Sys Rev Pharm 2020; 11(1):666-672
A multifaceted review journal in the field of pharmacy

An Analysis of Regulations and Legislations regarding Security in E-Commerce

[1]Sultan Al-masaeed*, [2]Johar MGM, [1]Anas Ratib ALSoud

[1]AL- Ahliyya Amman University, [2] Management and Science University
*Corresponding author: mdgapar@msu.edu.my

ABSTRACT

Electronic commerce or E-commerce uses the internet as its main medium of transaction, although there are other forms non-internet based transaction. The increase of business due to E-commerce is very encouraging and will be the mainstay of the global economy for many years to come. Nevertheless, the darker side of e-commerce exists. New breed of threats not seen in traditional form of commerce have come to existence. Nevertheless, it is always useful or vital for one to be armed with knowledge (especially with regards to the law) about safety and security issues in electronic commerce in order to ensure that doing business in the internet is a fruitful endeavor to ensure economic success

Keywords: legislation, cases, guidelines, regulations, e-commerce

Correspondence:
Sultan Al-masaeed
Management and Science University
Corresponding author: mdgapar@msu.edu.my

INTRODUCTION

The increase of business due to E-commerce is very encouraging and will be the mainstay of the global economy for many years to come. Nevertheless, the darker side of e-commerce exists. New breed of threats not seen in traditional form of commerce have come to existence. Also from the same report, business to business(B2B) e-commerce transaction, US statistics shows that B2B transactions account for USD995 billion or 93.3 percent of the US e-commerce in 2001. In the European Union, private sector estimates of B2B trade were USD 185 billion to 200 billion in the year 2002. Some projections have also shown that B2B trade was USD 4 billion in central and Eastern Europe. Growth is expected for the Asia Pacific region, from about USD 120 billion in 2002 to around USD 200 billion in 2003 and USD 300 billion in 2004 (Measuring the Information Technology, 2002). In Malaysia, the Multimedia Super Corridor(MSC) Impact Survey 2003, have shown that economic impact by the MSC has measured to the total sales of RM3.93 billion in 2002 and expected to increase to RM5.83 billion in 2003 and RM7.98 billion in 2004. Computer fraud refers to fraud committed using a computer. Hackers are unauthorized but talented people. A past study was the first to attempt to define the hacker's community. In the study, five categories were given to the hacker's community (Smedinghoff & Bro, 1998). They are:

- Novice- They are the least experienced and their activities are viewed as mischief.
- Student- They are explorers of other's information when they are bored with their work
- Tourist- They are hackers for the thrill of just being there.
- Crasher- They are intentional destructors of systems.
- Thief- They are the rarest and they profit from activities

The world in now interconnected by wires that carry data i.e. the Internet. By permitting computer networks to access the Internet, a door is now open to a huge number of people to launch attacks on privacy (Bygrave, 2000).

It is common in business practice that data mining is practiced. Websites are used to track customer activities and the information derived are used for future marketing purposes. Internet advertising companies follow users to create profiles on consumers by placing a small text file known as "cookie" on the users' computer. Cookies acts like a barcode, tracking the pages that were visited.

Millions of people use the Internet every day to innocently enjoy broad Internet access without realizing that the Internet contains most private information about them. They also do not track and supervise their acts once they are online. When shopping and doing business online, the privacy is vital to consumers. Businesses use data that are unknowingly collected from the user to directly solicit business and this is annoying and intrusive to one's privacy. Organizations that obtain this information are suffering from threats by internal and external users who only seek personal benefits. These attacks can disable a system infrastructure or remove confidential information such as credit card numbers in order to commit additional criminal offences (Braga, 2005).

Another issue relevant to internet privacy is spam. Spam or unsolicited bulk email messaging is relatively small because of the spammer's cost of delivering the messages. Analysis has shown that 80% of emails sent worldwide are spam, and the time workers spend deleting unwanted emails costs companies about $22 billion annually. The same article reported that research has also shown that 75 percent of Internet users receive spam on a daily basis and the average number of spam received on a daily basis is 18.5 and the average daily time spent on deleting them is 2.8 minutes, costing $21.6 billion in productivity loss per year. See Figure 1.

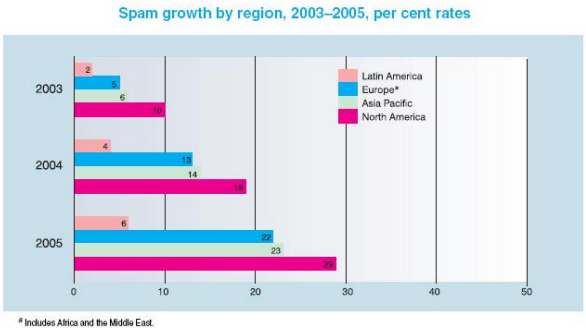

Figure 1: Spam growth by region

When e-business is part of the majority of people's everyday life, which appears to be risk-adverse, protection is crucial. Internet security issues take several forms: spam, malware, site squatting, abuse, denial of service, unauthorized intrusion into corporate or personal computers and networks (and misuse or exploitation of the information stored therein), infringements of privacy, bribery and harassment. United States tops the chart in digital attacks in 2002. The need for taking action is more acute in United States is partly the result of the September 11 attack and the concerns of 'cyber terrorism'. In the global world and advancement of technologies, the growth of telecom sector, the demand of internet speed and the speed and accuracy of application is grown. This research investigates and reports on the adaptation of telecommunication technology by ICT companies in Malaysia. The principal objectives of this research are, to measure the status of telecommunication services in Malaysia and identify the criterion that contributes to it, to identify drivers and barriers influencing the needs for telecommunication services in corresponding to the use of business applications and services, to evaluate whether features or technologies is the crucial criteria that lead to the adaptation of telecommunication services by ICT companies in Malaysia, to determine whether is there any significant relationship between level of familiarity and the level of acceptance towards VoIP service by ICT companies in Malaysia. This research aims to provide an answer and principles of practices by ICT companies in Malaysia towards adaptation of telecommunication technologies. In the growing world, telecommunication is also growth with some rapidness while evolving some strategies of new business which leads to the conditions of market changing, where some companies are also moving for the better parts. In the development of industry of telecommunication, some parts have been effected which contains telemedicine and interactive television while the other parts have been grown which contains mobile commerce, e government, e learning and e commerce. In the change of strategies of business, some challenges are also being faced with the global challenging environment. Many technologies can be adopted but certain ways have made it complex, while the wide range of opportunities and choices are provided by the companies of telecommunication to enable the competitive environment. Most of the companies' main focus now a days is to control their cost and many other procedures that are placing some constraints in the achievement of competitive advantage over the other companies in the global world. Over many decades, the companies are providing services and are competitors to each other with the advancement of technologies. Certain laws are made by the industries to overcome the threats that prevail in damaging companies repute and damaging the sense of customers, the Act of Telecommunication has restricted many international and local exchanges in prohibition of qualified or unqualified activities that disrupts the enhancement of such telecom facilities. Another way of promoting services of telecommunication is a media way, while the promotion via use of telecommunication services have far better enhanced the performance and efficiency of such networks which enabled not only better performances of organizations but also resulted in the margins of organizations with certain advancements. The system of telegraphy was an invention of Samuel in the United States in 1844, while the Morse code is particularly is an enhancement of the electric telegraph and an easy way for the letter representation while using alphabets for the pulses of shorts and long. There is diversion of pulses via which signals are transmitted and reverted back with same procedures, while the operating machines are important in such operations. The basic system consisted of a complete electrical circuit with a key at the transmitting end and an electromagnet connected to a device for making marks on paper at the receiving end. Not only could the IT Protection and Crime Prevention Approaches be used to deter crime in businesses, but it could also be used to secure private computer systems. It also provides an introduction to what an investigator needs to know about security measures in the field of information technology (IT) in order to conduct investigations in an IT environment and provide advice on methods of crime prevention. This commonality raises the possibility of integrating the functionality of the three elements - the transmission media, the program control and the intelligence. The sad truth is that the public Internet has barely been able to keep up with the ever-increasing demand for bandwidth. More and more sites, for example, are incorporating streaming audio and video and other bandwidth¬ hungry applications.

LITERATURE REVIEW

The European Parliament has issued a directive on 8 June 2000 to all member states on legal aspects of electronic commerce. On 1996, the UN Committee on International Trade Law drew up a model law on electronic commerce (Aljifri, Pons, & Collins, 2003). OECD recommends that these nine principles are used when developing, providing, managing, and servicing information systems and networks. The guidelines provide an avenue for self-regulation. ASEAN published its own E-Commerce legal framework in response of the increasing use of E-business in South East Asia. And European e-commerce and electronic signature laws. The 1998 Communications and Multimedia Act (CMA) came into force in the Malaysian context on 1 April 1999. This legislation provides the policy and regulatory framework for the telecommunications, radio and computer industries to converge. CMA Section 211 seeks to regulate controlling content that is obscene, indecent, and false and contains threats and harassment. Since self-regulation is a pinnacle of this Act, a forum of content will be established to draw up a code of practice. Section 212 of the CMA provides for the creation of the content forum in order to formulate the content code. The Content Code is in the formulation process now. The Code of Content should cover all content on electronic networks, including radio, television and internet services. The Broadcasting Guidelines and the Advertising Code prepared by the

Ministry of Information will continue to be enforced while the content code is being developed.

Malaysia's Communication and Multimedia Content Forum (CMCF) was established in February 2001 as a society represented by all relevant parties, including the communications and multimedia sector's "supply and demand" side-to govern content and address content-related issues disseminated via electronic networked media (CMCF, 2005). The Malaysian Communications and Multimedia Commission (MCMC) appointed CMCF on 29 March 2001 to promote the creation of the content code (Palmer, Robinson, Patilla, & Moser, 2001). MCMC a Communications and Multimedia Act (CMA) came into force on 1 November 2001 in the Malaysian context on 1 April 1999. This law establishes the telecommunications, media and computer industries' policy and regulatory structure for convergence (KTAK, 2005). Section 212 of the CMA provides for the creation of a Content Forum to formulate the content code (Communications and Multimedia Act 1998). The Content Code is in the formulation process now. The Code of Content should cover all content on electronic networks, including radio, television and internet services. The Broadcasting Guidelines and the Advertising Code prepared by the Ministry of Information will continue to be enforced while the content code is being developed.

Malaysia's Communication and Multimedia Content Forum (CMCF) was founded in February 2001 as a society represented by all relevant parties, including the communications and multimedia industry's "supply and demand" side-regulating content and addressing content-related issues disseminated via electronic networked media (CMCF, 2005). The Malaysian Communications and Multimedia Commission (MCMC) appointed CMCF on 29 March 2001 to facilitate the development of the software code (Yenisey, Ozok, & Salvendy, 2005).

The Council of Europe's Convention on Cybercrime on 2001 in Budapest has resolved to adopt the following resolutions with regards to computer crime:

At the national level:

- On unauthorized access- Each party shall adopt domestic laws which make intentional access to the computer system as a criminal offense without right in whole or in part. The crime may be committed by violating security controls, in order to acquire computer data or other deliberate dishonesty, or in relation to a computer system linked to another computer system (Mayayise & Osunmakinde, 2014).
- On system intervention- Every party shall adopt domestic laws which deliberately impede the functioning of the computer system without right by inputting, transmitting, destroying, removing, degrading, altering or suppressing computer data as a criminal offence (Furnell & Karweni, 1999).

This also includes a set of forces and procedures such as scanning and intercepting computer networks. The key goal is to implement a shared criminal strategy aimed at protecting society against cybercrime, in particular through the implementation of effective legislation and the promotion of international cooperation. In 2003, Interpol published a systematic framework for computer crime prevention. Not only could the IT Protection and Crime Prevention Approaches be used to deter crime in businesses, but it could also be used to secure private computer systems. It also provides an introduction to what an investigator needs to know about security measures in the field of information technology (IT) in order to conduct investigations in an IT environment and provide advice on methods of crime prevention (Duh, Sunder, & Jamal, 2002).

Interpol also suggested that different steps be taken to secure the data stored on a computer system: individual users should only be able to read the information required to do their job; they should only be able to alter information that is actually their task to alter. Finally, some information should not be accessible to individual users at all, e.g. the different log records (AlGhamdi, Drew, & Al-Ghaith, 2011b).

Certain calls were made for testing the technology through the system of clock, while the path of calling system was entirely arranged in the time period and then towards the other calls. This is also name as system of "synchronous" due the procedure of accurate clocks followed in clocks of standard time. It is stated that users are attached with bandwidth which users usually say, while when the idle user become there is no usage of bandwidth. The retrospective bandwidth is when allocated the number of calls goes on irrespective of being amount of calls. In the portion of Telecom Company, the providers of services of telephone internet and telephony of IP are growing portion of it, while the other providers are consisted to alternatives and mainstreams. There is difference in the certain companies that provide services of internet telecoms via which traffic calls are made. In the growing world, telecommunication is also growth with some rapidness while evolving some strategies of new business which leads to the conditions of market changing, where some companies are also moving for the better parts. In the development of industry of telecommunication, some parts have been effected which contains telemedicine and interactive television while the other parts have been grown which contains mobile commerce, e government, e learning and e commerce. In the change of strategies of business, some challenges are also being faced with the global challenging environment. Many technologies can be adopted but certain ways have made it complex, while the wide range of opportunities and choices are provided by the companies of telecommunication to enable the competitive environment. The important element of providing service is a way of telegram commercially, while the services via roads and other modes of providing is quite riskier but the improvement in telecommunication has overcome the issue that prevails in the risk factors of providing services of telecommunication. Certain ways, via which communication was confirmed, while the receiving of request through arranged bell which through the transmitter was connected called in the history of company of telephone in considered as the largest company of telephone in the world. The links of telephones were first installed in large private buildings and used for communication between the occupants. It is observed that STM faced a dimension of achieving higher profits between the intent commercially, while taking the responsibility of providing services of telegraph and telephone in all of the country.

While speaking operationally, it is observed that rural areas were neglected by the STM in Malaysia. In following such phase, Malaysia then strived hard to achieve the flaws that prevailed in such factors while performing reforms to the further stages. The main aim was to maintain at operation in the independence of financial sector while privatizing the process to perform more effectively in the atmosphere of competitiveness.

There is facilitation of new technologies in the transfer of plenty of networks which are being under facilitation and

being done. In the early stages, the ways of communication were different, while the invention of new technologies have made it easier and a convenient way of providing the same services that were provided in old days Thus, the current study has examined the e-commerce impact on the legislation and regulation of the country and try to find of information technology role on the legislation and regulation.

METHODS

The research was carried via review of related literature. Primary data will consist of statutes, enactments, directives, legislation, cases and regulations issued, written or recorded by legislators or related parties. Secondary data consists of related journals, articles and analysis written by authors, researchers and analyzers (Gefen, 2000).

ANALYSIS

In the following tables, Interpol has listed the various threats to which a system may be exposed. They are grouped according to where the information is located in the IT process.

Table 1: Architecture Independent Threats and their prevention methods

Threat	Prevention method
Disloyal staff	Often the best type of security is procedural security with knowledge and accountability of the attendant personnel.
Unauthorized access to information by users	Users should have specific written guidance on what they should and should not be doing. Guidelines for which to sign. Install a program called 'Identification and Authorization.' Take on a 'two-man rule' to grant privileges. Do not disclose to anyone your password too. Hold secure identity and authorization cards. Check logs periodically. Verify that configuration is correct regularly. Deploy a Detection System for Intrusion.
Unauthorized system managers, programmers, etc. access to information;	Like above, and: Using different frameworks to create programs and to 'produce.' Limit access to sensitive information equipment; adopt 'two-man rule.' Restricted use of the privileges 'power user'/'root.'
Unauthorized access to information by temporary staff, e.g. consultants, service engineers etc.	As for the other personnel, and: Limit their access to the system to the required time and day for the particular task. Do not forget to revoke your rights of access and lock your temporary accounts. Do not leave Remote Service communication lines open when not needed.

Unauthorized access from external sources

Threat	Prevention method
Unauthorized access	Install a program called 'Identification and Authorization.' Take on a 'two-man rule' to grant privileges. Check logs periodically. Verify that configuration is correct regularly. Firewall update.

Media handling

Threat	Prevention method
Total loss of information through theft of media	Media should be kept in a safe place under lock and key.

Loss of information (by copying or transferring) as a result of unauthorized access to or loaning of media	Sensitive information is encrypted. Press processing staff will not have access to the encryption keys. 'Two-man rule' means backup. 'Two-man rule "for archive access.
Loss of information during servicing	Always submit equipment for operation that includes confidential information about mounted media. (Due to 'Undelete/unease' possibilities 'Delete' confidential information is not sufficient)

Malicious program code

Threat	**Prevention method**
Viruses and other malicious programs	Enable the free 'anti-virus.' See chapter 'Investigations' in the Interpol Computer Crime Manual, section 'Malicious program code.'
Changed programs to access information, or manipulate it, without authorization	Depends upon the architecture of the machine. Using different frameworks to create programs and to 'produce.' Limit access to 'source code,' 'compilers' and 'editors' in 'production' system where possible, and restrict the use or installation of non-standard software packages. Such a problem may be observed by an intrusion detection system.

Electronic Emission

Threat	**Prevention method**
Given all the safeguards, a persistent attacker can still eavesdrop information by capturing and analyzing electromagnetic emissions from the Personal Computer or Workstation. In a way very similar to the way a TV receiver operation can be identified and calculated which channel is being watched. Such sort of eavesdropping is more likely to occur when extremely confidential information is involved, such as high-value commercial information or dealing with national security matters.	Use no or restricted signal leakage ('tempest') equipment or position the equipment in a shielded space. Though successful, these approaches are costly and should be recommended only when the risk is extremely high. To avoid pollution leakage from the lines running between peripherals and the Local Area Network (LAN), optical fibers may be used. Broad Area Network (WAN) encryption does not stop electromagnetic emissions but without the encryption key the eavesdropper won't be able to use the information.

Table 2: Threats on Network architectures and minicomputer systems and Prevention Methods

Threat	**Prevention method**
Manipulation or unauthorized access to applications or information in the network at each workstation (PC)	See Table 2: Threats to microcomputer systems (stand-alone, personal computers) i.e. threats to confidential information stored on PC systems and methods of prevention
Unauthorized access to information in the 'server' by users	Users should have specific written guidelines about what they are permitted to do and not allowed to do. Guidelines for that should be signed. Install a system of 'Identification and Authorization.' Put in a 'two-man law' to award privileges. Checks reports periodically. Regularly check that configuration is correct. IDS should be installed.

Unauthorized access to information by system administrators, programmers' etc.	Like above, and: Using different frameworks to create programs and to 'produce.' Limiting server access; following 'two-man law' Restricted use of the privileges 'power user'/'root.'
File corruption (program, or data). The introduction of viruses into computer systems is a major cause of data loss and corruption.	Both media should be screened for viruses prior to use, preferably on a device designed specifically for the purpose. Erase all unnecessary codes, default procedures and unused ones.
Maximum knowledge loss via 'disk crash' or deliberate file destruction	Standard data and device file backups are essential. They must include a detailed collection of security information along with the logging information.
Loss of information during servicing	Many mini-server maintenance can be performed 'on-site' but the service company/vendor would have to withdraw the equipment for repair in case of any hardware issues. Never send media sensitive equipment for servicing without a verifiable guarantee that the information will be destroyed. (Because of 'undelete' and 'unformed' possibilities, it is not enough to 'delete' the confidential information) Note that the disk drives may be reused somewhere else after repair and can compromise your details. If a disk with classified information is planned to remove it, kill it yourself.
Theft of the server	The server should be kept locked up in a safe place.

In the United States, the 1996 National Information Infrastructure Security (NIIP) Act was passed to legislate computer crime-related issues. The act was an amendment to the 1986 Computer Fraud and Abuse Act. The amended NIIP Act 1996 or USC 18 1030 includes the following (18 USC 1030):

- • The actions of a person who intentionally breaks into a computer without authorization or an insider who exceeds permitted access and thereby obtains confidential information and either discloses the information to another person or maintains it without disclosure to the appropriate authorities. Documentation is provided as to whether or not the person used a computer intentionally for the purpose of accessing confidential information without authority, or beyond authority. It is computer use that is focused on and not the unauthorized possession, access, or control of the classified information itself. Lawmakers have made it clear 'receiving information'
- The information includes information found in a financial record of a financial institution or issuer of a card, information from any US department or agency or information from any secure device engaged in interstate or international communication (Blythe, 2005).
- • The actions of a person who deliberately breaks into a computer without authorization or an intruder who exceeds permitted access with the purpose of committing certain crimes and defrauding (AlGhamdi, Nguyen, Nguyen, & Drew, 2012).
- • Conduct of a person who, while transmitting a program, code, information or order that causes harm, without authorization. Whether or not the injury is reckless the person is committing an offence.
- • A person's conduct through unauthorized access steals passwords or information and transmits it to foreign hands with the intent of defrauding it. One can imagine a situation where hackers penetrate a system, encrypt a database, and then demand the decoding key for money. This new provision would ensure that modern-day blackmailers who threaten to harm or shut down computer networks are prosecuted unless their demands for extortion are met. This act also covers the transmission of threats via any form of communication with the intention of extorting a protected computer to cause damage (Taddesse & Kidan, 2005).

DISCUSSIONS AND CONCLUSIONS

Thus, the current study has examined the e-commerce impact on the legislation and regulation of the country and try to find of information technology role on the legislation and regulation and concluded that the information technology and e-commerce have positive nexus with legislation and regulation of the county. The world's economies are driven in varying degrees by developments in IT with the robust growth of the e-commerce environment. The cyber marketplace's future will depend to a large degree on safety and security. Developing electronic commerce and facilitating international trade using electronic business has required

the creation of legal and regulatory framework. Safety and security or electronic commerce could not be left to legislative introduction, and the introduction of laws is not proactive to change. Legislation is sometimes created after a problem has arisen. Self-regulation means that businesses participating in the online industry actively agree to comply with certain codes of conduct when communicating with others electronically. It may take various forms such as implementing a code of conduct, engaging in a national or international scheme. For example, the Association for Data Processing Management (DPMA) has established a code of conduct for its members. The DPMA code of ethics and standards is as follows: industry leaders felt that the principle of self-control and performance should not be legislated but rounded up with ethics. Studies have shown that ethical behavior is more prevalent in companies that take a strong ethical stand and impose ethical behavior on employees. Through ethics, it is hoped that morals will have a positive impact (Shalhoub, 2006). Thus study has some limitation that is does not use any mediation and moderation analysis and suggested that future studies should undertake this aspect in their studies. In addition, this study also ignore the cross country analysis and recommended that future studies should add more countries under investigation. Finally, the current study has taken only limited predictor such as case studies, regulation and legislations and suggested that future studies should add more predictors in their evaluations.

REFERENCES

1. R. AlGhamdi, Drew, S., and Al-Ghaith, W., Factors Influencing e-commerce Adoption by Retailers in Saudi Arabia: a qualitative analysis. The Electronic Journal of Information Systems in Developing Countries, Vol 47, 1, pp. 1-23, 2011
2. R. AlGhamdi, et al., Factors influencing e-commerce adoption by retailers in Saudi Arabia: A quantitative analysis. " International Journal of Electronic Commerce Studies", Vol 3, 1, pp. 83-100, 2012
3. H. A. Aljifri, Pons, A., and Collins, D. J. I. M., Global e-commerce: a framework for understanding and overcoming the trust barrier. Information Management Computer Security, Vol 26, 3, pp. 222-228, 2003
4. A. H. Barkatullah, Does self-regulation provide legal protection and security to e-commerce consumers? Electronic Commerce Research Applications, Vol 30, 4, pp. 94-101, 2018
5. S. E. Blythe, Digital signature law of the United Nations, European Union, United Kingdom and United States: Promotion of growth in E-commerce with enhanced security. Richmond Journal of Law Technology, Vol 11, 2, pp. 6, 2005
6. C. A. P. Braga, E-commerce regulation: New game, new rules? The Quarterly Review of Economics Finance, Vol 45, 2-3, pp. 541-558, 2005
7. L. A. Bygrave, European Data Protection: Determining Applicable Law Pursuant to European Data Protection Legislation. Computer Law Security Review, Vol 16, 4, pp. 252-257, 2000
8. R.-R. Duh, Sunder, S., and Jamal, K. J. T. A. R., Control and assurance in e-commerce: Privacy, integrity, and security at eBay. Taiwan Accounting Review, Vol 3, 5, pp. 1-27, 2002
9. S. M. Furnell and Karweni, T., Security implications of electronic commerce: a survey of consumers and businesses. Internet research, Vol 45, 4, pp. 22-30, 1999
10. D. Gefen, E-commerce: the role of familiarity and trust. Omega, Vol 28, 6, pp. 725-737, 2000
11. T. Mayayise and Osunmakinde, I. O., E-commerce assurance models and trustworthiness issues: an empirical study. Information Management Computer Security, Vol pp. 2014
12. M. E. Palmer, et al., Information security policy framework: best practices for security policy in the e-commerce age. Information Systems Security, Vol 10, 2, pp. 1-15, 2001
13. Z. K. Shalhoub, Trust, privacy, and security in electronic business: the case of the GCC countries. Information Management Computer Security, Vol 54, 3, pp. 34-56, 2006
14. T. J. Smedinghoff and Bro, R. H., Moving with change: Electronic signature legislation as a vehicle for advancing e-commerce. J. Marshall J. Computer Info. L., Vol 17, 5, pp. 723, 1998
15. W. Taddesse and Kidan, T. G., e-Payment: Challenges and opportunities in Ethiopia. United Nations Economic Commission for Africa, Vol 45, 3, pp. 23-54, 2005
16. M. M. Yenisey, Ozok, A. A., and Salvendy, G., Perceived security determinants in e-commerce among Turkish university students. Behaviour Information Technology, Vol 24, 4, pp. 259-274, 2005