

Evaluate the Usability of ‘Security Audits’ in Electronic Commerce

K.A.D.C.P Kahandawaarachchi, M.C Adipola, D.Y.S Mahagederawatte and
P Hewamallikage

3rd Year Information Systems Undergraduates

Sri Lanka Institute of Information Technology, Malabe Campus, New Kandy Road, Malabe.
chathuri0802@yahoo.com, madurangi.c@gmail.com, suviyashi@gmail.com,
Pulathisi_911@yahoo.com

Abstract

The advent and the expansion of the Internet increases the amount of trade conducted electronically. Electronic commerce encompasses a series of business activities and processes from eBanking to offshore manufacturing to eLogistics. However, the expansion of eCommerce is found to be limited in the South Asian region and especially in Sri Lanka, mainly to: security issues and a lack of trust in conducting business over the Internet or any other network.

Security Audit helps to overcome eSecurity issues to a great extent. eSecurity Audit includes: Internet configuration, design and implementation assistance, development of information security policy, independent evaluation of security countermeasures and firewall service, firewall audit etc. Security audit can apply to all other South Asian countries too.

Our research was to identify and understand what eSecurity audit is, evaluate its usability in eCommerce and identify its usage in business organizations. These objectives were realized through discussions and interviews with Information Security Professionals, auditors and with the use of a questionnaire. The scope of the questionnaire was narrowed and used on a selected sample of business organizations using eCommerce in Sri Lanka.

1. Introduction

1.1 Electronic Commerce

Electronic commerce can be defined as businesses conducted electronically through electronic data transmission technologies such as the Internet and World Wide Web by using Web applications such as Web sites, email services, instant messaging, Electronic Data Interchange (EDI), File Transfer Protocol (FTP), shopping carts etc to transact goods, services, data and funds relating to transactions as well as regular money transfers between business and the consumer or another business organization. An important aspect to be borne in mind with electronic commerce is that important business transactions are conducted electronically.

Electronic methods to deal with business transactions are considered quite simple and help increase profits through increasing sales and decreasing transaction costs and can be available to customers at any time from anywhere. Electronic commerce, the types of which are described below, eliminates the middleman in transactions so that the business directly interacts with the customer and the relationship between businesses and the customer increases. It also allows for business to expand across geographical borders to help narrow market segments, geographically impossible, reach the global

marketplace with speedy transactions. Customers too benefit from electronic commerce with new market channels offering a wide range of choices for their business purposes.

Enterprise Resource Planning (ERP) software give greater flexibility to these businesses with standardised business object models and distributed object computing.

1.2 Types of Electronic Commerce

- Business to Business (B2B) - is business transactions between two business organizations using electronic means such as EDIs or engage in supply chain technology among trusted business partners.
- Business to Consumer (B2C) - unknown business partners access business information systems of the suppliers.
- Consumer to Consumer (C2C) - Auction sites where customers are buyers as well as sellers.
- Business to Government (B2G) - electronic business transactions between companies and governments.

1.3 The Electronic Commerce Architectures

- Two tier architecture
A client accesses the server using a Web browser resident in the client machine and the server provides the requested service.
- Three tier architecture
A middle tier is added to the client environment and the server environment.
- Distributed enterprise architecture
Distributed enterprise architecture Organizations that have extended their operations to many different physical locations need to manage and make data available for all users, therefore the database systems that are been used, store the same data in many different physical locations.

2. Security Issues

The use of the Internet and networks for on-line purchasing and electronic transactions, contribute towards growth in global electronic commerce. However, the public remains concerned about privacy, security and equitable access costs.

Any eCommerce on the Internet is subject to interception, tracking or attack and requires the use of cryptography to code transmissions for security and privacy with which encrypted data becomes reasonably secure at each end. There is a need for digital certificates to establish the authenticity of on-line users and also a Public Key Authentication Framework for security.

2.1 eCommerce Security Classification

Any eCommerce system has to meet four requirements: privacy which requires information to be kept from unauthorized parties, integrity which relates to messages that must not be altered or tampered with, authentication which refers to sender and recipient proving their identities to each other, and non-repudiation which refers to a necessity for proof that the message was indeed received.

Privacy is handled by encryption. In Public Key Infrastructure (PKI) a message is encrypted by a public key, and decrypted by a private key. The public key is widely distributed, but only the recipient has the private key. For authentication (proving the identity of the sender, since only the sender has the particular key) the encrypted message is encrypted again, but this time with a private key.

Digital signatures perform authentication and integrity. A plain text message is run through a hash function and so given a value: the message digest. This digest, the hash function and the plain text encrypted with the recipient's public key are sent to the recipient. The recipient decodes the message with their private key, and runs the message through the supplied hash function. The message digest value remains unchanged. Very often, the message is also time stamped by a third party agency, which provides non-repudiation.

Information sent over the Internet commonly uses the set of rules called Transmission Control Protocol / Internet Protocol (TCP/IP). The information is broken into packets, numbered sequentially, an error control attached and individual packets sent by different routes. TCP/IP reassembles in order and resubmits packets showing errors. Secure Socket Layers (SSL) use PKI and digital certificates to ensure privacy and authentication.

Firewalls protect a server, a network and an individual PC from attack by viruses and hackers. Equally important is protection from malice or carelessness within the system, and many companies use the Kerberos protocol, which uses symmetric secret key cryptography to restrict access to authorized employees.

2.2 Practical Consequences

The merchant is always responsible for security of the Internet-connected PC where customer details are handled. Virus protection and a firewall are the minimum requirements. In order to be absolutely safe, sensitive information and customer details should be saved on zip-disks, a physically separate PC or with a commercial file storage service. Multiple back-ups of essential information must be kept stored safely off-site and ensure they are secure.

3. Detailed Analysis of the Research

eCommerce includes the conduct of business with customers, suppliers, and other external business partners using Internet or any other public/private network. Mainly it can be categorized into B2B & B2C eCommerce. This is a vast area. We limited our research scope to B2C eCommerce conducted over the Internet.

More and more organizations now try to use electronic means to conduct business with customers. The connection with the internet exposes B2C applications to inherent threats such as hackers, viruses & impersonation which would affect the confidentiality, integrity and availability of the application. Therefore B2C eCommerce reviews would play a significant role to avoid from those threats by assessing the adequacy of the protection against such threats.

3.1 Objectives

- Identify and understand what eSecurity audit is
- Evaluate its usability in Electronic commerce
- Identify its usage in business organizations

3.2 Research Focus

Audits conducted in the following areas:

- Evaluating The Business Aspects Of An Ecommerce Application
- Change & Content Management Process
- Communication Control Reviews
- Data Storage Integrity Review
- Protection Against External Threats
- Availability Of The Application & Business Continuity Review
- Efficiency & Effectiveness Reviews
- Third Party Services Reviews.

3.2.1 Evaluating the Business Aspects

In order to evaluate the security audits in Business Aspects we focused our questionnaire as follows:

1. On evaluating the compatibility of business strategy with the B2C applications objectives
2. Extent to which the organizations financial viability depends on the site
3. Business viability (cost-benefit) of the B2C application in the business.

| Security audit conducted | No of org | % | Over all % |
|--|-----------|------|------------|
| 1.) Evaluate the compatibility of business strategy with B2C applications objectives | 20 | 100% | |
| 2.) Extent to which organizational viability depends on the site | 13 | 65% | 88% |
| 3.) Business viability | 20 | 100% | |

Table 1 – Results For Evaluating The Business Aspects

According to the research results almost all organizations, which is 88% carry out audits on business aspects. It is a combination of 100% contribution in evaluating the compatibility of business strategy with the B2C applications objectives and business viability (cost-benefit) of the B2C application. But the audit reviews in the extent to which the organizations financial viability depends on the site was carried out only by 65% of the population.

3.2.2 Evaluate the Change and Content Management Process

For the evaluation of the security audits carried out in Change & Content

Management Process of the organization we carried out our research on the areas of:

1. Maintenance of change logs of the application
2. Appropriateness of language used, presentation & correctness of information published,
3. Adequacy of audit trails relating to key contents (terms, conditions & prices).

| Security audit conducted | No of org | % | Over all % |
|--|-----------|------|------------|
| 1.) Maintenance of change logs of the application | 20 | 100% | |
| 2.) Appropriateness of language used | 20 | 100% | 88% |
| 3.) Adequacy of audit trails relating key contents | 13 | 65% | |

Table 2 – Results for Evaluate the Change & Content Management Process

According to our research almost all organizations carry out compliance audits on development process of the organization. Security audits carried in the area of maintenance of change logs of the application and appropriateness of language, presentation & correctness of information is done 100% by our population. The audit reviews regarding adequacy of audit trials relating to key contents (terms, conditions & prices) is done only by 65% of our population. Therefore, the overall reviews conducted under the area of Change & Content Management Process is 83.33% of the overall population, with which we can conclude that almost all organizations carry out security audits reviews in Change & Content Management Process.

3.2.3 Communication Control Review

The communication control review focuses on secure communication channel used by companies when communicating with external parties via the Internet or other

private networks they use. The available technologies include encryption methods.

The questionnaire contained questions based on the following:

1. Appropriate encryption technology/mechanism used in transmission
2. Security of communication across the network

| Security audit conducted | No of org | % | Over all % |
|---------------------------------------|-----------|-------|------------|
| 1.) Access Logs | 20 | 100 % | |
| 2.) Access privileges to the database | 11 | 57% | 86% |
| 3.) Archived data | 20 | 100 % | |

Table 3 – Results For Communication Control Review

With the table we can arrive at the following conclusion regarding Communication control reviews:

According to the survey conducted the companies that perform communication control reviews are 42.85% out of a total of 20 companies considered in the sample. 28.6% do compliance audits on encryption technologies used in transmitting their data through the network and only 57.1% conduct audits on security of the communication across the network. Therefore, it can be determined that companies pay very little attention in carrying out security audits in the area of communication control.

3.2.4 Data Storage Integrity Review

With data storage integrity review, our main concern was on how companies store their data, use authentication methods and access logs which are necessary to protect

data from unintentional or intentional access to them.

Under the data storage integrity the questionnaire contained questions on the following:

1. Access logs
2. Access privileges to the database
3. Archived data

| Security audit conducted | No of org | % | Over all % |
|--|-----------|-----|------------|
| 1.) Appropriate encryption technology/mechanism used in transmission | 6 | 29% | 43% |
| 2.) Security of the communication across the network | 11 | 57% | |

Table 4 – Results For Data Storage Integrity Review Process

According to the table we observe that except for access privileges to the database audits majority of the companies perform audits under the data storage integrity domain. We can arrive at the following conclusion regarding this domain reviews:

Most of the companies in the sample analyzed conduct reviews on the data storage integrity which remains at 85.7%. Audits on access logs and archived data are carried out by all the companies and audits on access privileges are conducted by 57.1%.

3.2.5 Protection against External Threats

In a B2C Web site security audit the auditor should evaluate the threats imposed by the environment, taking into account the nature of the business organization. External threats can arise from various sources such as hackers, competitors etc. The nature of the business organization: market share, intensity of competition, use of Information Technology for business, was used to

determine the possible threats and their sources.

In a security audit it should be assessed whether countermeasures are in place in order to commensurate those external threats. The questionnaire focused on five such areas reviewed under such process.

1. Security architecture of the application
2. Virus protection mechanism
3. Firewall implementation
4. Intrusion detection mechanism
5. Existence of relevant logs as well as their ongoing reviews.

| Security audit conducted | No of org | % | Over all % |
|---|-----------|-----|------------|
| 1.) Security Architecture of the application | 17 | 85% | |
| 2.) Virus protection mechanism | 17 | 85% | |
| 3.) Firewall implementation | 17 | 85% | 76% |
| 4.) Intrusion detection mechanism. | 17 | 85% | |
| 5.) Existence of relevant logs as well as their ongoing reviews | 8 | 40% | |

Table 5 – Results for Protection against External Threats

According to the observations except for the log reviews, other reviews are performed by a majority of 85% organizations. Taken as a whole, 76% of companies have conducted reviews under the External threats review domain. This is a positive sign.

3.2.6 Availability of the Application and Business Continuity

The loyalty & reliability of customers is retained and the revenue generation through

the Web site is greatly dependent on its availability. Therefore, the questionnaire included security audit assessments of:

1. Capacity planning process
2. Backup storage
3. Disaster recovery procedure
4. Fallback arrangements

| Security audit conducted | No of org | % | Over all % |
|---------------------------------|-----------|-------|------------|
| 1.) Capacity planning process | 17 | 85 % | |
| 2.) Backup storage | 16 | 80 % | 88 % |
| 3.) Disaster recovery procedure | 17 | 85 % | |
| 4.) Fallback arrangements | 20 | 100 % | |

Table 6 – Results for Availability of the Application & Business Continuity

From the above table we can conclude that businesses' concern, on availability & business continuity is as high as 88% since availability & business continuity is of vital importance for Web business. Performance of such reviews would safeguard company's Website objectives and thereby safeguard the company assets.

3.2.7 Efficiency and Effectiveness Reviews

The reviews carried under efficiency and effectiveness were to determine whether organizations carry out security audits regarding the volume of transactions handled by the Websites, how cost effective the application as well as how easy it is to use and to find any audit conducted on customer feedback regarding the Websites.

The questionnaire addressed the following areas:

1. Volume of transaction through B2C application

2. Cost efficiency of the eCommerce application
3. Ease of use of the application
4. Customer feedback

| Security audit conducted | No of org | % | Over all % |
|---|-----------|------|------------|
| 1.) Volume of transaction through B2C application | 5 | 25% | |
| 2.) Cost efficiency of the ECommerce application | 8 | 40% | 59% |
| 3.) Ease of use of the application | 20 | 100% | |
| 4.) Customer feedback | 14 | 70% | |

Table 7 – Results for Efficiency and Effectiveness Reviews

The table provides values for us to arrive at the following conclusion regarding reviews on Efficiency and effectiveness:

Companies who do perform reviews on their volume of transaction handled through the B2C applications are few and as a percentage it is 25 from the total sample of 20 companies. Most of the companies perform reviews on ease of use and customer feedback about the applications. A lesser number of companies perform reviews on cost effectiveness of the eCommerce application which is 40%. Therefore, we can arrive at a conclusion that a majority of the companies, which is 58.75%, do perform security audits on efficiency and effectiveness of the B2C applications they use.

3.2.8 Third Party Services Reviews

In reviews on third party services the research focuses on whether the B2C eCommerce solution depends on any third-

party service providers, such as an Internet Service Provider (ISP), Certificate Authority (CA), Registration Authority (RA) or Web-hosting agency) and protection mechanism provided by the third parties are reviewed in security audits.

The questionnaire was on the following areas:

1. Appropriate and adequate procedures at the third party's end

2. Adequate protection of the interests of the organization as related to contracts and service level agreements

| Security audit conducted | No of org | % | Over all % |
|---|-----------|-----|------------|
| 1.) Procedures at the third parties end are appropriate & adequate | 11 | 55% | 70% |
| 2.) Interest of the organization are being protected due to third party contracts | 17 | 85% | |

Table 8 – Results For Third Party Services Reviews

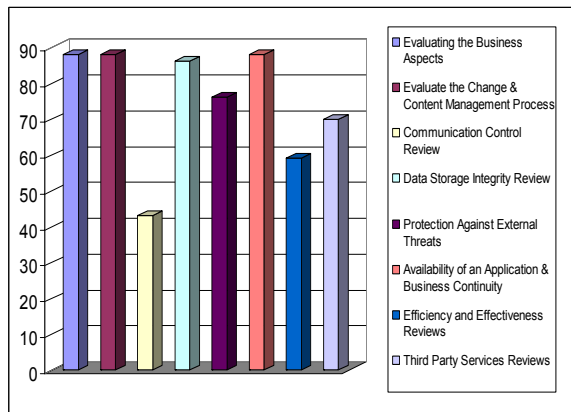
From the results we can come to following conclusion regarding the third party services:

The reviews on procedures at the third party's ends are appropriate and adequate enough as performed by 55% percent of the companies and 85% performs audits on interests of the organization are being protected adequately due to related contracts and service level agreements. Therefore, 70% of 20 companies, which is a majority from the total sample, do perform audits on third party services.

4. Conclusion

The research concentrated on eight major areas of electronic commerce to

determine whether they are currently used by businesses. It was revealed that different businesses had different and varied focus.



Graph1: Overall Performance Of eCommerce Security Audit

The highest focus has gone into “Availability of the application & Business continuity reviews”, “Evaluating the Business aspects audits” and “Evaluate the Change & Content management process”. As a percentage it is 88%, whereas the least number of audits that is only 43% of the companies have conducted “Communication control review”

However, it is interesting to note that there is use of security audits with many of the participant businesses indicating their awareness and performance of security audits. Accordingly, we could conclude that concerns regarding security reviews are on the rise and would remain so.

However there is a lack of computer aided tools available for the purpose. Perhaps, availability of such tools could entail better security facilities for eCommerce to become popular.

5. Recommendations

There should be awareness rising at regional level regarding the usability of security audit in

the B2C eCommerce and the importance to maintain such audits should be highlighted.

Some **regulatory body** or institution can be created at regional level to monitor or enforce the necessity of security audit requirements for B2C applications. This could be very much useful and productive for the organizations to achieve their web site objectives, profits and there by achieve organizational mission and vision.

Regional standards for B2C eCommerce security audits can be developed taking into account all international standards like COBIT available.

Further when organizations perform security audits on B2C applications they should look into all possible areas of possible security breach and perform the audit. It should not be biased towards any area.

6. References

- [1] Gary P. Schneider, “Electronic Commerce”. Fourth Annual Edition.
- [2] eCommerce Security: Securing the Network Perimeter [Online] www.isaca.org/TemplateRedirect.cfm?template=/ContentManagement/
- [3] Electronic Commerce - Wikipedia, The Free Encyclopedia (2006) [Online] http://en.wikipedia.org/wiki/Electronic_commerce
- [4] Basic Guide to eCommerce (Doing Business Over the Internet/Web) [Online] www.managementhelp.org/infomgmt/e_commerce/e_cmmrce/e_cmmrce.htm
- [5] eCommerce Advantages and Disadvantages [Online] www.marcbowles.com/sample_courses/a_mc/ec1/ec1_3.htm

- [6] Advantages of eCommerce
[Online]
www.isos.com.my/ecommerce/advantages.htm
- [7] eCommerce Architecture
[Online]
www.cmpe.boun.edu.tr/courses/cmpe472/spring2005/cmpe472archit-2003.ppt
- [8] eCommerce Architecture
[Online]
alfred.cse.buffalo.edu/DBGROUP/eCommerceArchitecture.pdf