



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

A Survey Paper on Web Security fear and Impact to E-Commerce Success

Karishma Tyagi¹, Prof. Deepak Agrawal²

Research Scholar (Cyber Security), Department of Computer Science & Engineering, Takshshila Institute of Engineering & Technology, Jabalpur [M.P], India¹

Assistant Professor & Head, Department of Computer Science & Engineering, Takshshila Institute of Engineering & Technology, Jabalpur [M.P], India²

ABSTRACT: E-commerce has created nice strides in providing a convenient, quick and secure searching expertise for shoppers. However, there's still a major portion of shoppers whose security fears impact however they pay their cash on-line. thanks to this, security problems related to e-commerce and client sites should be perpetually reviewed and updated with acceptable countermeasures. As internet security threats noxiously have an effect on the success of electronic consumerism, it's imperative to teach each shoppers Associate in Nursingd businesses on the problems and the way to eliminate or minimize the risks of security breaching in an e-commerce surroundings. This paper presents a survey and analysis on e-commerce connected security problems, the impact to E-commerce success, and therefore the out there integrated security methods. we have a tendency to try to supply an easy guide the way to properly cater to the protection threats that noxiously have an effect on e-commerce. additionally, this paper provides Associate in Nursinging analysis on the barriers that forestall several developing countries from adopting e-commerce. Some recommendations on the way to overcome these issues will be provided.

KEYWORDS: e-commerce; web security issues; security threats; protection strategies; developing countries.

I. INTRODUCTION

The World Wide Web popularity leads to a revolution towards electronic commerce. Network transactions, electronic payments and on-line receipts are changing the traditional ways of doing business. Many companies take benefits of the e-commerce chances and other institutions will follow. The rapid growth of e-commerce is attracting the attention of businesses with its characteristics high-efficiency, low-cost, high-profitability and global application. However, Security fears cause million dollars loss for e-commerce retailers [21].

Lack of trust is one of the main reasons which can make e-commerce less attractive because of the fear of credit card number/or sensitive information being stolen. The increasing number of the web security attacks causes fears to consumers that resulted in lack of trust. Hence, many businesses and internet users are reluctant to use the new technology. According to the largest internet security company McAfee [1], almost half of consumers had terminated an order or due to security fears. Even in an attempt to get a good deal, 63% consumers will refuse to purchase from a Web site that does not show a Trustmark or security policy. Usually, e-commerce firms seek to get trust of their users by creating and advertising new security strategies, but the security threat is still growing and affecting e-commerce firms negatively. The issues of available reliable security technology and exploitation are not only limited to e-commerce technologies, but also broadly impacting computer and information systems throughout the world especially in developing countries because there are many gaps and lack of awareness as they are still at the exploratory stages.

In focusing on internet security issues and their impact on e-commerce, this paper presents a survey and analysis on e-commerce related security issues and the available integrated security strategies. We attempt to offer a



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

simple guide how to properly deal with the security threats that detrimentally affect e-commerce's success. In addition, this paper provides an analysis on the barriers that prevent many developing countries from adopting e-commerce more quickly. Some recommendations on how to overcome these problems will also be provided. The rest of the paper is organized in the following sections. Section 2 provides the definition of electronic commerce and the components of E-commerce system. Section 3 gives an overview on web security. In section 4, the concepts and the technologies of the security threats on e-commerce are presented. Section 5 is about the barriers for adopting e-commerce in the developing countries and the recommendations how to deal with the issues in developing countries. Section 6 is the conclusion of the research.

II. E-COMMERCE & SECURITY ISSUES

A. E-commerce Transactions


E-commerce) is defined as exchange transactions which take place over the Internet primarily use digital technology [2]. These exchange transaction including buying, selling, or trading for goods, services and information. There are four categories of electronic commerce: Business to Business, Business to Consumer, Consumer to Consumer, and Consumer to Business. E-commerce has enabled companies to build a market presence or to improve an already larger market position by allowing for a less expensive and more efficient distribution chain for their products or services. From consumers' perspective, e-commerce is mostly conducted on the internet. Many people nowadays find shopping online much more convenient and cheaper.

Online banking (e.g., online bill payments, buying stocks, transferring funds from one account to another, and initiating wire payments to another country) is another example of e-commerce. All these activities can be done with a few strokes of the keyboard. On the organizational level, many financial institutions and companies use the World Wide Web to exchange financial data to facilitate domestic and international business.

B. E-commerce System Components

There are four major components of e-commerce, the Merchant Account, Security System, the Shopping System and the Payment Gateway (for real-time-processing).

Merchant account: Bank authorized account which allows the acceptance of Payment Transaction Software - Software that processes customer order information, address, credit card number, etc. Then credit card authorization network verifies that the credit card is applicable and confirm the matching between shipping and billing address. However, if the card and the billing and shipping addresses do not match that might be a sign of stolen credit card.

Secure server connection: 'https://' connects to a special computer which encrypts confidential ordering data for clients protection. The "s" on the end of https in the URLs or the lock in the lower part of a browser which will look something like this  are signs that shows that the page is secured if ordering information is not sent through a secure server it can be intercepted by computer hackers.

Shopping cart: Software which facilitate accepting product orders for several products from a certain website. This software automatically calculates orders for customers. Some setup must be done in the html code of that website, and the shopping cart software must be installed on the server which hosts the site or on the secure server which accepts sensitive ordering information.

Payment gateway: Payment of different business transactions has taken a new direction due to the introduction of e-commerce. Increased use internet and growth of information have led to use electronic money thereby bringing an easier way of settling commercial transactions. This mode of payment though has brought many security threats, which threatens this ingenuity. The transaction starts when the user sends his or her order and



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

transfers the information from his browser to the shop-cart. The Secure Socket Layer protects the message during the transfer of this data to the Payment Gateway. This gateway is the connection between the website and the banking networks. It has both the gateway and the processor where the former provides access to the banking network ATM, the later handles financial information and communicates with shop-cart and transfer the same to the ATM network where it is like a normal credit transaction. The ATM network is the one that now connects to the Customers Credit Card Issuer, where a yes or no notification appears after reception of the data. This shows the approval or disapproval of the transaction. The whole process now starts again in reverse order to give the user feedback on the status of his transaction. When the order is confirmed to be genuine, it will then charge amount on the customer's account and send the Gateway an authorization code and the customer bank settles the rest of the transaction later at the end of each business day during batch settlement.

III. E-SECURITY ISSUES AND TRUST

“A security threat has been known as a situation, or event with the potential to effect economic adversity to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse Security, then, is the protection against these threats”[4]. Under this definition, threats can be made either through network and data transaction attacks, or via unauthorized access by means of defective authentication. This definition must be tailored in order to be appropriate to consumer transactions to acknowledge that consumer information has value. For customers, it must be recognized that economic hardship encompasses damages to privacy as well as theft, of credit information and authentication issues for consumers will be overturned; as in whether the Web site is ‘real’ rather than whether the purchaser's identity is real. This modified definition explains the security threats from a consumer's point of view. Security in B2C electronic commerce is reflected in the technologies used to secure costumer data. Security concerns of consumers may be addressed by many of the same technology protections as those of businesses, such as encryption and authentication [4].

The enormous increase in the uptake of ecommerce has led to a new generation of related security threats, but any ecommerce system must meet four integral requirements as defined below[5].

Confidentiality: Data is protected and cannot be accessed during transition.

Integrity: The system does not corrupt information or allow accidental changes to information except by an authorized agent.

Availability: The computer system's hardware and software maintain to work efficiently and the system is able to recover quickly and completely if a disaster happen.

Authenticity: The capability to find out who is responsible for the result of an action. Also, the role of consumer awareness and education on risks and protective measures, the limitation of consumer liabilities in case of fraud, the provision of redress mechanisms, and the use of merchant trust marks as trust building.

With increased cyber crimes, trust has become a critical in creating business relations. Trust enables consumers to be able to transact business freely even in a uncertain environment as they believe the seller can keeps his or her words. It is important for vendors to build exchange relationship with consumers so that they can trust the web vendor. This is a great aspect which takes time before it establishes itself, just as it has been in traditional business transactions. [6]

- People feel more comfortable to order products by phone, as they do not have full control of the data via their transfer.
- The parties of the operation may be in different regions and then follow different legalization.
- In most cases, both parties are unknown to each other.

It is vital for the trust to be build during the first transaction and there after maintained trust will enhance the



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

continuation of transactions with the website. If the first purchase faces some problems, the consumer may not be willing to get involved with the web vendor again. There are various factors such as reputation of the brand, and other interface information like web design, site information, and usability of the web that determines the consumer decision. The payment method, pricing, security policy, data protection, seller information, and seals of approval also inform the consumer decision. [7].

IV. THREATS CATEGORIZATION AND SOLUTION STRATEGIES

A. Security threats

Studies have shown that prominent attacks on online commerce are increasing at an alarming level. A study conducted by Ponemon Institute and commissioned by NetWitness shows that online threats are on the rise. The research investigated 591 IT and IT security practitioners and showed that 83% of them believe their companies has experienced some attacks, with 71% reporting a growth of threats over the past 12 months. These attacks aim mainly at stealing sensitive data including source code, non-[financial](#) business information, confidential information, and financial information [8].

Investigating the whole process of e-commerce can help in identifying security requirements, starting with the consumer, and ending with the commerce server. In view of each connection in the “chain of e-commerce,” the system must protect the assets to ensure secure e-commerce does not comprise the customer computer system and the data transmitted via the communication channels, the website and the e-commerce servers.

B. Threats Categorization

A hacker can target different points during an e-commerce transaction such as: [10]

- Trick an online shopper
- Sniff the network connection between an e-commerce website server and a shopper
- Attack a website’s server

Tricking Online Shopper: Hackers will often get access to sensitive information. They try to access the information during login session by hacking the system. The data they usually steal includes the customer’s usernames and their passwords, hijacking into customer databases of large corporations, and using confidential and personal information belonging to the user.

Phishing is a common method to trick a user; the attacker sends an e-mail message pretending it is from a trusted web. The message connects the recipient to another website, which is “spoofed” and looks like original web but is not genuine. It asks the user to update his/her login and personal data such as details of the customer bank account, a billing address, Social Security number. By doing this, malicious people are able to steal credit information [10].

Sniffing the Network: Packet sniffers are pieces of software that monitor network traffic. When data transfers from the shopper’s computer to the e-commerce website, it needs to pass through multiple connections. Hence, the data can be read by any computer it passes through and an attacker can sniff the network easily and steal personal information such as credit card numbers and passwords.

Attack a Website’s Server: Denial of service (DoS) attacks and Distributed Denial of Service (DDoS) attacks is an example of impact site availability. It is a well-known strategy attacker’s use in e-commerce with a malicious intent [8]. Use of a few machines ‘spoofing’ where many computer systems are hacked with software known as “bot” which is in a robot form. The software simultaneously connects to a server website. The number of concurrent connections is so numerous that it overloads the e-

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

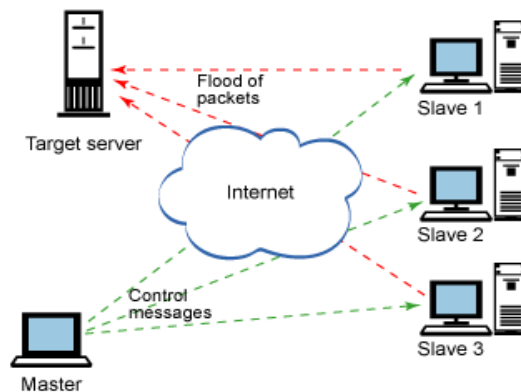


Fig 1: DOS Attack [10].

commerce servers making it hard for them to cope and finally they fail [9], as illustrated in Fig. 1.

C. E-commerce Security Solutions

A company-wide understanding of e-commerce security features, methods and threats will enable both users and security administrators to trust the system that they are working with. If accurate methods are utilized to secure and use a system, it is almost impossible for an unauthorized user to gain access. At the same time, the multitude of hacking and cracking applications available can cause a serious threat to e-commerce applications. Hence it is essential to understand security risks and find the best solutions to minimize the threats they impose. Fig. 2 shows available defenses against attacks.

Education: It is important to raise the awareness of web security. Educate people of how to choose strong password and keep their password confidential, is an easy way to minimize the risk of hacking attack. Users need to use good judgment when giving out information, and have knowledge about possible phishing schemes and other social engineering attacks [10].

Secure Socket Layer (SSL): This is the most common security method, public key encryption; it ensures confidentiality, authentication, data integrity, and non-repudiation of origin and return [17]. The technology used encloses transactions into encrypted envelopes and electronically seals where only people with the encryption key can view the contents of the envelopes that are sent securely over the internet [18]. However, partners must install the same software and coordinate their upgrade of their systems. Electronic Data Interchange(EDI) are used as wrappers to alter conventional EDI software into secure formats, such as Secure socket layer (SSL) encryption protocol which are good in protecting online transactions [19].

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

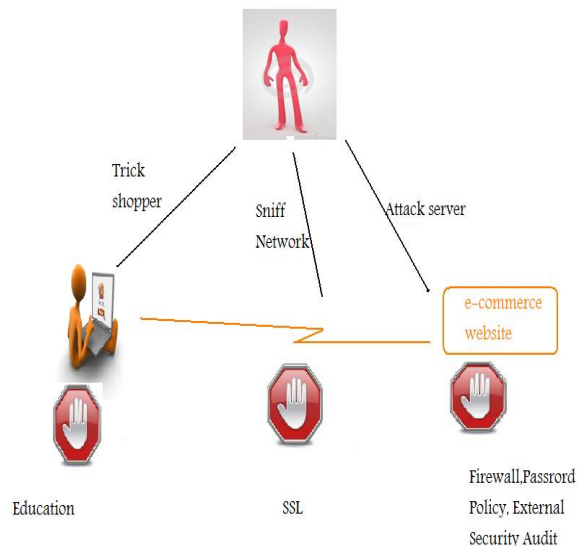


Fig 2: Attacks and their defenses.

Sensitive data, such as credit card details, health records, sales figures, etc, should be in encrypting form before transmission across the open internet via email or the web [11]. A 128-bit encryption protects the data from decryption by hackers easily in case they intercept it along the network. Digital certificates can be used here to encrypt email or establish a secure HTTPS connection with a web-server. For extra security, data can also be stored long-term in an encrypted format [11].

Personal Identification Number (PIN): This is another technique used in the payment system for internet users is on email callbacks. It uses a high-level protocol instead of using cryptography. It entails looking for a Personal Identification Number in database and then finds the email address of the consumer. [19]. An email message is then sent asking the payer to confirm the commitment whether he or she will pay a “yes,” “no” or “fraud.” Only when a receipt of a “yes” confirmation is the financial transaction actually initiated. Even “sniffings” cannot be used since the PIN is useless off internet and also other simple attacks.” Personal and sensitive data such credit card information never appears in internet messages and is linked to the virtual PIN after retrieval from database [17].

Personal firewalls: When a computer is connected to a network, it becomes vulnerable to attack. A firewall is a program that helps protect a computer by monitoring and blocking the types of traffic initiated by and directed to the computer. The intruder can also scan the hard drive to detect any stored passwords [10].

Security Policy: Making security policies is a very important step to secure an e-commerce business enterprise. The policy should clearly state the requirements for each element of the system the way of their interaction. An organization’s security policy define its position on the protection of its physical and IT assets. Security policy identifies physical, technological, legal and intellectual property assets and indicate how they should be protected [11].

When one gets a digital certificate from a trusted source it usually demand real proof and authentication identity and therefore, it is difficult to create a similar one. Digital signatures from sources such as VeriSign go through the web browser software of the client successfully since the software will note fake, digital signatures immediately.



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

V. ISSUES IN DEVELOPING COUNTRIES

According to the Organization for Economic Co-operation and Development (OECD), the major barriers for e-commerce adoption in developing countries are lack of legal mechanism to handle electronic related transactions. There is also lack of awareness about security issues and the IT security professionals. The initial set up cost is high and therefore, most companies in the developing countries cannot afford it. Pricing is also tricky and the fact that most of the population is unbanked and with limited knowledge on e-business and low penetration of using internet.

In developing countries, e-commerce is encountering problems, as people have not been experiencing to the e-business culture. This calls for urgent address of issues that are hindering the take off e-commerce in those countries. Agencies with legal credibility have to develop models and proper procedures. Business in developing countries has used a relatively developed, accessible, and affordable infrastructure. The cost, quality, availability, and accessibility of such infrastructure may hinder adoption of e-commerce. The lack of information and communications technology (ICT) transmission in an economy can also limit the level of e-commerce awareness which people in developed countries take for granted. Internet use has yet to reach a large population in developing countries and this has led to slow uptake of e-commerce. There are not even enough legal measures to ensure regulation of e-business and no institutions have been set. Lack of trust in the business has also led to large organizations to run the business failing to get involved.

Communication infrastructure must be in good condition for e-commerce to thrive in a business environment. For developing countries, initial investment is one of the main obstacles since most countries do not have the necessary resources to fund such an infrastructure. In addition, training and internet services must be accessible to the majority population in rural settings. To facilitate the diffusion of e-commerce there is the need for responsible government agencies to develop e-policies. Telecommunication infrastructure is clearly a necessary but not a sufficient requirement for the development and entry of a developing country into the cyber marketplace. The developing countries must also encourage investment and partnerships with vendors, suppliers, and telecommunications companies outside their borders. This requires a well-developed approach using the tools and strategies of an open and fair marketplace. In addition to the hard resources considerations made by many developing countries, a host of soft resources has to into play. The first of these is the establishment of national policies dealing with the information and telecommunication sector. This soft factor necessary so there can be a smooth adoption and penetration of e-commerce in these growing economies. Proper legal mechanism must also be set to protect e-business from loopholes brought about by legal issues. The laws dealing with consumer protection, privacy protection, and intellectual property rights are essential for the successful implementation of e-commerce programs.

Privacy and security of user information continue to be the most contentious topic in online transactions. The number of times security breaches such as data theft, file corruption, or web page shut down continues to rise as the number of online transactions rises. Telecommunication and e-commerce activities may face challenges if people in e-commerce cannot guarantee safety of their private information. In many developing countries use of security measures such as trusted third parties, data encryption, and secure telecommunication able to provide protection is needs to grow for e-commerce to thrive. The relations and confidence the e-e-business will create will determine the level of e-commerce diffusion in these countries.

VI. CONCLUSION

With today's high tech business and E-commerce environment, it is crucial to have the capability to protect information assets by implementing security measures. Losses of huge amounts of money and system damage are examples of the negative effects resulting from weak security measures. Security threats cause serious incident to e-commerce firms such as revenue loss, reputation damage, legal consequence and loss of market share. Therefore, e-commerce companies should use proper techniques to secure their system and increase user awareness of those



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

threats. To defeat the security obstacle for adoption in e-commerce in developing countries, decision-makers and IT Professionals should enhance the security of online payment and assure and educate the people about conducting online transactions. The government also should implement laws and procedures that allow businesses to function well and protect information. Dealing with the security issue will build and strengthen the trust in online transactions and lead to have a safe e-payment gateway for businesses and citizens. This will increase confidence in public and business to conduct online payment safely.

REFERENCES

- [1] McAfee study: online security fears affect online shopping. Ecommerce Journal. June29,2009.[Cited:0114,2011.] [http://ecommercejournal.com/news/16510_mcafee_study_online_security_fears_affect_online_shopping]
- [2] M. J. Schniederjans, Qing Cao. e-commerce Operations Management.s.l. : World Scientific Publishing Co., 2002.
- [3] BOILARD, ROBERT. HOW EXACTLY DOES ECOMMERCE WORK? I4Market. [<http://www.i4market.com/articles/d347.html>] Last retrived on March 15,2011
- [4] F.Belanger, Janine S. Hiller, Wanda J. Smith. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. 2002, The Journal of Strategic Information Systems, pp. 254-270.Scientific Publishing Co., 2002.
- [5] L. Clemer. Information Security Concepts: Confidentiality, Integrity, Availability, and Authenticity. May, 2010
- [6] S.M. Furnell, and Karweni, IT Security implications of electronic commerce: a survey of consumers and businesses., Internet Research: Electronic NetworkingApplications and Policy, 1999, pp.372-382C.
- [7] Centeno. Building Security and Consumer Trusting Internet Payments. April 2002.
- [8] Advanced security threats are growing in their scale. July, 2010 E- COMMERCE Journal[<http://www.e-commerce-journal.com>]
- [9] Protecting Online Banking from Denial of Service Attacks. Intru Guard. [<http://www.intruguard.com>]
- [10] Darshanad, Khusial & Ross, McKegny. IBM Developer Works. IBM. April, 2005. [http://www.ibm.com/developerworks/websphere/library/techarticles/0504_mckegney/0504_mckegney.html.]
- [11] Mazumdar, C, Barik, M and Sengupta, A. e-Commerce security – A life cycle approach. Kalkota, India : s.n., April/June 2005.
- [12] Lawson, M. Kapurubandara & Robyn. Barriers to Adopting ICT and e-commerce with SMEs in . 2006.[<http://www.scribd.com/doc/23874427/Barriers-of-e-commerce-and-e-government-in-Saudi-Arabia>.]
- [13] Kapurubandara1*, Mahesha and Lawson, Robyn.Availability of E-commerce Support for SMEs in Developing Countries. The International Journal on Advances in ICT for Emerging Regions, 2008, pp. 3-6.
- [14] Al-Gharbi, Khamis and Ashrafi, Rafi Factors Contribute To Slow Internet adoption in Omani sector.. IBIMA Publishing, 2010, pp. 7-8.
- [15] Alyabis. Examining the impact of Internet electronic commerce on commercial organizations in Saudi Arabia. Ph.D. Dissertation. University of Northern IOWA, December 2000. [16] A.Fahad.Scribd.2005/2006.[Cited:Feb23,2011.] [<http://www.scribd.com/doc/23874427/Barriers-of-e-commerce-and-e-government-in-Saudi-Arabia>.]
- [17] A.Sanayei and Rajabion, Lila. E-Commerce and Security Governance in Developing . Isfahan, Iran : s.n., 2008.
- [18] Herrmann, G. Herrmann and Peter Security and Trust in Electronic Commerce.. Business and Economics, 2004,pp. 1-2.
- [19] P.Prashant. The role of trust in e-commerce relational exchange: A uni ed model. Information & Management,2009, pp. 213-220.
- [20] J. Sheila. What Security Fears Cost E-Commerce. Ecommerce Times.[Cited: 01 24, 2011.][<http://www.ecommercetimes.com/story/smb/69667.html?wlc=1270740395&wlc=1271103816>]
- [21] Keizer, Gregg. Consumer Security Fears Cost E-Commerce \$2Billion. Information Week2006.