Journal of Scientific Research and Development 2 (13): 117-126, 2015
Available online at www.jsrad.org
ISSN 1115-7569

Model of security factors for electronic commerce

Fatima Ajmal *, Norizan Mohd Yasin

Department of Information System, Faculty of Computer Science and Information Technology; University Malaya, Kuala Lumpur, Malaysia

Abstract: Despite the recent economic downturn in the telecommunication sectors and the Internet, electronic-commerce (e-commerce) continues to grow, and websites remain as an important communication channel between companies and their customers. As with time, the number of Internet users continues to increase, but many customers are still reluctant to provide their sensitive personal information because of their lack of trust on the Business-to-Consumers (B2C) e-commerce sites security and privacy. This paper aims to find the factors to increase security and privacy in e-commerce sites. For that conducted a detail literature search covering the past 23 years. This had helped us to find a total of 32 security factors of e-commerce in businesses that are divided into seven main categories: Security, Privacy, Ethical & legal issues, Intellectual property right, Trust and Loyalty. Based on the factors a conceptual model will be developed, this model will assist businesses or individuals who currently considering or conducting business using e-commerce. This review will list, discuss, analyse and evaluate these e-commerce security factors.

Key words: Electronic commerce; Security factors; Model; Privacy; Trust; Loyalty

1. Introduction

E-commerce defined often simply as buying and selling using the Internet but according to Bocij (2003) it also covers the pre and post sales activities across a supply chain. E-commerce definition is different according to various authors such as Zwass (1996) look into a broader definition of e-commerce is sharing of business information and maintain business relationships. Kalakota and Whinston (1997) refer to range of different perspective on e-commerce. For example, from the perspective of communication: the delivery of information, product/services or payment by electronic means. A business perspective: the application of technology toward automations of business transaction and work flows. Service perspective is enabling cost cutting at the same time of increasing quality and speed of service quality; and from an on-line perspective, the on-line buying and selling of information and products.

Online sales offering from e-commerce firms can change the way consumer purchase goods and services but the potential has not been fulfilled due, in part to consumer perception of risks involve in conducting business online (Zavod et al. 2001). Customer on an e-commerce site, mostly comfortable with providing general information such as preference but not when it comes to sensitive information such as the credit's card number (Suh and Han, 2003). This is mostly not because of lack of e-commerce security it is just they don't trust these services (Zavod et al., 2001). For e-vendors, therefore, it is critical to promote trust in order to transform a potential consumer from curious observer to who is willing to transact over the site. Understanding the nature and antecedents of consumer trust in the web vendors with a set of manageable, strategic levers to build such trust, which will promote acceptance of B2C e-commerce (Choudhury et al., 2002). In this review, after going through several articles have identified 32 security factors for e-commerce that business can consider to safeguard their online presence. The objectives of the paper are:

1) To identify factors that can affect businesses toward secure adoption of e-commerce in their respective organization/companies.
2) To develop the conceptual model for e-commerce secure adoption

In this paper, later will list and explain the factors; and in next section will define the e-commerce origin and development. This paper will provide a holistic approach toward providing security and privacy for e-commerce rather than focusing on the single factors of e-commerce security.

2. Theoretical background of the study

2.1. Electronic-commerce evolution

Bose (2002), refers to business orientation from the last 150 years, starting from the years 1850 to

* Corresponding Author.

2000, including the production (1850), sales (1900), marketing (1950) and customer centric (2000). In 1850, businesses could sell anything to customers, and such they were more focussed on production. In 1900 however, businesses realised that customers had more power, thus giving rise to the era of sales. Following this, in 1950 businesses came to another realisation, namely that the products they made must be market oriented, with a focus on the customers' needs (Bose, 2002). Today we see a very customer centric market, with businesses capable of treating every customer uniquely and independently according to their preference (Berger and Bechwati, 2001; Bose, 2002).

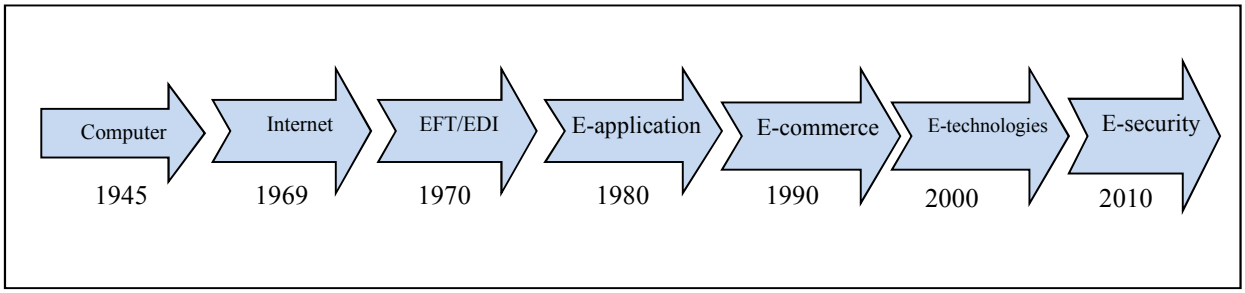

Fig. 1: E-commerce development over the last 67 years

Following the business orientation model has given rise to a model for e-commerce revolution over the years starting from 1945 to year 2014, as shown in Fig. 2.1. 1945 is the year that sees the invention of the computer, and although this year sees no development in e-commerce technology, it provides a framework for future technologies to take place. In 1969, the Internet introduces what is now the basis for today's e-technologies; the amount of trade conducted electronically must increase tremendously with the widespread use of the Internet in the present world. The e-commerce originally conceived to describe conducting e-commerce transactions electronically using Electronic Data Interchange (EDI) or Electronic File Transfer (EFT) (Kosiur, 1997; Trepper, 2000). These technologies emerge in 1970 with the innovation EFT; however, this technology is mostly used by financial institutions, large organisations and daring businesses (King et al., 2004; Zheng et al., 2005). Following this came the development of EDI, which transfers routine documents and executes electronic purchases in the form of invoices and orders (Kosiur, 1997; Sharda, 2000).

By 1980, more e- applications in e-commerce followed. A travel registration system for stocks trading, credit cards, ATM machines and telephone banking were a next step toward evaluation of e-commerce. Such systems are known as inter-organisational system applications, and their strategic value to businesses has been widely recognised. In the year 1990 when users started to flock to the World Wide Web, the term e-commerce became more commonly used between businesses (Black, 2000; Anumba and Ruikar, 2002). With this, many businesses began to open e-commerce sites known as dot.com. One reason for this sudden expansion was a development of new protocols, networks and software, as well as the increasing competitive pressure among businesses (King et al., 2004) thus allowing e-commerce to continue its growth. The Unites States estimates growing e-commerce revenue between 1999 through 2003 whilst Figs from the European union also show a constant upward increase in e-commerce activities implied by an explosion of the dot.com market bubble (Zheng et al., 2005), almost all medium to large enterprises currently have websites and portals through which to connect their suppliers and business partners. Since 2000, there has been a greater emphasis on small and medium-sized enterprises towards the adoption of e-commerce in their respective industries, whilst several studies have been conducted in this sector to improve the adoption process at a managerial level (King et al., 2004). From 2000 to 2015, extensive research is conducted to improve e-commerce adoption among businesses, as shown in Table 2.1.

With all of this said however, there remains a high tendency to not use the Internet when it comes to performing business transactions. A lack of trust on the part of internet users and SMEs when it comes to e-commerce is often assumed to be one of the many reasons for the disappointing development of Business to Consumers (B2C) in e-commerce (Reichheld and Schefter, 2000; Brengman et al., 2011). This lack of trust is thought to have many causes, and most literature centres on a perceived lack of security in Internet transactions, together with the fear of loss of privacy (Hamzah et al., 2001; Dresner et al., 2008; Lassala-Navarré et al., 2009; Polasik and Wisniewski, 2009; Zendehdel and Paim, 2012). As a direct result of these problems, e-commerce cannot grow at a rapid pace (Zendehdel and Paim, 2012). Therefore, from 2010, there has been an increase in research focussing on e-commerce security so as to encourage people to spend online by trusting the vendor.

2.2. Security in e-commerce

Online sales offering from e-commerce firms can change the way in which consumers purchase goods and services, although the potential has not been fulfilled due, in part, to consumer perception of the risks involved in conducting business online (Zavod et al., 2001; Lopez et al., 2005).

The current state of e-commerce is a good example that the supporting technology has not yet reached its full potential. During the late 90s there were many predictions regarding how e-commerce would develop in the near future (Zavod et al., 2001). For example, in 1990, Forrester Research (1999) predicted a volume of US$ 184 billion of US online retail sales in 2004 whereas the actual value is only US$ 69 billion, representing big gap. The potential of e-commerce has not been fulfilled due, in part, to consumers' perception of the risk involved with conducting business online (Lopez et al., 2005). Customers on an e-commerce site are mostly comfortable with providing general information to websites such as preferences, but are less comfortable when it comes to sensitive information such as a credit card number (Suh and Han, 2003). This is not because of a lack of e-commerce security, but it rather more to do with the fact that they do not trust these services (Zavod et al., 2001). For e-vendors, it is therefore critical to promote trust in order to transform a potential consumer from curious observer to one who is willing to transact over the site. It is crucial to understand the nature and antecedents of consumer trust in the web vendors, with a set of manageable, strategic levers to build such trust, which will in turn promote acceptance of B2C e-commerce (Choudhury et al., 2002).

According to Forrester Research, young consumers (59%) are primary reasons for not conducting business on-line whilst the remaining participants (approximately 43%) cite a concern for the on-line privacy of that data on the website (McQuivey, 2000). In order for e-commerce to reach, and exceed its full potential, there is a need for companies to provide an increase level of trust and confidence between the business and its customers. Indeed, the creation of technologies is essential in order to protect individual privacy and security in online business transactions.

Özkan, Bindusara, & Hackney (2010) study the critical factors (security, advantage, web assurance seals) which are necessary through customer intention to adopt e-commerce system. The perception of good security and trust will ultimately increase the use of e-commerce. In fact, customers' perception of the security of e-commerce systems has become major factor in the evolution of e-commerce in markets (Zhang and Wang, 2014).

Websites should adopt a privacy policy which allows a customer to trust the website with regard to sharing personal information (Choudhury et al., 2002). Interacting with online customers makes it possible to convey that the vendor is competent, honest, benevolent and predictable, thereby strengthening the customer's trusting belief (Ferrin et al., 2008). The vendor should advertise its good reputation in order to induce buying behaviour. Linking to other trusted sites allows for assurance building, thus enabling purchasing and Internet behaviour. Third party seals and guarantees from the sites such as BBB, AICPA's Webtrust or SysTrust increases the integrity of the vendor and allows a customer to trust the site (Choudhury et al., 2002).

When dealing with B2C clients, there is a great deal of responsibility imparted on the person or group of people which maintain the website. It is very important both in the context of ethical and legal business-to-consumer that what is written or portrayed about the company are factual. In addition, if proper business to business ethical behaviour is not being followed there is a possibility that trade secrets and/or intellectual property can be exposed. In order for e-commerce to exceed and to reach its full potential there is a need for companies to provide an increased level of trust and confidence between business and their customers. The technologies are needed to create to protect individual privacy and security in online business transactions.

3. Review research method

The reviews based on the reputable and reliable publication that help to fill the gaps in e-commerce research. These articles cover e-commerce and security of e-commerce in business. The articles that are selected are for on B2C commerce interaction and excluded the paper related to B2B and Consumer-to-Consumer (C2C) context. The reason for doing that is as determinants of security factors are likely to a difference in B2B and C2C environment than that of B2C in term for customer's type, trade/sales, business and decision making.

The articles are collected from two sources 1) Journal articles, books and literature on the topic of e-commerce security published. 2) From research paper published by authors in conference. The publication included in his review from year 1991 to 2001. There are a total of 300 articles selected from a collection of 530 articles, which were extracted from the 1,650 pre-investigated items. To find these articles, multidisciplinary databases are used. To find the relevant articles have used a list of keywords such as e-commerce security factors, e-security factors, security and privacy in e-commerce, e-loyalty, e-commerce trust, intellectual property right, ethical and legal issues in e-commerce. These keywords were used to find articles related all the topics discuss in this review.

4. Security factors in e-commerce

During the literature review, 32 security factors have been found to protect business from illegal activities and encourage them toward adoption of e-commerce. Here, the factors are divided into Independent factors that are Ethical & Legal issues, Security, Privacy, Intellectual property rights, Trust and Loyalty shown in Fig. 2. The factors are turned into a proposed model for defining e-commerce security in business. Under each Independent factor consists of variables or dependent (Contributing) factors shown in Fig. 3. This paper will explain all the factors in details and will define how it will be

beneficial for an organization in terms of research conducted on them by previous researchers.

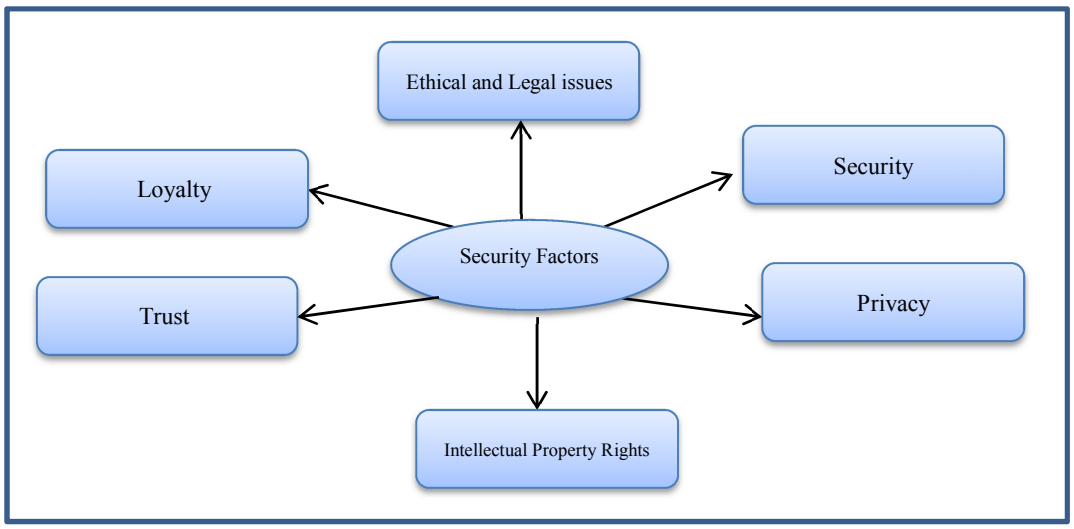

Fig. 2: Proposed model for E-commerce security

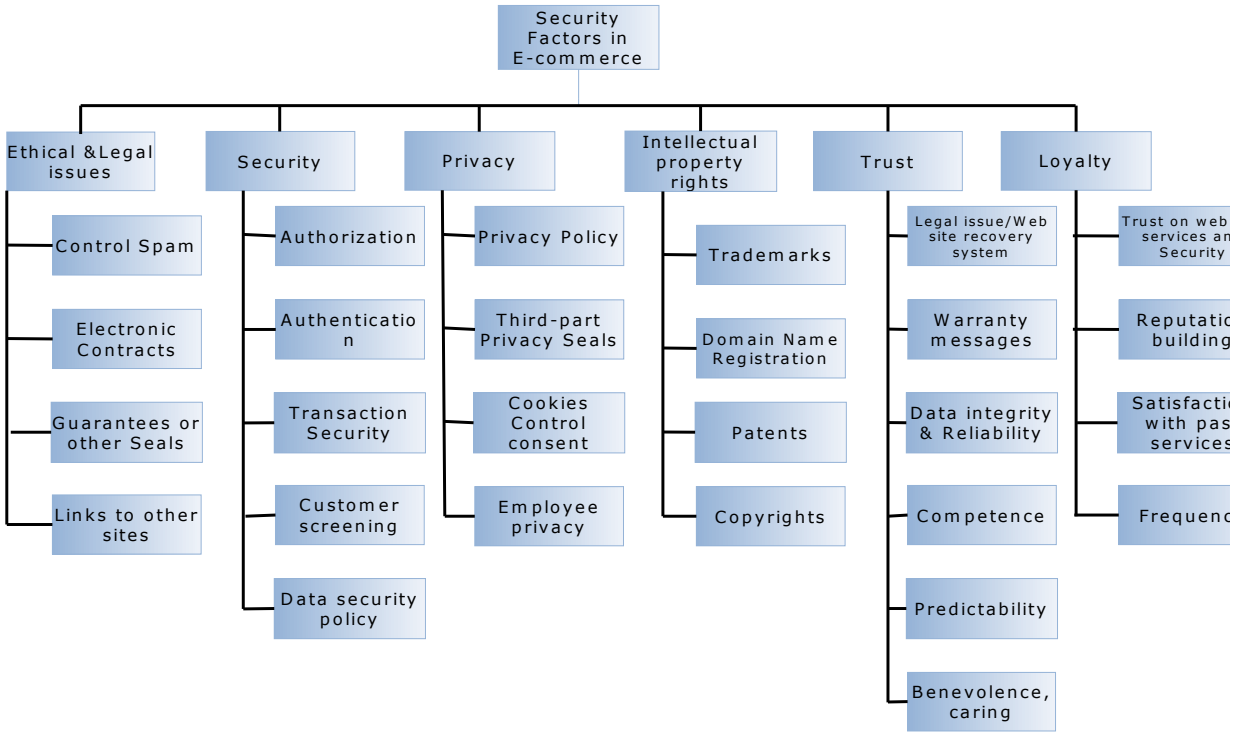

Fig. 3: E-commerce security factors

4.1. Trust factors

There are three characteristics to represent the perceived trustworthiness of the trustee, namely ability, benevolence integrity, competence and predictability (Ferrin et al., 2008; Sari and Rofiq, 2013). Indeed, should the trustee possess these qualities then trust will develop (an intention to accept vulnerability) toward the trustee (Ferrin et al., 2008; Zhang and Okoroafo, 2013).

(a) Warranty Messages: Site provides adequate and clear statement on warranty messages. Aspects like malfunctioning and misinforming must be clearly covered to improve the trust between buyer and seller.

(b) Data Integrity and Reliability: This means that one believes that the other party makes good faith agreements, tells the truth, acts ethically and fulfils promises (Bromiley and Cummings, 1995) to secure data against alteration and interception whilst also ensuring that the electronic record is not altered; electronic signature is used (Ter Kah, 1999).

(c) Competence: In the case of an Internet relationship, the consumer would believe that the vendor can provide the goods and services in a proper and convenient way.

(d) Predictability: Predictability is considered important in a trusting relationship as a consumer can predict the vendor's action. For example, in the case of Amazon, customers can predict that they will receive a book within seven

days, even if they receive no confirmation e-mail. This helps to build a trusting relationship between vendor and consumer (McKnight and Chervany, 2001).

(e) Benevolence (caring): Trusting belief-benevolence means that one party believes that the other party care about ones and is motivated to act in one's interest (McKnight and Chervany, 2001).

4.2. Security factors

According to Kalakota & Whinston (1996), Shahibi & Fakeh (2011), Zhang & Okoroafo (2014), a security threat is defined as a circumstance, condition, event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste and abuse. Security thus pertains to protection against these threats; security in e-commerce is reflected in the technologies used to protect and secure customer data (Hiller et al., 2002; bin Daud et al., 2011).

(a) Authorisation (Protection of a site from unauthorised outsiders): Access Rights should be granted on a need-to-know basis; security patches should be applied as soon as possible; sensitive or confidential data should be encrypted; web servers, network equipment, and other infrastructure components should be physically protected. Security best practices should be implemented as recommended by organisations such as the network security should be audited regularly by someone who specialises in intrusion detection and prevention.

(b) Authentication: Authentication ensures that the trading parties in an electronic transaction or communication are in fact who they claim to be (Suh and Han, 2003; Lassala-Navarré et al., 2009; Polasik and Wisniewski, 2009). The authentication can be implemented by some of the technology such as identity certificates, Public-Key Infrastructure (PKI), Privilege Management System (PMI) (Lopez et al., 2005; Luo et al., 2008).

(c) Transaction Security: Transaction security depends on the confidentiality of information between seller and buyer and non-repudiation that becomes even more important during the execution phase where secure payment is ensured as well as the secure delivery of the good (Shahibi and Fakeh, 2011). Therefore, according to Katsikas & Lopez et al. (2005) e-commerce security requirement depends on confidentiality, the integrity and availability of information and system, the authenticity of communication parties and the non-repudiation sources.

(d) Customer Screening: This is essential in order to protect a system from unauthorised access and can be done using a firewall and terminal, database, server, application, and operating system security measures (Suh and Han, 2003).

(e) Data Security Policy: The first step in securing entity, electronic data and the system involves a design security policy. Security policies are important because they define what is being protected and what type of restriction should be put on those controls (Smith, 2004).

4.3. Privacy factors

Privacy is "the condition of not having undocumented personal knowledge about one possessed by others" (Parent, 1983). Privacy related to issues of concern for both current and prospective e-commerce customers (Lanier, 2008; Okeke et al., 2013). There are a number of ways in which individual information can be found on the Internet, such as reading individual entries on a newsgroup posting; looking at individual names and identities in the Internet directory; by reading emails, conducting surveillance on employees, wiretapping wireless and listening to employees; asking an individual to complete website registration, and gathering information on individuals while they access the website by making use of cookies (King et al., 2004; Karakaya and Stark, 2013).

According to Harrison, McKnight & Choudhury et al. (2002), e-commerce allows for the maintenance of trust and development of relations with online clients such as privacy policy and third-part privacy seals, interacting with customers, reputation building, links to other sites and guarantees or other seals.

(a) Privacy Policy: An online privacy policy or OOP is often used by a website to provide a comprehensive description of their information practices (Antón and Earp, 2001). It informs users that their privacy rights are being considered and that the website understands the privacy concern faced by users (Alicia and Bardo, 2005). The information practices reflected in the firm's privacy policy should be open and honest, thus giving users the opportunity to evaluate the practices and make informed decisions regarding whether or not to disclose their personal information (Culnan and Bies, 2003). A website with a privacy policy will reassure consumers that the vendor is ethical, thus meaning that these consumers will be more willing to share information (McKnight and Chervany, 2001; Okeke et al., 2013). This will lead to an increase in repeat visits and more purchases (Marchewka et al., 2005).

(b) Cookies: Cookies and tracking software are used to follow consumers' online activities so as to gather information about their personal interests and preferences. This information is extremely valuable as it helps a company to sell customers the products and services tailored to their needs (Marchewka et al., 2005). According to Privacy and Electronic Communication Regulation, businesses have to inform their customers that they use cookies, and provide a choice for user who do not want to accept it; this means

providing users with a statement of privacy and cookies which tell them how they are being used and how they can be switched off by the users (King et al., 2004).

(c) Third Party Privacy Seals: Third party seals are increasingly used by businesses to communicate their commitment to security (e.g. Verisign) (Hiller et al., 2002). Groups like TRUSTe or BBBOnline, AICPA's Webtrust or SysTrust and Entertainment Software Board Real (ESRB) offer programs in which businesses can participate in order to show their commitment to privacy and security. Privacy seals offer a readily visible and easy way to reassure consumers that the online business respects individual privacy on the Internet (Marchewka et al., 2005).

(d) Employee's Privacy: In some cases technology has transformed arrangements, thus meaning that people can connect to company intranets from home. The growth of mobile Internet, whereby employees can access information on the move, has piled additional pressure on the security system (Anne-Marie et al., 2003). With this in mind, there should be a code of conduct for employees using a system that ensures privacy and security of consumer data. It is also not ethical for a company to access their employees' data and emails without their consent, and as such measures should be provided to protect individual employee privacy (Karakaya and Stark, 2013).

Organisations are educating their employees and provide necessary hardware and software that enhances user privacy. For example, if an organisation informs its employees of its policy and intention to monitor e-mails as well as the consequences of sending and/or receiving e-mails, considered inappropriate, then the employee may cut down on the number of such emails, and the organisation will have achieved their goals (Udo, 2001)

4.4. Ethical and legal issues factors

When dealing with 'Business to Consumer' clients, a great deal of responsibility lies with the person or group of people which maintains the website. It is very important in the context of an ethical and legal B2C perspective that what is written or portrayed about the company is factual. Furthermore, if proper business to business ethical behaviour is not being followed, there is the possibility that trade secrets and/or intellectual property may be exposed. As with any business's planning or publishing, website development involves a variety of legal issues and standards which should be followed. Such issues are considered to protect both the consumers and the owner of the site. The following details some of the areas that should be considered.

(a) Control Spam: Unsolicited commercial email commonly known as spam. The opt-in consent procedures for commercial e-mails were introduced by the Privacy and Electronic Communication Regulation, thus meaning that a business is only allowed to contact those people who have agreed to be contacted (Blanzieri and Bryl, 2008). In order to save businesses from the aggravation of having to obtain consent from all customers, the rule only applies to new customers (King et al., 2004). Businesses can continue selling their products to current customers, provided they can opt out of receiving future messages related to similar products and services. The US CAN-Spam Act (Controlling the Assault of Non-solicited Pornography and Marketing Act) of 2003 allows spam with new instructions, e.g. it demands that the advertiser's email address be included, that an opt-out link is present, that there is a legitimate return email address, and that messages are clearly marked as advertisement (Blanzieri and Bryl, 2008).

(b) Electronic Contracts: An electronic contract such as a digital signature is a mathematical scheme used to demonstrate the authenticity of a digital message or document. A digital signature provides a secure vehicle for the prevention of unauthorised alterations to the data and holds great potential for facilitating secure e-commerce transaction (Deng et al., 2012).

(c) Guarantees or Other Seals: Guarantees or other seals such as BBB, AICPA's Web Trust or SysTrust state that the reliability of a website would help to raise trusting belief in the integrity of the vendor, thereby endangering willingness to depend on that vendor. The trusting belief depends on the nature of the seal (McKnight and Chervany, 2001).

(d) Links to Other Sites: Linking to other trusted sites allows for assurance building, thus enabling purchasing and Internet behaviour (Stewart, 1999). The implication of the outside link is that one has a good company because that is good company. Indeed, this has an impact on the trusting beliefs relating to the site vendor (McKnight and Chervany, 2001).

4.5. Intellectual property rights factors

As privacy is a major concern for customers, intellectual property is a major concern for those who own intellectual property. According to the World Intellectual Property organisation, intellectual property refers to the creation of mind: invention, literary and artistic works and symbols, names and design used in commerce. There are four main types of intellectual property rights which link to e-commerce, including trademarks, domain name registration, copyrights, patents. There are differences when it comes to the way in which these rights operate. The patent holds for twenty years, whilst copyrights last until 70 years after the author's death, and trademarks can be continually renewed, meaning that they effectively last forever (Wilson, 2009).

(a) Trademarks: Trademarks are composed of symbols, letters, words, designs, numbers, shapes and combination of colours, etc. used by business to identify their goods and services. A trademark must be distinctive and original if it is to be registered and protected by the government (King et al., 2004).
(b) Domain Name Registration: the domain represents the virtual identity of the provider, and his/her products. In light of this, it also features as part of the trade name on visiting cards, brochures and in advertising copy (Thomas, 2000). A domain name refers to the upper category of a URL address. A variation of trademark is Domain name. Indeed, in 2002, the Internet's governing body on Website names approved the following top-level names; .Biz, .info, .name, .pro, .museum, .aero, .coop besides .com, .org and .gov which are already being used by the Internet community (King et al., 2004).
(c) Patents: A patent is comprised of documents, which provide the exclusive right on invention for a fixed number of years, e.g. 10 years in the United States and 5 years in the UK. The application of patents must include following one or more claims that it must be new, useful, non-obvious and industry applicable (King et al., 2004). The invention can be in the form of a physical device, method or a process of making a physical device.
(d) Copyrights: Copyright is an exclusive grant from the government that provides the exclusive rights to the creator of original work, including a right to copy, adopt and change the work. Copyright mostly exists in literary, musical, dramatic and artistic works; sound recording, film, broadcasting and cane program. In addition, copyright also protects images, photos, logos, text, HTML, java script and other material (King et al., 2004).

4.6. Loyalty factors

Modern day customers are in a very unique position, with many e-commerce businesses just a click away. Indeed, this provides a huge advantage to buyers, as they can compare the quality and price of products between the world-wide sellers (Chang et al., 2013). Therefore, in order for businesses to handle this type of competitive pressure, there is an ever growing interest in e-loyalty (Hansen and Jonsson, 2013). Customer loyalty increases sales of products and increases company profits over time (Chang and Chen, 2009; Kiran and Diljit, 2011). It also costs five to eight times more for a company to acquire new clients compared to keeping existing ones (Reichheld and Schefter, 2000).

(a) Trust in Website Services and Security: McKnight & Chervany (2001) present an interdisciplinary topology of trust which is related to e-commerce consumer actions. The typology consists of four concepts: disposition to trust, institution-based trust, trusting belief, and trusting intention (McKnight and Chervany, 2001). Trust is defined as a type of belief superior to faith and inferior to confidence; the faith-trust-confidence continuum (Egger, 2001). Trust in an e-commerce site helps to build loyalty in consumer behaviour (Cyr, 2008; Eid, 2011).
(b) Reputation Building: A web retailer's reputation is an important antecedent of trust, perceived risk and purchase intention (Pavlou, 2003). A positive reputation is considered a key factor for reducing risk and creating trust because it provides information which indicate that the selling party has honoured or met its obligation toward other consumers in the past (Ferrin et al., 2008) .
(c) Satisfaction with Past Services: Marketers are constantly attempting to discover the major factors leading to customer loyalty, satisfaction with services obviously representing one of the most important (Guinalíu et al., 2006; Chang and Chen, 2009). The best indication of customer satisfaction and business service quality is repeat visits to a website, a recommendation of the website to others, positive remarks or comments about the website and repeat purchases (Berry et al., 1996).
(d) Frequency: A peer may increase its trust value by increasing its transaction volume and numbers of transactions is an important scope factor in measuring satisfaction in different peers (Xiong and Liu, 2003). In addition, frequent shoppers are more likely to conduct a transaction (Pavlou, 2003).

5. Discussion

There is a lot of research conducted on the success factors of e-commerce, but limited research on secure e-commerce factors for e-commerce. This paper provides a basis for the research conducted in the field of e-commerce security. This review does not focus on a particular domain of e-commerce security such as privacy, trust, loyalty, intellectual property right but look at the holistic approach toward securing for e-commerce for business. This review will help businesses to consider security factors when implementing e-commerce site. So they will be able to provide a high level of security to their customers and achieve their trust and loyalty. For researchers, this research provides some interesting questions and a model to explore more on e-commerce security factors. This research also provides that the roles of security, privacy, trust, loyalty; Ethical and intellectual rights are all related and under one topic.

6. Conclusion

The e-commerce continues to grow in today's market, but still the on-line consumers are not spending much on the Internet. The reason and the main barrier to future growth of B2C e- commerce are a security concern among a consumer. The best

way to get over the barrier is to understand what the barriers are and how they work. This paper was intended to propose the holistic approach toward e-commerce security and privacy. In this review after going through past papers and research has identified 32 security factors that help businesses to understand these barriers and if followed can minimize these threats to security and privacy. Future research can be done for validating and empirically testing the security factor that will provide additional insights into e-commerce security and specific way to inspire it.

References

Aldás-Manzano, J., C. Lassala-Navarré, et al. (2009). "The role of consumer innovativeness and perceived risk in online banking usage." International Journal of Bank Marketing **27**(1): 53-75.

Alicia, L. and F. Bardo (2005). "Facilitating online privacy on eCommerce websites: an Australian experience." Journal of Information, Communication and Ethics in Society **3**(2): 59-68.

Antón, A. I. and J. B. Earp (2001). "A taxonomy for web site privacy requirements." North Carolina State University at Raleigh, Raleigh, NC.

Anumba, C. J. and K. Ruikar (2002). "Electronic commerce in construction--trends and prospects." Automation in Construction **11**(3): 265-275.

Article, F. R. (1999). "Forrester Research." Post-web retail, from http://forrester.com/.

Belanger, F., J. S. Hiller, et al. (2002). "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes." The Journal of Strategic Information Systems **11**(3-4): 245-270.

Berger, P. D. and N. N. Bechwati (2001). "The allocation of promotion budget to maximize customer equity." Omega **29**(1): 49-61.

Black, D. (2000). "What is electronic commerce." E-commerce Innovation Centre. University of Cardiff. UK. Mayo.

Blanzieri, E. and A. Bryl (2008). "A survey of learning-based techniques of email spam filtering." Artificial Intelligence Review **29**(1): 63-92.

Bocij, P. (2003). Business information systems : technology, development, and management for the e-business. Harlow, Financial Times/Prentice Hall.

Bose, R. (2002). "Customer relationship management: key components for IT success." Industrial Management & Data Systems **102**(2): 89-97.

Bromiley, P. and L. L. Cummings (1995). "Transactions costs in organizations with trust." Research on negotiation in organizations **5**: 219-250.

Chang, H. H. and S. W. Chen (2009). "Consumer perception of interface quality, security, and loyalty in electronic commerce." Information & Management **46**(7): 411-417.

Culnan, M. J. and R. J. Bies (2003). "Consumer privacy: Balancing economic and justice considerations." Journal of Social Issues **59**(2): 323-342.

Cyr, D. (2008). "Modeling Website Design across Cultures: Relationships to Trust, Satisfaction and E-loyalty." Journal of Management Information Systems **Vol. 24, 4:47-72, 2008.**

Egger, F. N. (2001). Affective design of e-commerce user interfaces: How to maximise perceived trustworthiness, Citeseer.

Eid, M. I. (2011). "Determinants of e-commerce customer satisfaction, trust, and loyalty in Saudi Arabia." Journal of Electronic Commerce Research **12**(1): 78-93.

Flavián, C., M. Guinalíu, et al. (2006). "The role played by perceived usability, satisfaction and consumer trust on website loyalty." Information & Management **43**(1): 1-14.

Hansen, E. and E. Jonsson (2013). "E-loyalty in fashion e-commerce: an investigation in how to create e-loyalty."

Harrison McKnight, D., V. Choudhury, et al. (2002). "The impact of initial consumer trust on intentions to transact with a web site: a trust building model." The Journal of Strategic Information Systems **11**(3-4): 297-323.

Kalakota, R. and A. B. Whinston (1996). Frontiers of electronic commerce, Addison Wesley Longman Publishing Co., Inc.

Kalakota, R. and A. B. Whinston (1997). Electronic commerce: a manager's guide, Addison-Wesley Professional.

Karakaya, F. and S. M. Stark (2013). "Online Trust: Strategies to build confidence from a business perspective." Journal of Advanced Management and Business Research **1**(1).

Karimov, F. P., M. Brengman, et al. (2011). "The effects of website design dimensions on intial trust: A synthesis of th empirical literature " Journal of Electronic Commerce Research **12**(4).

Katsikas, S., J. Lopez, et al. (2005). "Trust, privacy and security in e-business: Requirements and solutions." Advances in Informatics: 548-558.

Kim, D., D. Ferrin, et al. (2008). "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and

their antecedents." Decision Support Systems **44**(2): 544-564.

Kiran, K. and S. Diljit (2011). "Antecedents of customer loyalty: Does service quality suffice?" Malaysian Journal of Library & Information Science **16**(2): 95-113.

Kosiur, D. (1997). Understanding electronic commerce, Microsoft press.

Lanier, C. D. (2008). "Understanding Consumer Privacy: A Review for Future Directions." Academic Marketing Science Review **12 (2)**.

Ling, K. C., D. bin Daud, et al. (2011). "Perceived Risk, Perceived Technology, Online Trust for the Online Purchase Intention in Malaysia." International Journal of Business & Management **6**(6).

Lisa, H., C. Anne-Marie, et al. (2003). "Emerging ethical perspectives of e-commerce." Journal of Information, Communication and Ethics in Society **1**(1): 39-48.

Liu, C., J. T. Marchewka, et al. (2005). "Beyond concern--a privacy-trust-behavioral intention model of electronic commerce." Information & Management **42**(2): 289-304.

Liu, H., P. Luo, et al. (2008). "A scalable authentication model based on public keys." Journal of Network and Computer Applications **31**(4): 375-386.

Lu, L.-C., H.-H. Chang, et al. (2013). "Online shoppers' perceptions of e-retailers' ethics, cultural orientation, and loyalty: an exploratory study in Taiwan." Internet Research **23**(1): 47-68.

McKnight, D. H. and N. L. Chervany (2001). "What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology." International Journal of Electronic Commerce **6**(2): 35-59.

McQuivey, J., and Ham, C. (2000). "Why some young consumers don't shop online." Forrester Research brief.

Özkan, S., G. Bindusara, et al. (2010). "Facilitating the adoption of e-payment systems: theoretical constructs and empirical analysis." Journal of Enterprise Information Management **23**(3): 305-325.

Parent, W. A. (1983). "Privacy, morality, and the law." Philosophy & Public Affairs **12**(4): 269-288.

Pavlou, P. A. (2003). "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model." International Journal of Electronic Commerce **7**(3): 101-134.

Polasik, M. and T. P. Wisniewski (2009). "Empirical analysis of internet banking adoption in Poland." International Journal of Bank Marketing **27**(1): 32-52.

Reichheld, F. F. and P. Schefter (2000). "E-loyalty." Harvard business review **78**(4): 105-113.

Sari, D. P. and A. Rofiq (2013). "CUSTOMERS'INTENTION ON PURCHASING AIRLINES E-TICKET: THE ANALYSIS OF ONLINE TRUST AND TECHNOLOGY ACCEPTANCE MODEL IN GARUDA INDONESIA WEBCOMMERCE." Jurnal Ilmiah Mahasiswa FEB **1**(2).

Shah, M. H., R. Okeke, et al. (2013). "Issues of Privacy and Trust in E-Commerce: Exploring Customers' Perspective."

Shahibi, M. S. and S. K. W. Fakeh (2011). "Security Factor and Trust in E-Commerce Transactions." Australian Journal of Basic and Applied Sciences **5**(12): 2028-2033.

Sharda, R. (2000). "Electronic data interchange overview."

Shariffadeen, M., A. Hamzah, et al. (2001). "Women and the digital divide." Women in the New ICT Era: Challenges and Opportunities, Kuala Lumpur: UNDP.

Smith, A. D. (2004). E-security issues and policy development in an information-sharing and networked environment, Emerald Group Publishing Limited.

Stewart, K. J. (1999). Transference as a means of building trust in World Wide Web sites, Association for Information Systems.

Suh, B. and I. Han (2003). "The impact of customer trust and perception of security control on the acceptance of electronic commerce." International Journal of Electronic Commerce **7**(3): 135-161.

Ter Kah, L. (1999). "New laws on E-commerce: Singapore." Computer Law & Security Review **15**(1): 8-14.

Thomas, H. (2000). "E-commerce-Germany: E-commerce and law-some framementary thoughts for the future of internet regualtion from a german perspective " Computer Law & Security Review **16**(2): 113-117.

Trepper, C. (2000). ECommerce Strategies, Microsoft Press.

Turban, E., D. King, et al. (2004). Electronic Commerce 2004: A Managerial Perspective. Upper Saddle River, N.J. ; Harlow Boston, Mass; London, Pearson Prentice Hall**:** v.

Turner, C. W., M. Zavod, et al. (2001). Factors that affect the perception of security and privacy of e-commerce web sites, Citeseer.

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.

Wareham, J., J. G. Zheng, et al. (2005). "Critical themes in electronic commerce research: a meta-analysis." Journal of Information Technology **20**(1): 1-19.

Wilson, J. (2009). "Could There be a Right to Own Intellectual Property?" Law and Philosophy **28**(4): 393-427.

Xiong, L. and L. Liu (2003). "A reputation-based trust model for peer-to-peer ecommerce communities."

Zeithaml, V. A., L. L. Berry, et al. (1996). "The behavioral consequences of service quality." The Journal of Marketing: 31-46.

Zendehdel, M. and L. H. Paim (2012). "Perceived risk of security and privacy in online shopping: A study of Malaysia context." Life Science Journal **9**(4).

Zhang, H. and S. C. Okoroafo (2013). "An E-Commerce Key Success Factors Framework for Chinese SME Exporters." International Journal of Economics and Finance **6**(1): p129.

Zhang, H. and S. C. Okoroafo (2014). "An E-Commerce Key Success Factors Framework for Chinese SME Exporters." International Journal of Economics & Finance **6**(1).

Zhang, Y. and R. Wang (2014). "Comparison of E-payment of the B2C E-commerce in China from the Security and Trust Perspective."

Zhang, Y., X. Deng, et al. (2012). "Assessment of E-Commerce security using AHP and evidential reasoning." Expert Systems with Applications **39**(3): 3611-3623.

Zhou, M., M. Dresner, et al. (2008). "Online reputation systems: Design and strategic practices." Decision Support Systems **44**(4): 785-797.

Zwass, V. (1996). "Electronic commerce: structures and issues." International Journal of Electronic Commerce **1**(1): 3-23