ethical responsibility is to increase the profits of the business, without violating the law or engaging in fraudulent practices.

2) Social Contract Theory - States that companies have ethical responsibility to all members of society, which allow corporations to exist based on a social contract.

3) Stakeholder Theory - Maintains that managers have an ethical responsibility to manage a firm for the benefit of all of its stakeholders, which are all individuals and groups that have a stake in or claim on a company.

II. OBJECTIVE OF STUDY

The main objective of the study is to identify the ethical problems and issues related to e-commerce.

- To discover the major ethical and social issues in E-Commerce.
- To find out the major threats in E-Commerce.
- To give a better understanding on how businesses and consumers can be safe from online threats.

III. ETHICS IN E-COMMERCE

Behaving ethically is often practical because most of the time we are honest, we keep our promises, we do not steal, and we do our jobs. Therefore, behaving ethically, in personal or professional sphere, is usually not a burden. In business context, doing well ethically corresponds closely with good business in the sense that ethically developed products are more likely to please consumers. A professional can cause great harm through dishonesty, carelessness, or incompetence. Sometimes, it is difficult to do the right thing. It takes courage in situations where we could suffer negative consequences. Courage in professional setting could mean admitting to a customer that your program is faulty, declining a job for which you are not qualified,

or speaking out when you see someone else is doing something wrong. It is hard to gain trust on the web because customers do not know you. Thus, ethics is important in e-Business if an organization wants the people to trust it and do business with it. E-Businesses must honour their Business Policies and their customer's privacy and security.

E-Commerce security is plagued with ethical issues on responsibility. If fraud occurs, whose fault is it? Is it the business's fault for not securing their information correctly? Is it the consumer's fault for assuming that the technology used is secure? Is it the criminal's fault for stealing information, even if the information was being sent in the clear? Or is it a combination of the three?

It is critical that the system administrator of an e-commerce system be aware of the security of the system and the consumer's information. Is it ethical if an administrator could have prevented information but chose not to for particular reasons? Would it also be ethical for businesses to publicize only the criminal and not the security holes that allowed the hacker to get through? Would the opinion change if the business knew about the security hole but deemed it to expensive to fix and the probability of a break-in low? Ethics is a concern of humans who have freedom of choice. Ethics is about individual choice: When faced with alternative courses of action, what is the correct moral choice? What are the main features of ethical choice?

A) Basic Concepts: Responsibility, Accountability, And Liability

Ethical choices are decisions made by individuals who are responsible for the consequences of their actions. Responsibility is a key element of ethical action. *Responsibility* means that you accept the potential costs, duties, and obligations for the decisions you make.

Accountability is a feature of systems and social institutions: It means that mechanisms are in place to determine who took responsible action, who is responsible. Systems and institutions in which it is impossible to find out who took what action are inherently incapable of ethical analysis or ethical action.

Liability extends the concept of responsibility further to the area of laws. Liability is a feature of political systems in which a body of laws is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations. Due process is a related feature of law-governed societies and is a process in which laws are known and understood and there is an ability to appeal to higher authorities to ensure that the laws are applied correctly.

These basic concepts form the underpinning of an ethical analysis of information systems and those who manage them. First, information technologies are filtered through social institutions, organizations, and individuals. Systems do not have impacts by themselves. Whatever information system impacts exist are products of institutional, organizational, and individual actions and behaviours. Second, responsibility for the consequences of technology falls clearly on the institutions, organizations, and individual managers who choose to use the technology. Using information technology in a socially responsible manner means that you can and will be held accountable for the consequences of your actions. Third, in an ethical, political society, individuals and others can recover damages done to them through a set of laws characterized by due process.

IV. THE ETHICAL ISSUES IN E-COMMERCE

At the early ages of its emergence, the Internet only became the platform to search information and to communicate by each others. But now, we can say that Internet has been commercialized (thus the term e-commerce emerge). Nowadays, we can see almost all trading and business activities including banking can be done online. This trend gives a lot of advantages both to consumers and business organizations. However, the bad side about e-commerce also cannot be ignored. What we mean the bad side is about the ethical issue in e-commerce. These issues involve the irresponsible parties who always give threats both to consumers and business organization.

A) Web Spoofing

Web spoofing is an electronic deception relates to the Internet. It occurs when the attacker sets up a fake website which almost totally same with the original website in order to lure consumers to give their credit card number or other personal information. For example is the attacker setup a site called *www.micros0ft.com* using the number zero in place of the letter O, which many users sometimes type by mistake? Users might find themselves in a situation that they do not notice they are using a bogus web-site and give their credit card details or other information.

B) *Cyber-Squatting*

Cyber-squatting is an activity which a person or firm register, purchase and uses the existing domain name belong to the well-known organization for the purpose of infringing its trademarks. This type of person or firm, called cyber-squatters usually infringed the trademarks to extort the payment from original trademark's owner. The extortion of payment occur when they offers the prices far greater than they had purchased the organization's domain name upon. Some cyber-squatters put up derogatory remarks about the person or company which the domain is meant to represent (*eg: www.walmartsucks.com*), in an effort to encourage the subject to re-buy their domain from them. The following picture will worth explain the example of cyber-squatting.

C) Privacy Invasion

This issue is related to consumer. The privacy invasion occur when the personal details belong to consumers are exposed to the unauthorized party. It may occur in THREE ways.

1) Electronic commerce businesses buy information about individuals such as their personal details, shopping habits and web page visitation listings. This can be done with or without the individual's knowledge by using different computing technologies. A large number of web sites, which require users to create a

member name, also ask for personal details. These details are then often sold on to companies to aid in the marketing and selling of their products.

2) The personal information of consumers being transmit may be intercepted by anyone other than the person whom it is intended. Protecting the privacy of communication is a great challenge, due to the very nature of the online medium, an open network of digital telecommunications. It is technically and economically impossible to patch all the holes through which unauthorized intruders may gain access.

3) Malicious programs delivered quietly via web pages could reveal credit card numbers, usernames, and passwords that are frequently stored in special files called cookies. Because the internet is stateless and cannot remember a response from one web page view to another, cookies help solve the problem of remembering customer order information or usernames or passwords.

D) Online Piracy

The online piracy can be defined as unauthorized copyright of electronic intellectual property such as e-books, music or videos. This unethical activity occurs when the Internet users use the software and hardware technology in an illicit manner to transfer the electronic intellectual property over the Internet. For example, some web-based applications such as *www.napster.com* have enabled large scale exploitation of music samples and audio formats. Software that is available for free of cost on the Internet allows the transfer of music and videos without the authorization of rights holders. Moreover, CD burners and portable MP3 players allow copyright violations to occur rather easily.

E) Email Spamming

E-mail spamming, also known as unsolicited commercial e-mail (UCE) involves using e-mail to send or broadcast unwanted advertisement or correspondence over the Internet. The individual who spam their e-mail usually called spammer. Many spammers broadcast their e-mail for the purpose of trying to get people's financial information such as credit card or account bank numbers in order to defraud them. The example of fraud using e-mail is spammers will lure consumers to enter their personal information on fake website using e-mail, forged to look like it is from authorized organization such as bank. The content of e-mail often directs the consumers to the fake website in order to lure them to fill their personal information such as credit card or bank account's details. This technique is called phishing. The following picture is an example of phishing e-mail.

V. MAJOR THREATS IN E-COMMERCE

E-Commerce Security also has some main issues. They are interception of data, redirection of data, identification of parties, exploitable program errors, and being the weakest point in security. When administrating a secure e-commerce site, it is important to remember that you are part of a link of systems. If you're security is weak, it may be possible that you are allowing criminals access to information they may not have had access to. This leads to ethical issues where weak security on your system led to dire consequences for other people or companies.

Compare security issues over the Internet compared to real-life. Is it right to be protective of information over the Internet when people are not protecting that same information normally? Is it ethical to deliver different punishments to criminals who steal information over the Internet compared to those who steal information personally?

A) The Threats Posed to E-Commerce Servers

E-commerce tends to be at a higher echelon for risk and attacks. This is so because according to our definition, E-Commerce is the transaction of goods and services; and the payment for those goods and services over the Internet. Therefore, the physical place where all of these transactions occur is at the Server level. The server can be viewed as the central repository for your "E-Commerce Place of Business"[which consists of the actual website which displays your products and services, the customer database, and the payment mechanism]. If there are any attacks to this server, in one blow, there is the potential you could lose everything. Threats to E-Commerce servers fall into two general categories:

(1) Threats from an actual attacker(s); and
(2) Technological failure.

In terms of the former, the motivation is primarily psychological. The intent is to garner personal information from people for the sheer purposes of exploitation (such obtaining Credit Card and Bank Account information; Phishing schemes, obtaining usernames and passwords, etc.). With the latter, anything related to the Internet can cause problems. This can be anything from a network not configured properly to data packets being lost, especially in a wireless access environment. Even poorly written programming code upon which your E-Commerce site was developed can be very susceptible to threats. Most E-Commerce Servers utilize a Windows Operating System (such as Windows 2000 and 2003 Server), a Web Server Software to host the E-Commerce Site (such as Internet Information Services, or IIS), and a database (such as Access 2000 or SQL Server 2000) which contains your customer information and transaction history. These platforms have had various security flaws associated with them, which has made them wide open to threats and attacks. As a result, there has been a move in the business community to adopt more robust and secure platforms. A prime example of this is the use of Linux as the operating system, Apache as the Web Server Software, and either PostGRESql or My SQL as the database (these are database languages created from the Structured Query Language, or SQL). These latter platforms will be explored in much more detail in subsequent articles. We will now examine the various threats and risks that are posed to E-Commerce servers.

The direct threats to E-Commerce servers can be classified as either
(1) Malicious Code Threats; and
(2) Transmission Threats.

With the former, malicious, or rogue programming code is introduced into the server in order to gain access to the system resources. Very often, the intent of Malicious Code Attacks is to cause large scale damage to the E-Commerce server. With the latter, the threats and risks can be classified as either as active or passive. With passive threats, the main goal is to listen (or eavesdrop) to transmissions to the server. With active threats, the intent is to alter the flow of data transmission or to create a rogue transmission aimed directly at the E-Commerce server.

1. *Malicious Code Attacks*

a) Viruses and Worms

The most common threat under this category are the worms and viruses. In the media today, we keep hearing about these words on almost a daily basis, and there is confusion that the two are related, and synonymous. However, the two are very different. A virus needs a host of some sort in order to cause damage to the system. The exact definition is "a virus attaches itself to executable code and is executed when the software program begins to run or an infected file is opened." So for example, a virus needs a file in which to attach itself to. Once that file is opened, the virus can then cause the damage. This damage can range from the deletion of some files to the total reformatting of the hard drive. The key to thing to remember about viruses is that they cannot by themselves spread-they require a host file.

However, worms are very much different. A worm does not need a host to replicate. Rather, the worm replicates itself through the Internet, and can literally infect millions of computers on a global basis in just a matter of hours. A perfect example of this is once again the MS Blaster worm. Worms by themselves do not cause damage to a system like a virus does. However, worms can shut down parts of the Internet or E-Commerce servers, because they can use up valuable resources of the Internet, as well as the memory and processing power of servers and other computers.

b) Trojan Horses

A Trojan horse is a piece of programming code that is layered behind another program, and can perform covert, malicious functions. For example, your E-Commerce server can display a "cool-looking" screen saver, but behind that could be a piece of hidden code, causing damage to your system. One way to get a Trojan Horse attack is by downloading software from the Internet. This is where you need to be very careful. There will be times (and it could be often) that patches and other software code fixes (such as Service packs) will need to be downloaded and applied onto your E-Commerce server. Make sure that whatever software is downloaded comes from an authentic and verified source, and that all defence mechanisms are activated on your server.

c) Logic Bombs

A Logic Bomb is a version of a Trojan Horse, however, it is event or time specific. For example, a logic bomb will release malicious or rogue code in an E-Commerce server after some specific time has elapsed or a particular event in application or processing has occurred.

2. *Transmission Threats*

a) Denial of Service Attacks

With a Denial of Service Attack, the main intention is to deny your customers the services provided on your E-Commerce server. There is no actual intent to cause damage to files or to the system, but the goal is to literally shut the server down. This happens when a massive amount of invalid data is sent to the server. Because the server can handle and process so much information at any given time, it is unable to keep with the information and data overflow. As a result, the server becomes "confused", and subsequently shuts down.

b) Ping of Death

When we surf the Web, or send E-Mail, the communications between our computer and the server takes place via the data packet. It is the data packet that contains the information and the request for information that is sent from our computer to other computers over the Internet. The communication protocol which is used to govern the flow of data packets is called Transmission Control Protocol/Internet Protocol, or TCP/IP for short. The TCP/IP protocol allows for data packets to be as large as 65,535 bytes. However, the data packet size that is transmitted across the Internet is about 1,500 bytes. With a Ping of Death Attack, a massive data packet is sent-65,536 bytes. As a result, the memory buffers of the E-Commerce Server are totally overloaded, thus causing it to crash.

c) SYN Flooding

When we open up a Web Browser and type in a Web address, or click "Send" to transmit that E-Mail from our own computer (referred to as in this section as the "client computer"), a set of messages is exchanged between the server and the client computer. These set of exchanges is what establishes the Internet connection from the client computer to the server, and vice versa. This is also known as a "handshake." To initiate this Internet connection, a SYN (or synchronization) message is sent from the client computer to the server, and the server replies back to the client computer with a SYN ACK (or synchronization acknowledgement) message. To complete the Internet connection, the client computer sends back an ACK (or acknowledgement) message to the server. At this point, since the E-Commerce server is awaiting to receive the ACK message from the client computer, this is considered to be a half-open connection. It is at this point in which the E-Commerce server becomes vulnerable to attacks. Phony messages (which appear to be legitimate) could be sent to the E-Commerce server,

thus overloading its memory and processing power, and causing it to crash.

VI. IMPLICATIONS OF E - COMMERCE

The Internet has created a new economic ecosystem, the e-commerce marketplace, and it has become the virtual main street of the world. Providing a quick and convenient way of exchanging goods and services both regionally and globally, e-commerce has boomed. When using the Internet and E-Commerce is important to remember that there are many legal, moral and ethical issues to consider. Ethical, social, and political issues are closely linked. The ethical dilemma you may face as a manager of information systems typically is reflected in social and political debate. One way to think about these relationships is given in Figure 1. Imagine society as a more or less calm pond on a summer day, a delicate ecosystem in partial equilibrium with individuals and with social and political institutions. Individuals know how to act in this pond because social institutions (family, education, organizations) have developed well-honed rules of behaviour, and these are supported by laws developed in the political sector that prescribe behaviour and promise sanctions for violations. Now toss a rock into the centre of the pond. But imagine instead of a rock that the disturbing force is a powerful shock of new information technology and systems hitting a society more or less at rest. {see figure 1}

Figure-1, The Relationship Between Ethical, Social, And Political Issues In An Information Society

A) Ethical & Moral Implications

Businesses entering the e-commerce world will be facing a new set of ethical challenges. It is easy for businesses to become sidetracked in the technical challenges of operating in this way and to pay little attention to the ethical implications. There are many ethical implications for businesses to run into that would normally be addressed when doing business face to face, for example selling tobacco and alcohol to an underage minor over the internet, this is impossible to regulate easily and affectively as it would be if the person walked into a store, not only is this unethical but it is also illegal. Another case of this was a case when a community pharmacy decided to start up a E-Commerce site, of course here there was plenty of Moral and Ethical decisions to be made here, as Pharmaceuticals are different from other items of commerce, particularly in that they should only be used as and when they were required.

B) Legal Implications

The central issues of E-Commerce and the law include the development of E-Commerce, the role of consumers and regulation of e-commerce in regards to consumer protection. E-commerce is a new way of conducting business that takes place on the Internet; it has become an important way in which consumers purchase goods across the world as well as due to internet technology progressing rapidly in the last few years. Although E-Commerce has a big effect on the global trade, governments also have a large effect on the growth of E-Commerce on the internet by regulating is accordingly. As Governments set regulations for E-Commerce organisations managers are starting to worry if the regulations will be to tight or may reduce the market in the online trade. Regulation of E-commerce is very important for the cyberspace market as it can help or stop the organisations working with E-Commerce, as well as being able to protect the consumers in the online market.

C) Security Implications

There are a few security implications that come about when setting an E-Commerce website, especially when handling sensitive information such as credit card information and personal details such as address. Many

parts will have to be protected well including communication between the customer and the website server and the server itself from any hacker trying to intercept information or from trying to retrieve existing information from databases.

D) Customer & Server

To secure data between the customer and the web server there is a system called SSL (Secure Socket Layer) which encrypts the information between them so no one else can read it. The theory of it is quite basic and uses the following steps:

1. User want to send data to the server, before it leaves it is encrypted with a unique key for the session.
2. The server receives this information then encrypts the information one more time this time using its own unique session, this is completely different from the users unique key. It then sends back the data.
3. The user's computer now unlocks the data with the key it locked it with earlier; the data is still encrypted but now only with the servers key. The user's computer then sends the data back.
4. The server then receives this information and unlocks it with its key and now has the unencrypted data of what the user was sending to the server.

This type of encryption comes in different strings depending on the SSL certificate you purchase for your server, you can get certificates from 40-bit encryption up to 256-bit encryption.

E) Server Security

As well as security between the consumer and server there is also security needed on the server(s) as well, especially if sensitive information is stored under customers accounts, such as credit card information and other personal information. Servers will have to be protected to withstand any hack attempts to retrieve the information that is stored. Prevention measures such as firewalls, checking for root kits, antivirus systems and others should be put in place, as well as encryption of the data if possible so should a hacker gain entry the information he see's is useless to him or her.

VII. HOW TO KEEP YOUR COMPUTER SAFE FROM ONLINE THREATS?

The online world is full of both facilities and threats. Nowadays, a lot of users are getting virus infections in their computer while browsing the World Wide Web. A computer virus first enter in your PC silently, attach with a file, and then spreads its copies internally in the system files & Registry entries. In this write up, we will discuss the tips to keep your computer safe from the online threats. You can use them to secure your computer, important data, and information stored in it.

A) Security Applications First

You should install an antivirus with real-time protection and an antispyware in your computer. If you can opt for the paid antivirus then options are Norton, McAfee, Kaspersky, Panda, Bitdefender, Webroot, etc. Whereas the good free antivirus tools are AVG Antivirus, Avast Antivirus, Avira Antivirus, and Microsoft Security Essentials. You need antispyware to scan your computer for the spyware, adware, Trojan Horses, worm, and other malicious elements. Free and recommended antispyware solutions are Malware bytes Antimalware, SUPER Antispyware Free Edition, Spybot S&D, and Windows Defender. These free tools will not provide the real-time protection but remove all of the hidden & stuck infections, which are even not detected by antivirus.

B) Stay up-to-date

You should update your Operating System, Web browser, and antivirus regularly. Keep your Windows OS and antivirus to get automatic updates from their respective servers. Make sure to install the upgraded versions of Web browsers. Also, you should renew your license of antivirus to the latest upgraded version available. Remember the upgraded version of any software will have the latest fixes and security patches as compared to its outdated version. Also, the Windows Updates provides the latest security patches to its Windows OS to make it more secure from online threats.

C) Don't open unknown emails

If you are checking the emails in a client application like Outlook, Outlook Express, Windows Mail, Windows Live Mail, Eudora, Thunderbird, IncrediMail, etc. then make sure not to open the emails from unknown users. If you're browsing Webmail such as Gmail, Hotmail, AOL Email, Yahoo Mail etc. then don't open the attachments of emails sent from unknown persons. Make sure to mark as junk or spam those emails which are not sent by known users. This will let your email client to decide which emails are safe and which are unsecure.

D) Use the right Web browser

Make sure to use the right Web browser with its upgraded version. Google Chrome specifies the unprotected Websites with a banner before opening it. You can also install the extensions like McAfee SiteAdvisor, Web of Trust (WOT), AVG Browser Security Toolbar, and Avira Web Guard to enhance its security.

E) Sense Everything

Suppose you're opening the Website of your bank but suddenly you diverted back to a similar Website asking for complete credit card details with CVV number even without login. In this case, either you have typed a wrong URL or your browser is infected to divert you to an unsafe Website. Check each and every character you've typed in the Web browser before visiting a Website. The phishing Websites are those which shows you the exact snippet of the targeted site with a similar name. Such as go0gle.com is phishing whereas Google.com is good. The only difference is

that second O letter has been replaced with 0 (Zero).

F) Authentication

Most notable are the advances in identification and elimination of non-genuine users. Ecommerce service designers now use multi-level identification protocols like security questions, encrypted passwords (Encryption), biometrics and others to confirm the identity of their customers. These steps have found wide favour all around due to their effectiveness in weeding out unwelcome access.

G) Intrusion Check

The issue of tackling viruses and their like has also seen rapid development with anti-virus vendors releasing strong anti-viruses. These are developed by expert programmers who are a notch above the hackers and crackers themselves. Firewalls are another common way of implementing security measures. These programs restrict access to and from the system to pre-checked users/access points.

H) Educating Users

E-Commerce is run primarily by users. Thus, e-commerce service providers have also turned to educating users about safe practices that make the entire operation trouble free. Recent issues like phishing have been tackled to a good extent by informing genuine users of the perils of publishing their confidential information to unauthorized information seekers.

VIII. CONCLUSIONS

The Internet is a growing and a continually evolving creature that will live on in perpetuity. As such, it would be wise to ponder the various e business legal and Internet marketing ethical issues of both B2B and B2C business practices online. Whatever is written and published online today will likely be there tomorrow and possibly be recoverable forever. Imagine the billions upon billions of text information in web pages, publications, and books that are and will be stored for a long time to come. There is even a site where you can go way back in time to check out archives of other websites and view pages that were created at the beginning of their infancy. Additionally, old videos, films, movies, and audio in various applications formats are also viewable. With text messaging, wireless web mail, picture uploading, video recordings, and even video conferencing from cell phones and other personal communication devices with built in microphones and cameras, the Internet will be affecting more lives than ever before. Security and privacy concerns, along with e-business regulatory issues will become more prevalent. It will become more difficult to figure out who you can trust online, which websites are safe to visit, along with all the unethical, illegal, Internet marketing schemes, search engine optimization, search engine marketing, and online advertising frauds and all types of e- business email scams to contend with.

Applying good ethical standards to the online world is a direct reflection of your business online. Ethics affects all aspects of your business. It affects first and foremost your company's brand image and subsequently how sales, marketing, and advertising principles are applied to the task of making your company profitable for the long haul. Ethics affects your employees, and how they represent your company online, on the phone, in person, and all types of customer service and customer relations when dealing with buyers, engineers, sales leads, and potential customers.

ACKNOWLEDGEMENT

We would like to express our deepest appreciation and gratitude to our employers, friends, and colleagues for their kind cooperation and their support in writing this article. Special thanks to *Mr. Shekhar Anand* for his moral support and proper encouragement in preparing this. A tons of thanks to our parents for their tremendous support.

REFERENCE

[1]. Conklin, W.A, White, G.B., Cothren, C., Williams, D. & Davis, R.L. 2004, *Principles of Computer Security. Security+ and Beyond*, McGraw Hill, Illinois.

[2].Ford, W. 1994, 'Standardizing Information Technology Security', *StandardView*, vol. 2, issue 2, pp. 64-71.

[3].Gaur, N. 2000 'Assessing the Security of your Web Application' in *Linux Journal*, Vol 2000, Issue 72es, Article No. 3. Specialized System Consultants Inc. Seattle

[4]Gehling, B. & Stankard, D. 2005 'eCommerce Security' in *Information Security Curriculum Development Conference*, September 23-24 2005 pp32-38, Kenneshaw GA.

[5]Iachello, G. & Abowd, GD, 2005 'Privacy and proportionality: adapting legal evaluation techniques to inform design in ubiquitous computing' in *Proceedings of the SIGCHI conference on Human factors in computing systems*, Portland, Oregon, USA, pp91-100

[6]Kemmerer, RA. 2003'Cybersecurity' in *Proceedings of the 25th International Conference on Software Engineering* Portland Oregon, pp705-715, IEEE Computer Society.

[7]Leprévost, F., Erard, R. & Ebrahimi, T. 2000 'How to bypass the Wassenaar arrangement: a new application for watermarking' in *Proceedings of the 2000 ACM workshops on Multimedia*, Los Angeles, California, US. pp161-164

[8]Logan, PY. & Clarkson, A. 2005 'Teaching students to Hack' in *Proceedings of SIGCSE '05, February 23-27*, St Louis, Missouri, USA.

[9]McDermott, JP. 2001 'Attack net penetration testing' in *Proceedings of the 2000 workshop on New security paradigms*, County Cork, Ireland, pp15-21. ACM Press New York .

[10]McQuaid, H., Goel, A. & McManus M. 2003 'When you can't talk to customers: using storyboards and narratives to elicit empathy for users' in *Proceedings of the 2003 international conference on Designing pleasurable products and interfaces.* Pittsburgh, PA, USA pp120-125.

[11]Mitnick, K. & Simon WL. 2003 *The Art of Deception: Controlling the Human Element of Security* Wiley Publishing, Indiana.
[12]Prasad, B. 1998 'Decentralized cooperation: a distributed approach to team design in a concurrent engineering organisation' in *Team Performance Management* Vol 4, No.4 pp138-165 MCB University Press.
[13]Ray, I. & Ray, I. 2002 'Fair Exchange in E-commerce' in *ACM SIGecom Exchanges* Vol 3, Issue 2 Spring, pp9-17, ACM Press New York
[14]Rockwell, B. 1998, *Internet World*, Wiley & Sons, USA
[15[Suh, B and Han I., 2003, The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce, *International Journal of Electronic Commerce, Vol 7, No. 3, pp. 135-161*
[16]Tanenbaum, A.S. 2003, *Computer Networks*, Prentice-Hall, India
[17] Miller, Roger (2002). The Legal and E-Commerce Environment Today (Hardcover ed.). Thomson Learning. pp. 741 pages. ISBN 0-324-06188-9.
[18]Kotler, Philip (2009). Marketing Management. Pearson:Prentice-Hall. ISBN 978-81-317-1683-0.
[19]Nissanoff, Daniel (2006). **FutureShop**: How the New Auction Culture Will Revolutionize the Way We Buy, Sell and Get the Things We Really Want (Hardcover ed.). The Penguin Press. pp. 246 pages. ISBN 1-59420-077-7.
[20]Seybold, Pat (2001). Customers.com. Crown Business Books
[21]Chaudhury, Abijit; Jean-Pierre Kuilboer (2002). e-Business and e-Commerce Infrastructure. McGraw-Hill. ISBN 0-07-247875-6.
[22]Frieden, Jonathan D.; Roche, Sean Patrick (2006-12-19). "E-Commerce: Legal Issues of the Online Retailer in Virginia"(PDF). Richmond Journal of Law and Technology **13** (2).

