Sys Rev Pharm 2020; 11(1):673-679
A multifaceted review journal in the field of pharmacy

How do Legislations, Regulations, Policies and Cases Influence the Security in E-Commerce?

[1] Omar Abdel Jaber*, [2]Johar MGM, [1]Sultan Al-masaeed

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

ABSTRACT

As e-business becomes part of a majority of people's everyday life that appears to be risk-adverse, protection becomes crucially important (E-Commerce & Growth Study 2003). Internet security problems take several forms: spam, malware, site squatting, piracy, copyright infringement, denial of service, unauthorized intrusion into corporate or personal computers and networks (theft or misuse of the information stored therein), infringements of privacy, abuse and harassment. The following topics will be discussed for the purpose of this study: e-commerce laws, computer crimes, e-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.

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

Correspondence:
Omar Abdel Jaber
Management and Science University
Corresponding author: mdgapar@msu.edu.my

INTRODUCTION

In the 21st century, doing business is distinctly different than in the preceding century. With the rapid growth of the internet and the burgeoning use of ICT, trade has changed in terms of its trade and exchange medium. Trade is now done electronically and it is a big part of the ICT-based economy. Electronic commerce or e-commerce uses the internet as its main transaction medium, though other non-internet-based forms of transaction exist. Data revealed that in 2002 the number of Internet users worldwide exceeded 591 million (E-Commerce & Technology Survey, 2003). The study by the Secretariat of the United Nations Conference on Trade and Development (UNCTAD) also revealed that overall online revenues for 2002 were estimated at USD 43.47 billion for the United States, USD 28.29 billion for the European Union, USD 15 billion for the 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; Pamb).

In 2004, 494 information security practitioners in US companies, government departments, financial institutions, medical institutions, and universities were surveyed by the Computer Security Institute and the FBI (AlGhamdi, Nguyen, Nguyen, & Drew, 2012; Doa et al., 2019; Maghfuriyah et al., 2019; Nguyen et al., 2019). The Sarbanes-Oxley Act is starting to influence information security in many industries. (The Sarbanes-Oxley Act is an act intended to protect investors by enhancing the quality and reliability of corporate filings provided under the securities laws (H.R. 3763). The legislation is intended to improve corporate governance after the Enron scandal. Fraud and white collar corruption are subject to tougher punishments. Total sentences rose from 5 to 10 years for mail and wire fraud).

• Security awareness training is seen by the vast majority of organizations as relevant while (on average) respondents from all sectors do not believe that their organization is investing enough in this field (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.

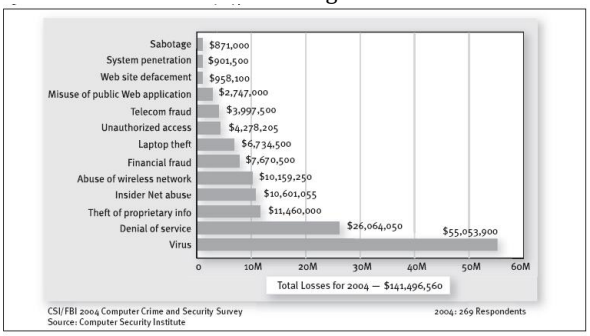

Figure 1: Estimated Losses due to security incidents by type

The E-commerce & Development Report also stated that sales of IT security are increasing and are expected to reach USD 45 billion by 2006, compared to USD 17 billion in 2001, indicating that the value of IT security in the ICT economy. Yet investing in IT security solutions does nothing to secure e-commerce protection. While technology helps reduce risk, it is ultimately the essential function of governments to maintain peace and security in the Internet and e-commerce as a whole, and the rule of law as well. A number of companies were subsequently set up to implement this new technology (Braun, 2007). Individual sub-scribers were linked to each other via an exchange. Each subscriber was connected directly to the

exchange and the operator had a manual switchboard for connecting the subscribers to each other. This was followed by the introduction of electromechanical switching. In a step-by-step switch, a call was established and routed in a set of progressive electromechanical steps, each under the direct control of the user's dialing pulses. The first crossbar switch was used in 1932 in Sweden. The usefulness of the telegraph system was soon appreciated and a rapid growth resulted. Eventually the wires of the telegraph system covered the USA and Europe. While this was going on the next step was to extend the telegraph system between countries separated by water. The first successful underwater cable was put across the channel of English between France and England in 1851 and seven years later, a cable was laid across the Atlantic Ocean. A network of underwater telegraph cables began to be established around the world. Bolster groups will confront new issues one of a kind to VoIP, for example, low volume and misshaped voice quality and will require unique preparation to react fittingly and structure some adaptability into each agreement and relation.

VoIP is as yet developing and nobody knows precisely what's in store. Try not to stall out with an agreement that binds you to the past. Pushing voice correspondence onto the information organize doesn't mean laying off the whole telecom staff. Voice information and customary information present totally different issues. Your VoIP group needs mastery into two regions. In the environment of competition where many innovations are being competitive to both of them, the innovation rate is higher as compared to the industry of old telecom. In the old days of such industry it was quite complicated to implement such equipment before the process of labor for trial purpose in the advancement of such equipment, where it is understood that when there is any sort of failure to such network switch there will be disruption of network services. Prices of equipment have declined, quality of call has improved and specialist organizations have increased significant experience making VoIP administration works. Consolidating those variables has changed VoIP from intriguing innovation idea to genuine corporate resource. Early adopters concentrated solely on the considerable cost reserve funds that can result from VoIP organization.

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) Applies to the management of business relationships and the selling of information, services and resources through electronic telecommunications networks. E-commerce usually often applies to the exchange of goods and services over the Internet, including wider economic activity. E-Commerce consists of business-to - consumer and business-to - business, carried out through the Internet or other electronic networks (Barkatullah 2018).

The international essence of cybercrimes has resulted in international cyber legislation. Cyber laws is a body of law that affects the computer networks world, particularly the Internet. As Internet traffic has increased, so the amount and kind of legal problems surrounding the technology have increased. Hotly discussed topics include the obscenity of certain web pages, privacy protection, and freedom of speech, electronic commerce enforcement and the applicability of copyright laws. Crime is the deliberate conduct of an act that is generally considered socially detrimental or illegal, and is clearly specified, forbidden and punished by criminal law. Crimes in the common-law tradition were initially largely established by a court ruling. Most offences under common law are codified today. There can be no crime without a rule according to a widely recognized theory, nullius crime sine leg. The legislation and regulations are the essential part of the country regulatory control regarding the country security measures that is the provide the confidence to the society being safe in the country.

Right to privacy is a person's right to be free of intrusion into personal matters. Symmetric encryption involves both encryption and decryption of the same key. Asymmetric encryption, or cryptography with a public key, involves a pair of keys, one for encryption and one for decryption. Cryptography is a practice of enciphering and deciphering secret code messages in order to make them incomprehensible to all but the intended recipient.

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 in relation to the purpose of this study is vital as policies are a high-level overall plan that embraces the general goals and acceptable procedures of a government body in particular. It also provides an idea of the overall goals of a government's macro-level implementation of e-commerce.
- 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).

A review 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.

LITERATURE REVIEW

UNCITRAL's decision to devise model legislation on electronic commerce was made in response to the fact that current legislation regulating the exchange and storage of information in a number of countries is insufficient or obsolete because it does not envisage the use of electronic commerce. 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 the law requires that the information be in its original form, the data message must be accompanied by a reliable assurance that it must be possible to display the information and the information to the person to whom it is to be submitted (Bygrave, 2000).
- Evidential weight. Data messages will be given evidential weight where reliability is assured.

Information classification

Data classification must be achieved at the correct level of availability, such as 'available,' 'confidential,' 'classified' or 'top secret.' Classification should be done by management or the 'details holders'.

IT security policies and organizational security laws as well as contingency planning information in case of a major incident should be recorded in a Security Manual.

Administration and personnel

Interpol has suggested certain administrative and workplace roles in cyber security

Leadership duties

Management must take a series of initial steps to achieve functional and cost-effective IT security:

- Risk analysis-Threats and risks, acceptable or inacceptable, vary from one organization to another. Risks need to be evaluated to form policies.
- Policy-Information security policies must be set down and accepted by management. This will include the main security objectives, principles of information management, responsible individuals, and guidelines for achieving the goals.
- Security plan-A strategic plan will be drawn up to determine how the priorities and objectives in the strategy document are to be accomplished. The plan is a living document and the IT security officer needs to scrutinize the program.
- Security architecture-Security architecture must be chosen using risk analysis, policy and plan as a basis (Gefen, 2000).

The level of access for system managers should be restricted to the minimum number of workers needed. The IT Security Manager must be in a position to monitor the activities of the system manager. The origin of the problem has to be determined by examining the logging information stored on the computer, either accidentally or deliberately. Analysis of this information must show when the problem occurred, where, and how.

User Responsibilities

Users should have clear instructions for what to do, and should NOT do. These guidelines should be distributed and signed in written form. Interpol gives examples of these Guidelines. They are not exhaustive and are as follow:

1. without permission to use any computer equipment.
2. Seek not to access details unless you know you are entitled to do so.
3. Should not use a company or authority computer without authorization for personal matters.
4. Should not leave unattended a working machine without using protection options that allow a password to be retyped (e.g. password for screen saver).
5. In case a virus is found on the machine, make sure you know what to do. Using the tools to guard against viruses.
6. Be mindful of malicious software code when loading internet or other media files, mails etc.
8. Keep confidential your password and User ID.
9. Let nobody else use your password. (If such persons need access to the system, they should be referred to the system manager.)
10. Do not use password for anyone else.
11. Remember that it is your responsibility to do anything done on the system using your ID and password.

User Identification and Authorization

You can monitor access to a computer based on different forms of 'Identification and Authorization' systems.

Identification is implemented in two stages:

1. Identifying the Client and
2. To authenticate the name

Interpol recommended two identification systems. They are:

This offers protection against casual information searching, but can never stop a committed criminal. A password on a computer is like a key to a computer. This enables several users to use the same password as those using the same key (Mayayise & Osunmakinde, 2014).

Interpol recommends that passwords should:

- They should be sent to a person and kept private, and should not be shared with others. (ONE PERSON ONE PASSWORD is the Golden rule). When a temporary user wishes to access a program, adding to the list of allowed users is typically relatively simple; once the temporary user has done his work, his user-ID must be removed from the system.)
- Delete automatically when an employee leaves the company or notifies them of their departure.

METHODS

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 Notification Act
- Accurate and fair credit transaction legislation
- Act Gramm-Leach-Bliley
- 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

This section provides the analysis of the study that is mentioned bellow:

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

Threat	Prevention method
Unauthorized access of computer-saved information	Restrict physical access to the Personal Computer, by locking the door (and the machine if possible) when left unattended. Unless a reliable software protection mechanism is installed, machines should never be left switched on and running.
Unauthorized use of the computer	As above.
Malicious programs (i.e. viruses)	See chapter 'Investigations,' section 'Malicious program code' in the Interpol Computer Crime Handbook.(Note: this manual is a confidential document and available to authorized users)
Loss of information (by copying or transferring) during operation	Never send devices with sensitive information for servicing on mounted media. (Because of the possibilities of 'undelete/unease' it is not enough to 'delete' confidential information).

Store

Threat	Prevention method
Physical loss of information	As above, it is recommended that removable hard disks be installed, which should be kept in a safe place.
Comprehensive loss of information through computer and/or media theft	Daily data and device file backups are indispensable. They must include a complete set of security information, along with the logging information.
Loss of information (by copying or transferring) as a result of unauthorized access to or loan of the media	See Table 1: Architecture-independent threats above.

Table 2: Threats on Mainframe computer systems and Prevention Methods

Threat	Prevention method

Manipulations or unauthorized access to software	Use separate computers to develop and 'produce' the system / program. Restricted access to 'source code,' 'compilers' and 'editors' within the 'development' program where possible.
Unauthorized access to information	Users should be provided with clear written instructions about what they should and should not be doing. Guidelines for that should be signed. Install a system of 'Identification and Authorization.' Put in a 'two-man rule' to grant privileges. IDS and firewall One should use it. Checks reports periodically. Verify the configuration is accurate periodically.
Unauthorized system administrators, programmers and so on access to information.	As previously mentioned and: Test / development systems separate from production systems. Entry to the computer room is prohibited. 'Closed store' for anyone other than those who work in the computer room. Limit the use of the privileges 'super user'/'root.' Confidential details can be used for cryptography.
File corruption (program or data) associated with malicious programs	Use 'checksums' on sensitive software to enable control that it has not been altered intentionally. Clear all unnecessary codes, default procedures and unused ones.
Loss of information (by copying or transferring) during operation	Mainframe systems service is done 'on site.' They should be replaced in case of hardware problems with disk drives and, if possible, the faulty ones should be sent to the vendor for repair. They may be used as replacements later, perhaps at a different location. Never send media-sensitive equipment for service without a verifiable guarantee that the information will be destroyed. (Because of the 'undelete' and 'unformed' options, it is not enough to 'delete' sensitive information). To use cryptography 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 minicomputer systems (LAN, WAN and the Internet) and Prevention Methods	See Table 3: Threats on Network architectures and minicomputer systems (LAN, WAN and the Internet) and Prevention Methods

Transport of media

Threat	**Prevention method**
Confidential or confidential knowledge lost during transportation	Carrying media in sealed envelopes or boxes closed. You should use cryptography for confidential information.
Manipulation of media during transport	As previously mentioned, electronic seal (Crypto logical checksum)

	information.
Total loss of media during transport	Never leave media unattended in cars etc.

Store

Threat	Prevention method
Insecurity (by copying or transfer) of data	The media should be kept under lock and key in a secure place. 'Two man law' for archive access.
Total loss of information via media theft	Daily data and device file backups are indispensable. They must include a complete set of security information, along with the logging information.

In the Michelangelo virus case, this virus can wipe the entire hard drive off. The virus first appeared on the internet in March of 1999 in the case of the Melissa virus. It spread rapidly across US and European computer systems. The virus is estimated to have caused damage of $80 million to computers around the world. In the United States alone, the virus has made its way through 1, 2 million computers in one-fifth of the biggest businesses in the world. The defendant pleaded guilty had been convicted in violation of Sections 1030(a) (5) (A) and 2(Scott, 2008) of Title 18 United States Code (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.

DISCUSSIONS AND CONCLUSIONS

Without enforcement no laws can work. External enforcement is required to ensure that these laws are complied with. Law and codes of conduct can only be taken seriously if it is seriously enforced. Companies that do not prosecute individuals for computer crime because they fear that the advertising will harm their reputation will only establish an atmosphere conducive to these acts. 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 too 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. Such values are drawn from this paper's analysis of all the rules, cases, guidelines, legislation, and regulations. Both of these concepts are complementary to each other. Trust is important for the creation of electronic business between parties who have never previously interacted with each other. Governments, foreign organizations, regional organizations, and consumer associations have recognized self-regulation to build 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