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

SECURITY IN E-COMMERCE- A REVIEW OF LEGISLATIONS, CASES, GUIDELINES, POLICIES AND REGULATIONS

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

Abstract---*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. 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 (Barkatullah, 2018; De Silva et al., 2018a; De Silva et al., 2018b; Nikhashemi et al., 2013).*

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

I. 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.

In another report by the Organization for Economic Co-operation and Development (OECD) in 2002 have stated that the internet is still mainly used for marketing purposes and its purpose of use varies according to business's position in the value chain(Measuring the Information Technology, 2002). The propensity to carry our internet purchases and sale is higher in services than in manufacturing and financial services. Business services and wholesale trade are generally the most intensive users. 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.

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

Computer crime has no precise definition. It is often refer to computer related activities which are either criminal or just antisocial. Computer crimes fall into three categories: computer fraud, computer abuse and software piracy. Computer fraud refers to fraud committed using a computer. Computer abuse refers to abusive misuse of computer resources, i.e. the unauthorized access and use of computing facilities and data, also known as hacking; the unauthorized modification of data; and the propagation of viruses. Hackers are unauthorized but talented people. Apast study was the first to attempt to define the hackers community. In the study, five categories were given to the hacker's community (Smedinghoff & Bro, 1998; Dewi et al., 2019; Pambreni et al., 2019; Tarofder et al., 2017). 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 most rare and they profit from activities

Another study by Hollinger concluded that hackers fit into three categories. They are:

- **Pirates**- they are the least technical and confined their activities to pirating software.
- **Browsers**- they have moderate technical ability and used this ability to gain unauthorized access.
- **Crackers**- they are the most technical and are abusers.

A past study concluded that hackers fit into three categories. They are:

- **The elite group** that display a high level of knowledge and motivated by a desire to achieve, self-discovery and by the excitement and challenge
- **The neophytes** that display a sound level of knowledge and are usually followers for the elite group.
- **The losers and lamers group** that display little intellectual ability and are motivated by a desire for profit, vengeance, theft and espionage.

It was discovered that only 30 percent of the hacker community fell into the elite group, 60 percent were neophytes and 10 percent were losers and lamers.

Hacking and computer viruses are two major threats to information systems security. Although in some countries they are not illegal because of lack of legislation outlawing hacking and computer viruses. In countries where legislations are present to outlaw hacking and computer viruses, the following are provided in their legislations:

- **Unauthorized access.** Accessing a computer is defined as a causing a computer to perform any function. Thus trying to log-in to a computer causes the computer to check its authenticity and therefore will be regarded as accessing the computer whether or not the log-in is successful.
- **Tempering with computers, program, or data.** The damage of property when tempering is done includes causing a computer not to function normally, altering or erasing any program or data held in any form or medium and adding any program or data to the contents or any computer storage medium.
- **Accessing a computer to commit further crimes.** It is provided that it is an offence for anyone to access a computer with a criminal or dishonest intent regardless of whether the access in authorized or not.
- **Trespassing with intent to tamper with computers, programs, or data.** This includes physical trespassing of a building or permanent structure.

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. Privacy refers to the ability of the

individual to protect information about himself. There are two types of threats to one's privacy in the cyberspace according to past studies (Bygrave, 2000; Doa et al., 2019; Maghfuriyah et al., 2019; Nguyen et al., 2019). They are:

1. Passive and active activities on the Internet could be monitored by unauthorized parties and
2. These activities could be logged and preserved for future access and disclosed without permission.

On the Internet, a remote Web site can determine the following information about a visitor:

1. The IP address the user is accessing the Web site from;
2. The number of prior visits to the Web site, and the dates;
3. The URL of the page that contained the link to get the user to the Web site;
4. The user's browser type and operating system and version;
5. The user's screen resolution;
6. Whether JavaScript and VBScript are enabled on the user's computer;
7. How many Web pages the user has visited in the current session;
8. The local time and date; and
9. FTP username and password

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.

The Internet could also provide companies with the ability to collect personal information about an individual. These information are listed as follow:

1. Social Security number
2. Current and previous addresses
3. Worker's compensation records
4. Bankruptcies, tax liens, judgments
5. Vehicle identification number trace
6. Non-published phone numbers
7. Background check

Millions of people use the Internet every day to enjoy the wide access of the Internet innocently without knowing that the Internet contains a lot of private information about them. Findings have also shown that given the right circumstances, online users easily forget about their privacy concerns and communicate their personal detail without any reason to do so in particular when the online exchange is entertaining and benefits are offered in return of the information. Although many users have strong opinions on privacy and state their privacy preferences, they are unable to act. Once they are online, they often do not monitor and control their actions. Privacy is important to consumers when they shop and do business online. Data collected unknowingly from the user are used by businesses to solicit business directly and this is annoying and intrusive to one's privacy. Companies that collect this information suffer attacks from internal and external users who have only personal gains in mind. These attacks can disable a system infrastructure or pilfer confidential information like credit card numbers to commit further criminal offences (Braga, 2005; Pathiratne et al., 2018; Rachmawati et al., 2019; Seneviratne et al., 2019; Sudari et al., 2019; Tarofder et al., 2019).

Another pertinent issue in privacy on the Internet is spam. Spam or unsolicited bulk email messaging thrives because of the costs incurred by the spammer sending the spam are extremely low. Research has shown that 80 percent of e-mails sent worldwide are spam and the time employees spend deleting junk e-mails costs companies nearly $22 billion a year. The same article has reported that research has also shown that 75 percent of Internet users receive spam daily and the average number of spam received per day is 18.5 and the average time spent daily in deleting them is 2.8 minutes costing productivity loss of $21.6 billion per year. It was reported that spam has increased by at least 10 percent in all regions. See Figure 1.

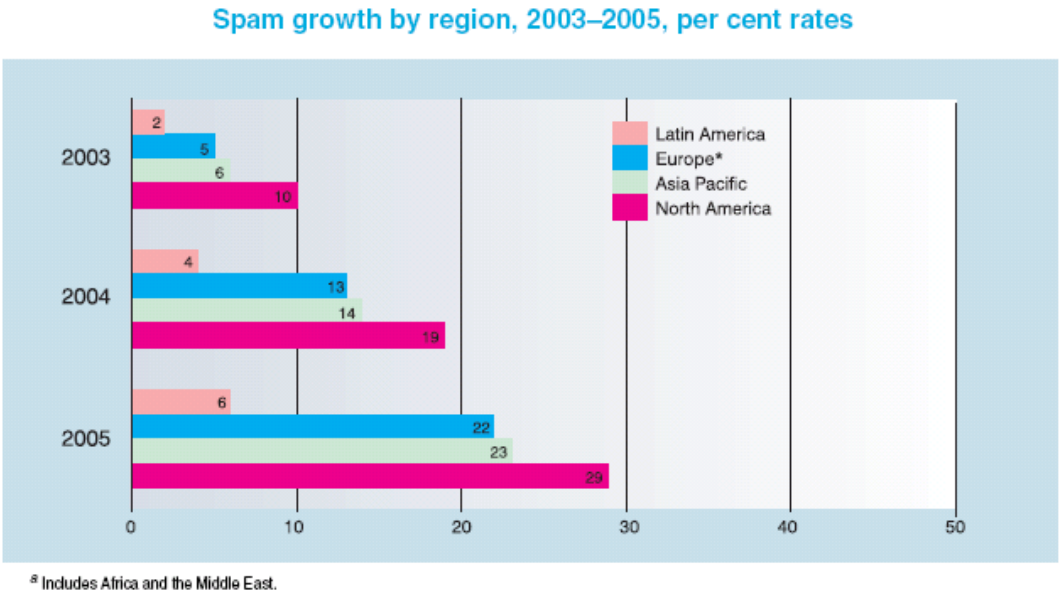

Figure 1: Spam growth by region

As e-business becomes part of an everyday experience of the majority of people who tends to be risk-adverse, security become crucially important. Internet security problems take multiple forms: spam, viruses, web squatting, fraud, 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. 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'.

II. Literature Review

The European Parliament has issued a directive on 8 June 2000 to all member states on legal aspects of electronic commerce. Directive 2000/31/EC(Directive on E-commerce) has the following objectives as outlined in the directive text:

- To forge ever closer links between the states and peoples of Europe.
- To ensure economic and social progress in accordance to the Treaty where the internal market comprises an area without internal frontiers in which the free movements of goods, services and the freedom of establishment are ensured
- To ensure the development of information society services within the area without internal frontiers

The directive provides measures that are strictly limited to the minimum needed to achieve the objectives.

The following are addressed in the directive:

- **Establishment of Information Society service providers.** The directive provides a rule that these providers are located for jurisdiction purposes.

- **Commercial communication.** The directive outlines transparency in advertising and promotional offers. It also gave member states the option of controlling unsolicited emails in their territory. These emails must be clearly identifiable immediately upon receipt and those sending them. The respect of the wish of those who register not to receive such emails must be present.
- **Electronic Contracts.** All member states must ensure that their legislation permits contracts to be concluded electronically. Acceptance must be signified by technological means such as clicking an icon.
- **Liability of service providers.** Service providers are mere conduits are not liable for the information transmitted with the condition that the provider does not initiate the transmission, does not select the receiver of the transmission and does not select or modify the information contained in the transmission.
- **Implementation.** As far as possible this directive must be used with existing laws and rules and when drawing up of codes.

The United Nations Commission on International Trade Law has drawn a Model Law On Electronic Commerce on 1996. This law applies to any kind of information in the form of a data message used in the context of commercial activities. The use of modern means of communication such as electronic mail and electronic data interchange (EDI) for the conduct of international trade transactions has been increasing rapidly and is expected to develop further as technical supports such as information highways and the internet become more widely accessible. However, the communication of legally significant information in the form of paperless messages may be hindered by legal obstacles to the use of such messages, or by uncertainty as to their legal effect or validity. The purpose of the Model Law is to offer national legislators a set of internationally acceptable rules as to how a number of such legal obstacles may be removed, and how a more secure legal environment may be created for electronic commerce. The principles expressed in the Model Law are also intended to be of use to individual users of electronic commerce in the drafting of some of the contractual solutions that might be needed to overcome the legal obstacles to the increased use of electronic commerce (Aljifri, Pons, & Collins, 2003; Nikhashemi et al., 2017; Tarofder et al., 2019; Ulfah et al., 2019; Tarofder et al., 2016; Udriyah et al., 2019).

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. The e-ASEAN Reference Framework For Electronic Commerce Legal Infrastructure provides a guide for the following:

- Helping ASEAN member states that do not have any e-commerce laws in place to draft their own;
- Helping ASEAN member states that already have e-commerce laws in place to facilitate cross-border e-commerce and the cross-recognition/ cross-certification of digital certificates/digital signatures.

The reference framework is developed based on the following e-commerce laws of ASEAN member states, and in consultation with the legal experts from the governments of these member states. These laws are:

- Electronic Transactions Act (ETA) of Singapore
- Digital Signature Act (DSA) of Malaysia
- Electronic Commerce Act (ECA) of Philippines
- Electronic Transactions Order (ETO) of Brunei
- Draft Electronic Transactions Bill (ETB) of Thailand

These e-commerce laws are based on UNCITRAL's Model Law on Electronic Commerce and Draft Model Law on Electronic Signatures, as well as the e-commerce and electronic signature laws of the U.S. and Europe.In the Malaysian

context, the Communications and Multimedia Act 1998(CMA) was brought into force on the 1st April 1999. This legislation provides the policy and regulatory framework for convergence of the telecommunications, broadcasting and computer industries. The Act is based on the basic principles of transparency and clarity; more competition and less regulations; bias towards generic rules; regulatory forbearances; emphasis on process rather than content; administrative and sector transparency; and industry self-regulation. Section 211 of the CMA seeks to regulate the control of content which are obscene, indecent, and false and contents that contain threats and harassment. As self-regulation is a pinnacle of this Act, a content forum will be set up to draw a code of practice. Section 212 of the CMA provides for the establishment of the Content Forum for the formulation of the content code. The Content Code in now in the process of being formulated. The Content Code will cover all content that is provided over the electronic networks including radio, television and online services. While the content code is being developed the Broadcasting Guidelines and the Advertising Code developed by the Ministry of Information will continue to be enforced.

The Communication and Multimedia Content Forum of Malaysia(CMCF) was established in February 2001 as a society with representation from all relevant parties, including the "supply and demand" side of the communications and multimedia industry - to govern content and address content related issues disseminated by way of electronic networked medium(CMCF, 2005). CMCF was designated on 29 March 2001 by the Malaysian Communications and Multimedia Commission(MCMC) to facilitate the formation of the content code (Palmer, Robinson, Patilla, & Moser, 2001; De Silva et al., 2018a; De Silva et al., 2018b; Nikhashemi et al., 2013).

The Malaysian Communications and Multimedia Commission(MCMC) is no doubt the single regulator for the converging communications and multimedia industry(MCMC). Its key role was in the regulation of the communications and multimedia industry based on the powers provided for in the Malaysian Communications and Multimedia Commission Act (1998) and the Communications and Multimedia Act (1998). The role of the Malaysian Communications and Multimedia Commission is also to implement and promote the Government's national policy objectives for the communications and multimedia sector. The Malaysian Communications and Multimedia Commission is also responsible for overseeing the new regulatory framework for the converging industries of telecommunications, broadcasting and on-line activities. The regulatory framework is as follow:

- **Economic regulation**, which includes the promotion of competition and prohibition of anti-competitive conduct, as well as the development and enforcement of access codes and standards. It also includes licensing, enforcement of license conditions for network and application providers and ensuring compliance to rules and performance/service quality.
- **Technical regulation**, includes efficient frequency spectrum assignment, the development and enforcement of technical codes and standards, and the administration of numbering and electronic addressing.
- **Consumer protection**, which emphasizes the empowerment of consumers while ensuring adequate protection measures in areas such as dispute resolution, affordability of services and service availability.
- **Social regulation** which includes areas of content development and content regulation; the latter includes the prohibition of offensive content and public education on content-related issues (Scott, 2008).

On 1 November 2001, MCMC a In the Malaysian context, the Communications and Multimedia Act(CMA) was brought into force on the 1st April 1999. This legislation provides the policy and regulatory framework for convergence of the telecommunications, broadcasting and computer industries(KTAK, 2005). The Act is based on the basic principles of transparency and clarity; more competition and less regulations; bias towards generic rules; regulatory forbearances; emphasis on process rather than content; administrative and sector transparency; and industry self-regulation. Section 212 of the CMA provides for the establishment of the Content Forum for the formulation of the content code(Communications

and Multimedia Act 1998). The Content Code in now in the process of being formulated. The Content Code will cover all content that is provided over the electronic networks including radio, television and online services. While the content code is being developed the Broadcasting Guidelines and the Advertising Code developed by the Ministry of Information will continue to be enforced.

The Communication and Multimedia Content Forum of Malaysia(CMCF) was established in February 2001, as a society, with representation from all relevant parties, including the "supply and demand" side of the communications and multimedia industry - to govern content and address content related issues disseminated by way of electronic networked medium(CMCF, 2005). CMCF was designated on 29 March 2001 by the Malaysian Communications and Multimedia Commission(MCMC) to facilitate the formation of the content code.The Malaysian Communications and Multimedia Commission(MCMC) is no doubt the single regulator for the converging communications and multimedia industry(MCMC). Its key role was in the regulation of the communications and multimedia industry based on the powers provided for in the Malaysian Communications and Multimedia Commission Act (1998) and the Communications and Multimedia Act (1998). The role of the Malaysian Communications and Multimedia Commission is also to implement and promote the Government's national policy objectives for the communications and multimedia sector. The Malaysian Communications and Multimedia Commission is also responsible for overseeing the new regulatory framework for the converging industries of telecommunications, broadcasting and on-line activities (Yenisey, Ozok, & Salvendy, 2005; Dewi et al., 2019; Pambreni et al., 2019; Tarofder et al., 2017).
The regulatory framework is as follow:

- **Economic regulation**, which includes the promotion of competition and prohibition of anti-competitive conduct, as well as the development and enforcement of access codes and standards. It also includes licensing, enforcement of license conditions for network and application providers and ensuring compliance to rules and performance/service quality.
- **Technical regulation**, includes efficient frequency spectrum assignment, the development and enforcement of technical codes and standards, and the administration of numbering and electronic addressing.
- **Consumer protection**, which emphasizes the empowerment of consumers while at the same time ensures adequate protection measures in areas such as dispute resolution, affordability of services and service availability.
- **Social regulation** which includes the twin areas of content development as well as content regulation; the latter includes the prohibition of offensive content as well as public education on content-related issues.

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 illegal access- each party shall adopt domestic laws that make intentional access without right on whole or part of a computer system as a criminal offence. The offence may be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.
- On illegal interception- each party shall adopt domestic laws that make dishonest intentional interception of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data without right as criminal offence.
- On Data interference- each party shall adopt domestic laws that make intentional damaging, deletion, deterioration, alteration or suppression of computer data without right as a criminal offence.

- On System interference- each party shall adopt domestic laws that make intentional hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data without right as a criminal offence.
- On Computer-related forgery- each party shall adopt domestic laws that make the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible, without right as a criminal offence
- On Computer-related fraud- each party shall adopt domestic laws that make intentional causing of a loss of property to another by: any input, alteration, deletion or suppression of computer data, and any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another; as a criminal offence.

For international co-operation

- Each party shall co-operate with each other to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence through application of relevant international instruments on international co-operation in criminal matters, and arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws (Furnell & Karweni, 1999; Doa et al., 2019; Maghfuriyah et al., 2019; Nguyen et al., 2019).
- Each party shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence (Mayayise & Osunmakinde, 2014; Pathiratne et al., 2018; Rachmawati et al., 2019; Seneviratne et al., 2019; Sudari et al., 2019; Tarofder et al., 2019).
- A party may within the limits of its domestic law, without prior request, shall forward to another party, information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving party in initiating or carrying out investigations or proceedings concerning criminal offences

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and nurturing international co-operation. The Convention is the result of four years of work by Council of Europe experts, the United States, Canada, Japan and other countries which are not members of the organization.The Interpol issued a comprehensive computer crime prevention method in 2003. The IT Security and Crime Prevention Methods could not only be used to prevent crime in companies, but could also be used to protect private computer systems. It also gives an introduction to what an investigator needs to know about Information Technology (IT) security measures in order to be able to carry out investigations in an IT environment and to give advice in crime prevention methods (Duh, Sunder, & Jamal, 2002; Nikhashemi et al., 2017; Tarofder et al., 2019; Ulfah et al., 2019; Tarofder et al., 2016; Udriyah et al., 2019).

Interpol has defined some terms related to IT security in their report containing the Methods. They are as follow:

IT security: definitions

Confidentiality (Secrecy)

Information and other resources are only disclosed for those 'users' (persons, entities or processes) who are authorized to have access to it.

Integrity

Information and other resources are modified only by those 'users' who have the right to do so. The accuracy and completeness of the data and information is also guaranteed (AlGhamdi, Drew, & Al-Ghaith, 2011a; De Silva et al., 2018a; De Silva et al., 2018b; Nikhashemi et al., 2013).

Availability

Authorized 'users' can access information and other resources when needed.

Threat

A 'threat' is a potential undesirable incident.

Risk

A 'risk' is the estimated probability that a 'threat' will be activated.

Interpol has also recommended that in order to protect the data held on a computer system, various steps have to be taken: individual users should only be able to read the information which is needed to do their job; they should only be able to modify information which is specifically their job to modify. Finally, some information should not be accessible at all for individual users, e.g. the various log records (AlGhamdi, Drew, & Al-Ghaith, 2011b).

III. Research Methodology

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; Dewi et al., 2019; Pambreni et al., 2019; Tarofder et al., 2017).

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.

Note:

Read/Create/Modify/Deleterefers to information (data and software) inside the computer system.

Transport refers to information (data and software) 'transported' via a network or on media.

Storerefers to information (data and software) when it is stored on computer media and taken out of the computer system. (I.e. back-up tapes/diskettes).

Table 1: Architecture Independent Threats(members of staff, unauthorized access from external sources, media handling, malicious program code and electronic emission) and their prevention methods

Members of staff

Threat	Prevention method
Disloyal staff	The strongest form of security is often procedural security with attendant staff awareness and responsibility.

Unauthorized access to information by users	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. Do not reveal your password too anyone. Keep identification and authorization cards in a safe place. Regularly check logs. Regularly check that configuration is correct. Install an Intrusion Detection System.
Unauthorized access to information by system administrators, programmers, etc.	The same as above and: Use separate systems for program development and for 'production'. Restrict access to equipment with sensitive information; adopt 'two-man rule'. Restrict use of 'super user'/'root' privileges.
Unauthorized access to information by temporary staff, e.g. consultants, service engineers etc.	As for other staff and: Limit their access to the system to the time and day required for the specific task. Do not forget to cancel their access rights and close their temporary accounts. Do not leave communication lines for remote servicing open when not needed.

Unauthorized access from external sources

Threat	**Prevention method**
Unauthorized access	Install an 'Identification and Authorization' system. Adopt a 'two-man rule' for granting privileges. Regularly check logs. Regularly check that configuration is correct. Install a firewall.

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 (by copying or transfer) of information as a result of unauthorized access to, or loan of, media	Encrypt sensitive information. Staff handling the media should not have access to the encryption keys. 'Two-man rule' for back-up. 'Two-man rule' for access to archives.
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)

Malicious program code

Threat	**Prevention method**
Viruses and other malicious programs	Install 'anti-virus software'. 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**)
Programs altered to obtain access to, or manipulate, information without authorization	Depends on computer architecture. Use separate systems for program development and for 'production'. If possible, restrict access to 'source code', 'compilers' and 'editors' in 'production' system and restrict use or installation of non-standard software packages. An Intrusion Detection System might detect this type of problem.

Electronic Emission

Threat	**Prevention method**
Despite all precautions, it is still possible for a determined intruder to eavesdrop on information by picking up and interpreting electromagnetic emissions from the Personal Computer or workstation. In a manner somewhat similar to the way in which it is possible to detect the operation of a television receiver and determine which channel is being watched. This type of eavesdropping is most likely to occur when very sensitive information, such as that of high commercial value or dealing with matters of national security is involved.	Use equipment with no or limited signal leakage ('tempest') or put the equipment in a shielded room. Although effective, those methods are expensive and are only to be recommended when there is an extremely high risk. Optical fibres can be used to prevent emission leakage from the lines running between peripherals and the Local Area Network (LAN). Encryption of the Wide Area Network (WAN) will not stop electromagnetic emissions but the eavesdropper will not be able to use the information without the encryption key.

Table 2: Threats on Network architectures and minicomputer systems (LAN, WAN and the Internet) and Prevention Methods

Read/Create/Modify/Delete

Threat	**Prevention method**
Manipulations or unauthorized access to software or information in each workstation (PC) in the network	See Table 2: Threats on Microcomputer (stand-alone, Personal Computer) systems i.e Risks on Sensitive Information stored on PC systems and Prevention Methods
Unauthorized access to information in the 'server' by users	Users should be given specific written guidelines on what they are allowed and not allowed to do. Guidelines should be signed for. Install an 'Identification and Authorization' system. Adopt a 'two-man rule' for granting privileges. Regularly check logs. Regularly check that configuration is correct. IDS should be installed.
Unauthorized access to information by system administrators, programmers' etc.	As above and: Use separate systems for program development and for 'production'. Restrict access to server; adopt 'two-man rule'. Restrict use of 'super user'/'root' privileges.
Corruption of files (program or data). A major cause of data loss and corruption is the introduction of viruses to computer systems.	All media should be scanned for viruses, preferably on a system specially designated for the purpose, before use. Erase all unnecessary codes, default and unused procedures.
Total loss of information through 'disk crash' or deliberate destruction of files	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 during servicing	Some mini-server servicing can be done 'on-site' but in the case of some hardware problems the equipment will have to be taken away for repair by the service company/vendor. 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' the sensitive information because of 'undelete' and 'unformat' possibilities)

	Remember that after repair, the disk drives could be reused somewhere else and your information might be compromised. If it is decided to replace a disk with sensitive information, destroy it yourself.
Theft of the server	The server should be kept locked up in a safe place.

TRANSPORT in Local Area Network (LAN)

Threat	**Prevention method**
Interception of cables	Segmentation of the LAN. Use optical fibres. Regularly inspect LAN. Encrypt LAN.
Interception of networks components (like 'routers', 'bridges', 'gateways', 'repeaters' etc.)	Restrict physical access to components. Regularly check that the configuration of each individual component is correct.
Manipulation of network components	As above.
Unapproved workstations	The system should be set up in a way that the management must approve the workstations before they can be used. Regularly check that the configuration is correct.
Network administrator accessing user files	Network Administrators should be given specific written guidelines on what they should and should not do. Guidelines should be signed for. Restrict use of 'administrator' privileges. Install an 'Identification and Authorization' system. Adopt a 'two-man rule' for granting privileges.
Access to the LAN from 'outside'	Provide guidelines for the use of modems or other connections. IDS and firewall should be used. Regularly check that the configuration is correct.

Transport in Wide Area Network (WAN)

Threat	**Prevention method**
Interception of cables	Communications can be encrypted, but there may be legal restrictions.

Interception of radio communications	As above.
Intruders ('hacking'/'cracking')	Use special modems at each end, which recognize each other's signals (mutual signal recognition). Install an 'Identification and Authorization' system. Adopt a 'two-man rule' for granting privileges. IDS and firewall should be used..

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.
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.

In the US, the National Information Infrastructure Protection (NIIP) Act 1996 was enacted to legislate issues relating to computer crime. This act was an amendment of the Computer Fraud and Abuse Act 1986. The NIIP Act 1996 or 18 USC 1030 Amended covers the following(18 USC 1030):

- The conduct of a person who deliberately breaks into a computer without authority, or an insider who exceeds authorized access, and thereby obtains classified information and then communicates the information to another person, or retains it without delivering it to the proper authorities. Proof is required whether or not that the individual knowingly used a computer without authority, or in excess of authority, for the purpose of obtaining classified information. It is the use of the computer which is being focused upon and not the unauthorized possession of, access to, or control over the classified information itself. Law makers have made clear that 'obtaining information' includes observing the data.
- The information includes information contained in a financial record of a finance institution or a card issuer, information from any department or agency of the United States or information from any protected computer involved in interstate or foreign communication (Blythe, 2005).
- Protection of non-public computers, and computers used by or for the government from intentional unauthorized access is also provided by this act.

- The conduct of a person who deliberately breaks into a computer without authority or an insider who exceeds authorized access with the intention to conduct other crimes and defraud (AlGhamdi, Nguyen, Nguyen, & Drew, 2012).
- The conduct of person who without authorization when transmitting of a program, code, information or command causing damage. Whether the damage is reckless or not the person is committing an offence.
- The conduct of person through unauthorized access steals passwords or information and transmits them to foreign hands with the intent to defraud. One can imagine a situation in which hackers penetrate a system, encrypt a database and then demand money for the decoding key. This new provision would ensure prosecution of modern-day blackmailers who threaten to harm or shut down computer networks unless their extortion demands are met. This act also covers the conduct of transmitting threats via any form of communication with the intent of extortion to cause damage to a protected computer (Taddesse & Kidan, 2005).

IV. Conclusion

In varying degrees, the economies of the world are driven by developments in information technology with the robust growth of the e-commerce environment. The future of the cyber marketplace will depend to a large degree of safety and security.The development of electronic commerce and facilitation of international trade using electronic business has necessitated the creation of legal and regulatory framework. The safety and security or electronic commerce could not be left to introduction of legislations and introduction of legislations are not proactive to change. Legislations are often created after a problem occurs. Self-regulation means that businesses involved in electronic business voluntarily undertake to comply with certain rules of conduct when dealing electronically with others. It can take different forms such as adopting a code of conduct, participating in a national or international scheme.For example, the Data Processing Management Association(DPMA) has developed a code of conduct for its members. The DPMA code of ethics and standards are as follow:Industry leaders felt that ethics should be not be legislated but rounded on the principle of self-control and performance. Studies have shown that ethical behavior is more prevalent in companies that take a strong ethical stand and enforce ethical employee behavior. With ethics, it is hoped that positive influences on values (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.
[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