Cross Current International Journal of Economics, Management and Media Studies
*Abbreviated Key Title: Cross Current Int J Econ Manag Media Stud*
**ISSN:** 2663-2462 (Print) & Open Access
**DOI: 10.36344/ccijemms.2020.v02i02.003**

Volume-2 | Issue-2|Feb, 2020 |

Review Article

# Software Engineering Management for Increased E-Commerce Security and to Overcome E-Commerce Threats

**Mohammad Akbar**
Lecturer, Department of Software Engineering, Computer Science Faculty, Kunduz University, Afghanistan

***Corresponding author:**
Mohammad Akbar
**Received:** 09.01.2020
**Accepted:** 18.02.2020
**Published:** 29.02.2020

**Abstract:** The use of the internet has experienced tremendous developments in the business sector, especially in large scale companies. Since the discovery of internet technology. Basically, e-commerce is the buying and selling of goods and services on the internet and on different online networks especially World Wide Web. The development of e-commerce has led to companies moving much of their business efforts to online environments. Relying on security measures should be taken to provide the users with reliable e-commerce services such as encryption, digital signature, and verification technology and intrusion detection.
**Keywords:** E-commerce, online shopping, Cyber security, network security.

## INTRODUCTION

Electronic commerce or e-commerce, is the buying and selling of goods and services on the Internet (Nanehkaran, 2013). Other than buying and selling, many people use Internet as a source of information to compare prices or look at the latest products on offer before making a purchase online or at a traditional store. E-Business is sometimes used as another term for the same process. More often, though, it is used to define a broader process of how the Internet is changing the way companies do business, of the way they relate to their customers and suppliers, and of the way they think about such functions as marketing and logistics. For the purpose of this study e-commerce is taken to mean doing business electronically.

The application of e-commerce technology is one of the important factors to support the success of a product from a company. It is a familiar mode of shopping for many consumers. To accelerate and increase sales quickly, by looking at the rapid development of information technology, we can utilize an on-line service in the form of ecommerce. So far, the sales system of customers used by companies is only in writing and manual, which often tends to be misleading. With the existence of e-commerce services that can be quickly enjoyed by customers and companies themselves, all services desired by customers can be immediately followed up as quickly as possible, so that the company will be able to provide the best and fastest service for customers.

The main benefits of e-commerce from sellers' point of view is increasing revenue and reducing operation and maintenance costs through internet. These include as follows: • Increases revenue. • Reduces operation and maintenance costs. • Reduces purchase and procurement costs. • Raises customer loyalty and retention. • Reduces transportation costs. • Develops customer and supplier relationships. • Improves speed of the process of selling. • Improves internal and external communication. and • Develops the company image and brand.

The importance of security and privacy concerns in an online environment has been broadly discussed and reported in many studies. Godwin (2001) reported that privacy and security concerns were found to be a major barrier to Internet shopping. This concern has been extended to the Internet banking environment. Security has been widely recognized as one of the main

Quick Response Code
Journal homepage:
http://crosscurrentpublisher.com/ccemms/

obstacles to the adoption of electronic banking (Aladwani 2001), and privacy issues have proven important barriers to the use of online services.

E-commerce security is specifically applied to the components that affect e-commerce namely computer security, data security, integrity, availability and other wider realms of the Information Security framework. Many scholars have argued that trust is a prerequisite for successful commerce because consumers are hesitant to make purchases unless they trust the seller (Gefen, 2002; Jarvenpaa et al., 1999; Kim et al., 2005; Urban et al., 2000). The key to success in Internet business is the establishment of trusted transaction processes where e-sellers create an environment in which a prospective consumer can be relaxed and confident about any prospective transactions. Web e-commerce applications that handle payments such as electronic transactions using credit cards or debit cards, online banking, PayPal or other tokens have more compliance issues and are at increased risk from being targeted than other websites as they suffer greater consequences if there is data loss or alteration. Mule, Trojan horse and worms if launched against client systems, pose the greatest threat to e-commerce privacy and security because they can subvert most of the authorization and authentication mechanisms used in an ecommerce transaction.

Ecommerce web site owners on one side are thinking of how to attract more customers and how to make the visitors feel secured when working on the site, while on the other side how the end users should rate a ecommerce website and what they should do to protect themselves as one among the online community (Srikanth, 2012). Viruses are a nuisance threat in the e-commerce world. They only disrupt e-commerce operations and should be classified as a Denial of Service (DoS) tool. Password protection, encrypted client-server communication, public private key encryption schemes are all negated by the simple fact that the Trojan horse program allows the hacker to see all cleartext before it gets encrypted (Randy et al., 2002). Due to the increase in warnings by the media from security and privacy breaches like identity theft and financial fraud, and the elevated awareness of online customers about the threats of performing transactions online, e-commerce has not been able to achieve its full potential. Many customers refuse to perform online transactions and relate that to the lack of trust or fear for their personal information (Yazdanifard and Edres, 2011). Clearly, the online transaction requires consumers to disclose a large amount of sensitive personal information to the vendor, placing themselves at significant risk. Understanding (indeed, even precisely defining) consumer trust is essential for the continuing development of e-commerce.

A security objective is the contribution to security that a system is intended to achieve. E-commerce is conducted on global network that is Internet which is untrusted. Therefore, confidentiality is required during transaction and sending information should be kept secure against all type of threats. Security has emerged as an increasingly important issue in the development and success of an E-commerce organization. Gaining access to sensitive information and replay are some common threats that hackers impose to E-commerce systems (Berlin, 2007). The successful functioning of E-commerce security depends on a complex interrelationship between several applications development platforms, database management systems, systems software and network infrastructure (Kesh and Nerur, 2002).

## CONCLUSION

Information security has become a very critical aspect of modern communication system. Privacy, integrity, confidentiality and non-repudiation are main security dimension to protect E-commerce transactions against threats. Security is the key element that ensures the development of e-commerce. Although the Internet has its weakness in security, almost all layers of the network have formed security protocols. The security of network is the foundation of e-commerce, and the commonly used technologies include firewall, VPN and anti-virus. The firewall technology protects data in the Intranet with IP filtering and proxy. VPN ensures the security of data between enterprises in the Extranet and access to central system by using IP tunnel technology. Relying on any one of these measures alone is not sufficient. Other security measures should also be taken to provide the users with reliable e-commerce services such as encryption, digital signature, and verification technology and intrusion detection.

## REFERENCES

1. Aladwani, A. M. (2001). Online banking: a field study of drivers, development challenges, and expectations. *International Journal of Information Management*, *21*(3), 213-225.
2. Berlin, D. (2007). Information Security Perspective on Intranet. *Internet and E-Commerce Infrastructure*, *12*, 545-554.
3. Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *33*(3), 38-53.
4. Udo, G. J. (2001). Privacy and security concerns as major barriers for e-commerce: a survey study. *Information Management & Computer Security*9(4): 165-174.
5. Grabosky, P. (2001). The nature of trust online. *The Age*, pp. 1–12.
6. Tractinsky, N., Jarvenpaa, S. L., Vitale, M., & Saarinen, L. (1999). Consumer Trust in an Internet Store: a cross-cultural validation. *Journal of Computer-Mediated Communication*, *5*(2), 48-65.

7. Kesh, S.R.S., & Nerur. S. (2002). A Framework for Analyzing E-Commerce Security," *Information Management and Computer Security, 10*(4), 149-158.
8. Kim, D. J., Song, Y. I., Braynov, S. B., & Rao, H. R. (2005). A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia/practitioner perspectives. *Decision support systems*, *40*(2), 143-165.
9. Nanehkaran, Y. A. (2013). An Introduction to Electronic Commerce. *International Journal of Scientific & Technology Research, 2*(4), 190-193.
10. Marchany, R. C., & Tront, J. G. (2002, January). E-commerce security issues. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences* (pp. 2500-2508). IEEE.
11. Srikanth, V., & Dhanapal, D. R. (2012). E-commerce online security and trust marks. *International Journal of Computer Engineering and Technology*, *3*(2), 238-255.
12. Urban, G. L., Sultan, F., & Qualls, W. J. (2000). Placing trust at the center of your Internet strategy. *Sloan Management Review*, *42*(1), 39-48.
13. Yazdanifard, R., Edres, N. A. H., & Seyedi, A. P. (2011). Security and privacy issues as a potential risk for further ecommerce development. In *International Conference on Information Communication and Management-IPCSIT* (16).