International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 7, 2020
ISSN: 1475-7192

THE ROLE OF CASES, REGULATIONS, POLICIES, GUIDELINES AND LEGISLATIONS ON THE E-COMMERCE SECURITY

[1]Omar Abdel Jaber, Johar, MGM, Sultan Al-masaeed

Abstract---*As e-business becomes part of an everyday experience of the majority of people who tends to be risk-adverse, security become crucially important(E-Commerce & Development Report, 2003). Internet security problems take multiple forms: spam, viruses, web squatting, fraud, copyright violation, denial of service, unauthorized entry into corporate or personal computers and networks(and theft or manipulation of the information stored in them), privacy infringements, fraud and harassment. The following issues will be examined with reference to the purpose of this study: E-commerce policies, Computer crimes, Electronic Privacy and Authentication & Encryption. It is proposed that these three(3) principles are examined in order to tackle security and safety in e-commerce. These principles are derived from the review of all the legislations, cases, guidelines, policies and regulations in this paper. All these principles are complementary to each other. Self-regulation, Ethics, Enforcement. Security and safety will remain the most vital issues in electronic commerce that will continue to be discussed, examined and addressed. Actions will be continue to be taken by the society to create new laws, technology, methods and processes to increase security and safety in the cyberspace as e-commerce technologies grow. One must not be deterred from electronic commerce just because of these issues. There will always be a downside for everything including electronic commerce. Business growth from this new method of doing business is very lucrative to be abandoned (AlGhamdi, Drew, & Al-Ghaith, 2011a; De Silva et al., 2018a; De Silva et al., 2018b; Nikhashemi et al., 2013).*

Keywords---*Policies, E-commerce, Legislation, Cases, Guidelines, Regulations*

I. Introduction

Doing business in the 21st century is distinctively different than of the previous century. With the rapid growth of the internet and the burgeoning use of information and communications technologies(ICT), commerce have changed in terms of its medium of trade and exchange. Commerce is now done electronically and it forms a major part of the ICT based economy. Electronic commerce or E-commerce uses the internet as its main medium of transaction, although there are other forms non-internet based transaction. Report has shown that the number of internet users in the world reached 591 million in 2002(E-Commerce & Development Report, 2003). The report by United Nations Conference on Trade and Development(UNCTAD) secretariat has also shown that the estimates of total online sales for 2002 were USD 43.47 billion for the United States, USD 28.29 billion for the European Union, USD 15 billion for Asia Pacific region, USD 2.3 billion for Latin America and USD 4 million for Africa (AlGhamdi, Drew, & Al-Ghaith, 2011b; Dewi et al., 2019; Pambreni et al., 2019; Tarofder et al., 2017).

1, 3 AL- Ahliyya Amman University, 2 Management and Science University
mdgapar@msu.edu.my

In 2004, Computer Security Institute and FBI surveyed 494 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities. The findings of the survey are shown as the following:

- Unauthorized use of computer systems is on the decline, as is the reported dollar amount of annual financial losses resulting from security breaches.
- In a shift from previous years, both virus attacks and denial of service outpaced the former top cost, theft of proprietary information. Virus costs jumped to $55 million.
- The percentage of organizations reporting computer intrusions to law enforcement over the last year is on the decline. The key reason cited for not reporting intrusions to law enforcement is the concern for negative publicity.
- Most organizations conduct some form of economic evaluation of their security expenditures, with 55 percent using Return on Investment (ROI), 28 percent using Internal Rate of Return (IRR), and 25 percent using Net Present Value (NPV).
- Over 80 percent of the organizations conduct security audits.
- The majority of organizations do not outsource computer security activities. Among those organizations that do outsource some computer security activities, the percentage of security activities outsourced is quite low (AlGhamdi, Nguyen, Nguyen, & Drew, 2012; Doa et al., 2019; Maghfuriyah et al., 2019; Nguyen et al., 2019).
- The Sarbanes-Oxley Act is beginning to have an impact on information security in some industries. (The Sarbanes-Oxley Act is an act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws(H.R. 3763). The law is aimed at improving corporate governance after the Enron crisis. Stiffer penalties are provided for fraud and white collar crime. Maximum penalty for mail and wire fraud increased from 5 to 10 years).
- The vast majority of the organizations view security awareness training as important, although (on average) respondents from all sectors do not believe their organization invests enough in this area (Aljifri, Pons, & Collins, 2003; Pathiratne et al., 2018; Rachmawati et al., 2019; Seneviratne et al., 2019; Sudari et al., 2019; Tarofder et al., 2019).

The survey further reported that because of computer security incidents, estimated losses for 2004 was USD141.5 million with security incidents due to viruses amount to USD55 million. See **Figure 1**.

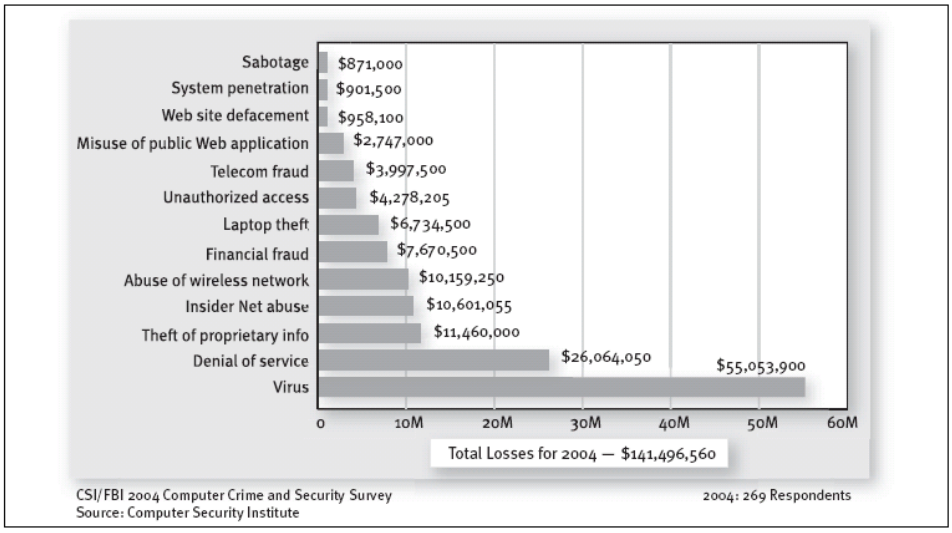

Figure 1: Estimated Losses due to security incidents by type

The E-commerce & Development Report has also reported that IT security sales is expanding and are expected to reach USD 45 billion by 2006 compared to USD 17 billion in 2001 showing that the importance of IT security in the ICT-based economy. Nevertheless, does the investment in IT security products enough to protect the security of E-commerce. While technology helps to reduce risk, in the end, it is the essential function of governments to maintain peace and security and the rule of law in the Internet and e-commerce as a whole.

The purpose of this study is to review available legislation, cases, guidelines, policies and regulations formed by governments and related bodies to maintain security in e-commerce. In order to define the purpose of this study in a more concise and focused manner, some key issues relating to security in E-commerce must be ascertained. These issues will not be well determined unless some key terms relating security, e-commerce and the internet technology are not defined.

The related key terms and their definitions are as follow:

Security is something that secures and offers protection. They aremeasures taken to guard against espionage or sabotage, crime, attack, or escape(Merriam-Webster Online).

Electronic Commerce(or E-commerce) refers to maintaining business relationships and selling information, services, and commodities by means of computer telecommunications networks.**E-commerce** usually refers only to the trading of goods and services over the Internet, broader economic activity is included. **E-Commerce** consists of business-to-consumer and business-to-business conducted by way of the **Internet** or other electronic networks. **Internet** is a system architecture that has revolutionized communications and methods of commerce by allowing various computer networks around the world to interconnect and sometimes referred to as a "network of networks"(Encyclopedia Britannica Online) (Barkatullah, 2018).

Cybercrime also known as computer crime is defined as any use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. **Cybercrime**, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. The international nature of **cybercrimes** has led to international **cyber laws**. **Cyber laws**is a body of law bearing on the world of computer networks, especially the Internet. As traffic on the Internet has increased, so have the number and kind of legal issues surrounding the technology. Hotly debated issues include the obscenity of some on-line sites, **the right of privacy**, freedom of speech, regulation of electronic commerce, and **the applicability of copyright laws**. **Crime** is the intentional commission of an act usually deemed socially harmful or dangerous and specifically defined, prohibited, and punishable under criminal law. **Crimes** in the common-law tradition were originally defined primarily by judicial decision. Most common-law crimes are now codified. According to a generally accepted principle, nulliuscrime sine leg, there can be no crime without a law.

Right of **privacy** is the right of a person to be free from intrusion into matters of a personal nature. The E-mail has spawned one of the most significant forms of cybercrime—spam, or unsolicited advertisements for products and services, which experts estimate to comprise roughly 50 percent of the e-mail circulating on the Internet. Spam is a crime against all users of the Internet(Encyclopedia Britannica Online).

Encryption is a process of disguising information as "cipher text," or data that will be unintelligible to an unauthorized person. Decryption is the process of converting cipher text back into its original format, sometimes called plaintext. Computers encrypt data by applying an algorithm to a block of data. A personal key known only to the message's transmitter and intended receiver is used to control the encryption. Well-designed keys are almost impregnable. A key 16 characters long selected at random from 256 ASCII characters could take far longer than the 15-

billion-year age of the universe to decode, assuming the perpetrator attempted 100 million different key combinations per second. Symmetric encryption requires the same key for both encryption and decryption. Asymmetric encryption, or public-key cryptography, requires a pair of keys, one for encryption and one for decryption. **Cryptography** is a practice of the enciphering and deciphering of messages in secret code in order to render them unintelligible to all but the intended receiver(Encyclopedia Britannica Online) (Blythe, 2005; Nikhashemi et al., 2017; Tarofder et al., 2019; Ulfah et al., 2019; Tarofder et al., 2016; Udriyah et al., 2019).

Based on the definitions of the key terms above, the following issues were identified and will be examined with reference to the purpose of this study:

- **E-commerce policies**. The study of general policies with respect to the purpose of this study is vital as policies are high-level overall plan embracing the general goals and acceptable procedures especially of a governmental body. It also gives an idea the overall objectives of E-commerce implementation of a government at a macro level.
- **Computer crimes.** Also known as cybercrimes is the main theme of the study of Security in E-Commerce. A new form of cybercrime is cybersquatting.
- **Electronic Privacy.** Privacy is the most important challenge in security in E-commerce. In order for new business models on the Internet to succeed, the right of privacy must be maintained as users do not want their personal information to be shared openly, their identity to be stolen or their private lives are intruded.
- **Authentication & Encryption.** The security of information can be increased by the use of encryption and cryptography technologies. Every E-commerce practitioner must be knowledgeable of laws pertaining to these technologies and also their rights when a contract is done electronically on the internet. Key points to note will be whether the offer and acceptance methods in an e-contract are the same as of contracts done in real life (Braga, 2005).

Areview of legislations, cases, guidelines, policies and regulations formed by governments and related bodies to maintain security in e-commerce will be carried out according to these issues.

II. Literature Review

The decision by UNCITRAL to formulate model legislation on electronic commerce was taken in response to the fact that in a number of countries the existing legislation governing communication and storage of information is inadequate or outdated because it does not contemplate the use of electronic commerce. Existing legislation imposes or implies restrictions on the use of modern means of communication, for example by prescribing the use of written, signed or original documents. While a few countries have adopted specific provisions to deal with certain aspects of electronic commerce, there exists no legislation dealing with electronic commerce as a whole. This may result in uncertainty as to the legal nature and validity of information presented in a form other than a traditional paper document. The Model Law may also help to remedy disadvantages that stem from the fact that inadequate legislation at the national level creates obstacles to international trade, a significant amount of which is linked to the use of modern communication techniques. At an international level, the Model Law may be useful in certain cases as a tool for interpreting existing international conventions and other international instruments that create legal obstacles to the use of electronic commerce, for example by prescribing that certain documents or contractual clauses be made in written form.

The objectives of the Model Law, which include enabling or facilitating the use of electronic commerce and providing equal treatment to users of paper-based documentation and to users of computer-based information, are essential for fostering economy and efficiency in international trade. By incorporating the procedures prescribed in the Model Law in its national

legislation for those situations where parties opt to use electronic means of communication, an enacting State would create a media-neutral environment.

The Model law covers the following:

- **Legal recognition of data messages**. Information in the form of data message is valid and enforceable.
- **Writing.** Where if there is a law requiring that information is in writing, data messages of that information will be usable.
- **Signature.** Where if the signature is required by the law, the data message must be accompanied with a method to identify the person.
- **Original.** Where if the law requires the information to be in its original form, the data message must be accompanied with a reliable assurance that as to the integrity of the information and the information must be able to be displayed to the person to whom it is to be presented (Bygrave, 2000).
- **Evidential weight**. Data messages will be given evidential weight where reliability is assured.
- **Retention of Data Messages**. Where if the law requires information to be retained, this requirement is met by retaining data messages.

In October 1997, during the Clinton's Administration, the President's Commission issued its report, calling for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures, such as telecommunications, banking and finance, energy, transportation, and essential government services. The Presidential Decision Directive 63(PDD 63) is an interagency effort to evaluate recommendations and produce workable and innovative framework for critical infrastructure protection. The President's policy:

- Sets a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003, and significantly increased security for government systems by the year 2000, by:
    - Immediately establishing a national center to warn of and respond to attacks.
    - Building the capability to protect critical infrastructures from intentional acts by 2003.
- Addresses the cyber and physical infrastructure vulnerabilities of the Federal government by requiring each department and agency to work to reduce its exposure to new threats;
- Requires the Federal government to serve as a model to the rest of the country for how infrastructure protection is to be attained;
- Seeks the voluntary participation of private industry to meet common goals for protecting our critical systems through public-private partnerships;
- Protects privacy rights and seeks to utilize market forces. It is meant to strengthen and protect the nation's economic power, not to stifle it.
- Seeks full participation and input from the Congress.

PDD-63 sets up a new structure to deal with this important challenge:

- a **National Coordinator** whose scope will include not only critical infrastructure but also foreign terrorism and threats of domestic mass destruction (including biological weapons) because attacks on the US may not come labeled in neat jurisdictional boxes;
- The **National Infrastructure Protection Center** (NIPC) at the FBI which will fuse representatives from FBI, DOD, USSS, Energy, Transportation, the Intelligence Community, and the private sector in an unprecedented attempt at information sharing among agencies in collaboration with the private sector. The NIPC will also provide

the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts;

- An **Information Sharing and Analysis Center** (ISAC) is encouraged to be set up by the private sector, in cooperation with the federal government;
- A **National Infrastructure Assurance Council** drawn from private sector leaders and state/local officials to provide guidance to the policy formulation of a National Plan;
- The **Critical Infrastructure Assurance Office** will provide support to the National Coordinator's work with government agencies and the private sector in developing a national plan. The office will also help coordinate a national education and awareness program, and legislative and public affairs (Duh, Sunder, & Jamal, 2002).

Acknowledging that information systems and networks will be always changing, the Organization for Economic Co-operation and Development(OECD) published the Guidelines for the Security of Information Systems and Networks in 2002(OECD, 2002). The guidelines are introduced with the main goal of promoting a culture of security among its participants namely governments, businesses, other organizations and individual users who develop, own, provide, manage service and use information systems and networks. The aims of these guidelines are to:

- Promote a culture of security among all participants as a means of protecting information systems and networks.
- Raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation.
- Foster greater confidence among all participants in information systems and networks and the way in which they are provided and used.
- Create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices,
- Measures and procedures for the security of information systems and networks.
- Promote co-operation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures.
- Promote the consideration of security as an important objective among all participants involved in the development or implementation of standards.

The guidelines also outline nine principles. They are complementary to each other and as follow:

1. **Awareness** - Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.
2. **Responsibility** - All participants are responsible for the security of information systems and networks.
3. **Response** - Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.
4. **Ethics** - Participants should respect the legitimate interests of others.
5. **Democracy** - The security of information systems and networks should be compatible with essential values of a democratic society (Furnell & Karweni, 1999).
6. **Risk assessment** - Participants should conduct risk assessments.
7. **Security design and implementation** - Participants should incorporate security as an essential element of information systems and networks.
8. **Security management** - Participants should adopt a comprehensive approach to security management.

9. **Reassessment** - Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

Interpol stresses that as well as knowledge of computer architecture, those involved in computer security also needs to be familiar with a number of important IT security functions and organizational matters. Some important functions are:

Information classification

Classification of information must be done according to the appropriate level of availability, e.g. 'open', 'confidential', 'secret' or 'top secret'. The classification should be carried out by the management or by the 'information owner'.

Documentation rules

IT security policy and the security rules for the organization as well as details of contingency plans in the event of a major incident should be documented in a Security Handbook.

Administration and personnel

Interpol has recommended some responsibilities for the management and employee in information security

Management responsibilities

To achieve functional and cost-effective IT security, a number of initial steps must be taken by the management:

- Risk analysis - Threats and risks, acceptable or unacceptable, vary between different organizations. Risks must be analyzed to form policies.
- Policy - There must be an Information security policy written and approved by management. It should include the main security targets, information classification principles, responsible persons, and principles to reach the targets. Security plan - A prioritized plan has to be made to define how the targets and the intentions in the policy document should be realized. The plan is a living document and has to be scrutinized by the IT security officer.
- Security architecture - With the risk analysis, the policy and the plan as a base, security architecture must be chosen.
- Implementation - With the security architecture as a base, different security functions and products must be selected to implement the security architecture (Gefen, 2000).

All senior management, and not just the computer security manager, should be familiar with the computer systems in use. The role of the system manager is crucial. He/she must have a highest degree of integrity, and computer literate to be able to administer the system in a secure and responsible manner. The system manager access level should be restricted to the minimum number of staff required. The IT security manager must be able to check on the system manager's activities. The origin of the problem either accidental or deliberate must be determined by examining the logging information stored on the computer. Analysis of this information must show when, where and how the problem occurred (Yenisey, Ozok, & Salvendy, 2005).

User Responsibilities

Users should be given specific guidelines about what they should do and should NOT do. These guidelines should be distributed in written form, and signed for. Examples of these guidelines are given by Interpol. They are not exhaustive and are as follow:

1. Do not use any computer equipment without permission.
2. Do not try to access information unless you know you are authorized to do so.
3. Do not alter any information on a computer system unless you know you are authorized to do so. (It is also important to provide a clear written statement of what information each user is allowed to access, to whom that information may be disclosed and what action will be taken if the rules are broken.)
4. Do not use a company or authority computer for personal matters without permission.

5. Do not leave a working computer unattended, without using security options that demand retyping a password (e.g. screen saver password).
6. Make sure you know what to do in the event of a virus being discovered on the system. Use virus protection programs.
7. Be aware of malicious program code, when loading files, mails etc. from the internet or other media.
8. Keep your password and user-ID confidential.
9. Do not allow anyone else to use your password. (If people like engineers need access to the system, they should be referred to the system manager.)
10. Do not use anyone else's password.
11. Remember that anything done on the system using your ID and password can be your responsibility.

User Identification and Authorization

Access to a computer can be controlled based on various kinds of 'Identification and Authorization' systems.

Identification is a two-step function:

1. to Identify the user and
2. to Authenticate (validate) the identity

Interpol recommended two identification systems. They are:

Password Systems

It gives protection against casual browsing of information, but will rarely stop a determined criminal. A computer password is like a key to a computer. It allows several people to use the same password like everyone using the same key (Mayayise & Osunmakinde, 2014).

Interpol recommends that passwords should:

- Be issued to an individual and kept confidential, they should not be shared with anyone. (The golden rule is ONE PERSON ONE PASSWORD). Should a temporary user need access to a system, it is usually fairly simple to add to the list of authorized users; once the temporary user has finished his work, his user-ID must be deleted from the system.)
- Be distinct from the user-ID.
    - Ideally be:
        - alphanumeric and
        - at least six characters long.
- Be changed regularly, at least every 30 days. It is possible to warn the user automatically when his password expires.
- Be properly managed. This will involve using a password history list. New passwords will be checked against the list and not accepted if they have already been used. It also involve making a list of frequently used passwords such as names, brands and other words that are easy to guess and not suitable as passwords.
- Be removed immediately if an employee leaves the organization or gives notice of leaving.

III. Research Methodology

These data and information are collected via internet search engines such as Yahoo! and Google. On-line journal and article database such as Ebscohost and Emerald-library were used for data and information collection (Taddesse & Kidan, 2005).

The keywords used for the search are as follows but not limited to:

- Electronic Commerce
- Electronic Commerce Laws
- Internet Law
- United Nations + Electronic Commerce
- OECD + Electronic Commerce
- EU Directives + Electronic Commerce
- Privacy Laws
- Data Protection
- UN + Privacy
- UN + Data Protection
- OECD + Privacy
- OECD + Data Protection
- EU Directives + Privacy + Data Protection
- Digital Signature
- UN + Digital Signature
- OECD + Digital Signature
- Cybercrime

From the initial material collected from the search, specific keywords learnt from the reading of these materials are used to search for topic-specific materials. These keywords are the following but not limited to:

- UNCITRAL + Electronic Commerce
- UNCITRAL + Electronic Signature
- EU Directive + Electronic Signature
- Communication Act
- Data Protection Act + UK
- Electronic Communication Privacy Act
- Fair Credit Reporting Act
- Fair and Accurate Credit Transaction Act
- Gramm-Leach-Bliley Act
- National Information Infrastructure Protection Act
- CAN-SPAM Act
- Spam
- Spam Laws
- E-sign Act
- E-PRIVACY Act
- Ant cybersquatting Consumer Protection Act
- Sarbanes-Oxley Act
- Malaysian Communications and Multimedia Commission
- Communication and Multimedia Content Forum of Malaysia

- Communications and Multimedia Act + Malaysia
- Cryptography
- Electronic Agreement
- Interpol + Computer Crime

From these keywords, primary data and secondary data were collected and reviewed in this paper; to prepare for comparison, discussion, recommendations and finally to derive a conclusion to the research topic (Palmer, Robinson, Patilla, & Moser, 2001).

Analysis

Table 1: Threats on Microcomputer (stand-alone, Personal Computer) systems i.e Risks on Sensitive Information stored on PC systems and Prevention Methods

Read/Create/Modify/Delete

Threat	**Prevention method**
Corruption of files (program or data). A major cause of data loss and corruption is the introduction of viruses to computer systems.	Keep program diskettes write-protected at all times. Do not keep data and software on the same diskette. Otherwise, if software becomes corrupted or infected, the data will usually be lost as well. Making files read-only will prevent them from being infected by some viruses, but not all of them. All media should be scanned for viruses before use, preferably on a system specially designated for the purpose.
Unauthorized access of information stored in the computer	Restrict physical access to the Personal Computer, by locking the door (and the machine if possible) whenever it has to be left unattended. Machines should never be left switched on and running, unless a reliable software protection mechanism has been installed.
Unauthorized use of the computer	As above.
Malicious programs (i.e. viruses)	See Chapter 'Investigations', Section 'Malicious program code' in the Interpol Computer Crime Manual**.(Note: This manual is a confidential document and available to authorized users**)
Loss (by copying or transfer) of information during servicing	Never send equipment with sensitive information on mounted media for servicing. (It is not enough to 'delete' sensitive information because of 'undelete/unerase' possibilities).

Theft of the computer	Restrict physical access to the Personal Computer, by locking the door (and the machine if possible) whenever it has to be left unattended. Laptops are particularly at risk when left unattended in hotel rooms etc. Use cryptography to protect information from unauthorized access.

Transport

Threat	**Prevention method**
Loss of confidential or secret information during transport	Transport media in sealed envelopes and/or locked boxes.
Manipulation of media during transport	As above and electronic seal (cryptologic checksum) on information.
Total loss of media during transport	Never leave media unattended in cars, hotel rooms etc.

Store

Threat	**Prevention method**
Loss (by copying or transfer) of information	Diskettes and other media should be kept locked up in a safe place when not in use.
Physical loss of information	As above and it is advisable to install removable hard disks, which should be kept in a safe place.
Total loss of information through theft of computer and/or media	Regular back-ups of data and system files are essential. Together with the logging information, they will provide a comprehensive security information package.
Loss (by copying or transfer) of information as a result of unauthorized access to, or loan of, media	See Table 1: Architecture-independent threats above.

Table 2: Threats on Mainframe computer systems and Prevention Methods

Read/Create/Modify/Delete

Threat	**Prevention method**
Manipulations or unauthorized access to software	Use separate computers for system/program development and 'production'. If possible, restrict access to 'source code', 'compilers' and 'editors' in 'production' system.

Unauthorized access to information	Users should be given specific written guidelines on what they should and should not do. Guidelines should be signed for. Install an 'Identification and Authorization' system. Adopt a 'two-man rule' for granting privileges. IDS and firewall should be used. Regularly check logs. Regularly check that configuration is correct.
Unauthorized access to information by system administrators, programmers, etc.	As above and: Separate test/development systems from production systems. Restrict access to the computer room. 'Closed shop' for all other than those working in the computer room. Restrict use of 'super user'/'root' privileges. Cryptography should be used for confidential information.
Corruption of files (program or data) by malicious programs	Use 'checksums' on sensitive software to make it possible to control that it has not been changed deliberately. Erase all unnecessary codes, default and unused procedures.
Loss (by copying or transfer) of information during servicing	Servicing of mainframe systems is done 'on site'. In the case of hardware problems with disk drives they should be replaced and the faulty ones sent to the vendor for repair, if possible. They can later be used as replacements, perhaps at another site. Never send equipment with sensitive information on media for servicing without a verifiable guarantee that the information will be destroyed. (It is not enough to 'delete' sensitive information because of 'undelete' and 'unformat' possibilities). Cryptography should be used for confidential information.

Transport in Local Area Network (LAN)/ Wide Area Network (WAN)

Threat	**Prevention method**
Same as above. See Table 3: Threats on Network architectures and mini computer systems (LAN, WAN and the Internet) and Prevention Methods	See Table 3: Threats on Network architectures and mini computer systems (LAN, WAN and the Internet) and Prevention Methods

Transport of media

Threat	Prevention method
Loss of confidential or secret information during transport	Transport media in sealed envelopes or locked boxes. Cryptography should be used for confidential information.
Manipulation of media during transport	As above and electronic seal (cryptologic checksum) on information.
Total loss of media during transport	Never leave media unattended in cars etc.

Store

Threat	Prevention method
Loss (by copying or transfer) of information	Media should be kept in a safe place under lock and key. 'Two-man rule' for access to archives.
Total loss of information through theft of media	Regular back-ups of data and system files are essential. Together with the logging information, they will provide a comprehensive security information package.

A virus is a set of illicit instructions which passes itself on to other programs or documents which it comes in contact. A virus can slowly sabotage a computer system and remain undetected for months. It can delete files, display words or obscene messages or bizarre screen effect. In the case of the Michelangelo virus, this virus can wipe out the whole hard drive. In the case of the Melissa virus, the virus first appeared on the Internet in March of 1999. It spread rapidly throughout computer systems in the United States and Europe. It is estimated that the virus caused $80 million in damages to computers worldwide. In the United States alone, the virus made its way through 1.2 million computers in one-fifth of the country's largest businesses. The creator of the virus, David Smith pleaded guilty on December 9, 1999 to state and federal charges associated with his creation of the Melissa virus. The defendant pleaded guilty was charged in violation of Title 18 United States Code Sections 1030(a)(5)(A) and 2 (Scott, 2008) (Smedinghoff & Bro, 1998).

The US Department of Justice published 100 cases of cybercrime relating to computer intrusion in its website <www.usdoj.gov/criminal/cybercrime/cccases.html> . The cases are non-exhaustive and have been updated since 1998. At least 20 percent of the cases are originated from current and former employee of the victim organization.

IV. Conclusion

No laws can be effective without enforcement. Enforcement that is external in nature is required to ensure that these law are abided. Law and codes of conducts can only be taken seriously if it is enforced seriously. Companies not prosecuting individuals for computer crime because of they feel that the publicity will hurt their image will only create an environment that such acts acceptable. In conclusion, security and safety will remain the most vital issues in electronic commerce that will continue to be discussed, examined and addressed. Actions will be continue to be taken by the society to create new laws, technology, methods and processes to increase security and safety in the cyberspace as e-commerce technologies grow.

One must not be deterred from electronic commerce just because of these issues. There will always be a downside for everything including electronic commerce. Business growth from this new method of doing business is far to lucrative to be abandoned. 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.It is proposed that these principles are examined in order to tackle security and safety in e-commerce. These principles are derived from the review of all the legislations, cases, guidelines, policies and regulations in this paper. All these principles are complementary to each other.Trust is essential for the development of electronic business between parties that have never dealt with each other before. Self-regulation has been recognized by Governments, international organizations, national organizations and consumer organization to create trust in electronic business (Shalhoub, 2006).

REFERENCES

[1] AlGhamdi, R., Drew, S., & Al-Ghaith, W. (2011a). Factors Influencing e-commerce Adoption by Retailers in Saudi Arabia: a qualitative analysis. The Electronic Journal of Information Systems in Developing Countries, 47(1), 1-23.

[2] AlGhamdi, R., Drew, S., & Al-Ghaith, W. (2011b). Factors Influencing e-commerce Adoption by Retailers in Saudi Arabia: a qualitative analysis. The Electronic Journal of Information Systems in Developing Countries, 47(1), 1-23.

[3] AlGhamdi, R., Nguyen, J., Nguyen, A., & Drew, S. (2012). Factors influencing e-commerce adoption by retailers in Saudi Arabia: A quantitative analysis. " International Journal of Electronic Commerce Studies", 3(1), 83-100.

[4] Aljifri, H. A., Pons, A., & Collins, D. J. I. M. (2003). Global e-commerce: a framework for understanding and overcoming the trust barrier. Information Management

[5] Computer Security, 26(3), 222-228.

[6] Barkatullah, A. H. (2018). Does self-regulation provide legal protection and security to e-commerce consumers? Electronic Commerce Research

[7] Applications, 30(4), 94-101.

[8] Blythe, S. E. (2005). 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

[9] Technology, 11(2), 6.

[10] Braga, C. A. P. (2005). E-commerce regulation: New game, new rules? The Quarterly Review of Economics

[11] Finance, 45(2-3), 541-558.

[12] Bygrave, L. A. (2000). European Data Protection: Determining Applicable Law Pursuant to European Data Protection Legislation. Computer Law

[13] Security Review, 16(4), 252-257.

[14] Duh, R.-R., Sunder, S., & Jamal, K. J. T. A. R. (2002). Control and assurance in e-commerce: Privacy, integrity, and security at eBay. Taiwan Accounting Review, 3(5), 1-27.

[15] Furnell, S. M., & Karweni, T. (1999). Security implications of electronic commerce: a survey of consumers and businesses. Internet research, 45(4), 22-30.

[16] Gefen, D. (2000). E-commerce: the role of familiarity and trust. Omega, 28(6), 725-737.

[17] Mayayise, T., & Osunmakinde, I. O. (2014). E-commerce assurance models and trustworthiness issues: an empirical study. Information Management

[18] Computer Security, 45(2), 24-42.

[19] Palmer, M. E., Robinson, C., Patilla, J. C., & Moser, E. P. (2001). Information security policy framework: best practices for security policy in the e-commerce age. Information Systems Security, 10(2), 1-15.

[20] Scott, M. D. (2008). The FTC, the unfairness doctrine, and data security breach litigation: Has the commission gone too far. Admin. L. Rev., 60(5), 127.

[21] Shalhoub, Z. K. (2006). Trust, privacy, and security in electronic business: the case of the GCC countries. Information Management

[22] Computer Security, 54(3), 34-56.

[23] Smedinghoff, T. J., & Bro, R. H. (1998). Moving with change: Electronic signature legislation as a vehicle for advancing e-commerce. J. Marshall J. Computer

[24] Info. L., 17(5), 723.

[25] Taddesse, W., & Kidan, T. G. (2005). e-Payment: Challenges and opportunities in Ethiopia. United Nations Economic Commission for Africa, 45(3), 23-54.

[26] Yenisey, M. M., Ozok, A. A., & Salvendy, G. (2005). Perceived security determinants in e-commerce among Turkish university students. Behaviour
[27] Information Technology, 24(4), 259-274.

[28] De Silva A.D.A., Khatibi A., Azam S.M.F. (2018a). Can parental involvement mitigate swing away from science? Sri Lankan perspectives, Cogent Education

[29] De Silva A.D.A., Khatibi A., Azam, S. M. F. (2018b). Do the Demographic Differences Manifest in Motivation to Learn Science and Impact on Science Performance? Evidence from Sri Lanka, International Journal of Science and Mathematics Education

[30] Delafrooz N., Paim L.H., Khatibi A. (2009). Developing an instrument for measurement of attitude toward online shopping, European Journal of Social Sciences

[31] Dewi N.F., Azam, S. M. F., Yusoff S.K.M. (2019). Factors influencing the information quality of local government financial statement and financial accountability, Management Science Letters

[32] Doa N.H., Tham J., Khatibi A.A., Azam S.M.F. (2019). An empirical analysis of Cambodian behavior intention towards mobile payment. Management Science Letters

[33] Maghfuriyah A., Azam, S. M. F., Shukri S. (2019). Market structure and Islamic banking performance in Indonesia: An error correction model, Management Science Letters

[34] Nguyen H.N., Tham J., Khatibi A., Azam S.M.F. (2019). Enhancing the capacity of tax authorities and its impact on transfer pricing activities of FDI enterprises in Ha Noi, Ho Chi Minh, Dong Nai, and Binh Duong province of Vietnam , Management Science Letters

[35] Nikhashemi S.R., Paim L., Haque A., Khatibi A., Tarofder A. K. (2013). Internet technology, Crm and customer loyalty: Customer retention and satisfaction perspective , Middle East Journal of Scientific Research

[36] Nikhashemi S.R., Valaei N., Tarofder A. K. (2017). Does Brand Personality and Perceived Product Quality Play a Major Role in Mobile Phone Consumers' Switching Behaviour? Global Business Review

[37] Pambreni Y., Khatibi A., Azam, S. M. F., Tham J. (2019). The influence of total quality management toward organization performance, Management Science Letters

[38] Pathiratne S.U., Khatibi A., Md Johar M.G. (2018). CSFs for Six Sigma in service and manufacturing companies: an insight on literature, International Journal of Lean Six Sigma

[39] Rachmawati D., Shukri S., Azam, S. M. F., Khatibi A. (2019). Factors influencing customers' purchase decision of residential property in Selangor, Malaysia , Management Science Letters

[40] Seneviratne K., Hamid J.A., Khatibi A., Azam F., Sudasinghe S. (2019). Multi-faceted professional development designs for science teachers' self-efficacy for inquiry-based teaching: A critical review, Universal Journal of Educational Research

[41] Sudari S.A., Tarofder A.K., Khatibi A., Tham J. (2019). Measuring the critical effect of marketing mix on customer loyalty through customer satisfaction in food and beverage products, Management Science Letters

[42] Tarofder A.K., Azam S.M.F., Jalal A. N. (2017). Operational or strategic benefits: Empirical investigation of internet adoption in supply chain management, Management Research Review

[43] Tarofder A.K., Haque A., Hashim N., Azam, S. M. F., Sherief S. R. (2019). Impact of ecological factors on nationwide supply chain performance, Ekoloji

[44] Tarofder A.K., Jawabri A., Haque A., Azam S.M.F., Sherief S.R. (2019). Competitive advantages through it-enabled supply chain management (SCM) context, Polish Journal of Management Studies

[45] Tarofder A.K., Nikhashemi S.R., Azam S. M. F., Selvantharan P., Haque A. (2016). The mediating influence of service failure explanation on customer repurchase intention through customers' satisfaction, International Journal of Quality and Service Sciences

[46] Udriyah, Tham J., Azam, S. M. F. (2019). The effects of market orientation and innovation on competitive advantage and business performance of textile SMEs, Management Science Letters

[47] Ulfah R., Amril Jaharadak A., Khatibi A.A. (2019). Motivational factors influencing MSU accounting students to become a certified public accountant (CPA), Management Science Letters