The State of E-Government Security in Malaysia: Reassessing the Legal and Regulatory Framework on the Threat of Information Theft

Sonny Zulhuda
Ahmad Ibrahim Kulliyyah of Laws
International Islamic University Malaysia
Selangor, Malaysia
sonny@iium.edu.my

Abstract— **Electronic government is the way ahead for Malaysia, embracing the advances of new technologies while targeting more efficiency in delivering its services to the citizens. However, there have been many challenges and threats that stand in the way before achieving e-government advantages to the fullest. Among those threats is the problem of information theft, which is an illegal acquisition of information assets in a myriad of modes and methods. This emergence of information theft is an obvious threat to the sustainability and resilience of Malaysian electronic government. It is contended here that in order to succeed in the e-government initiatives, authorities would need to relook at the legal and regulatory framework they currently have at their disposal. Laws need to be reassessed and repositioned to enable its enforceability in the digital environment especially in the context of e-government security. If this aspect fails to be examined and improved, the e-government initiative is likely destined to fail too.**

Keywords-E-government; information security; information theft; law and regulation

I. INTRODUCTION

The World Bank[1] defines "electronic government" (or "e-government") as "the use by government agencies of information technologies that have the ability to transform relations with citizens, businesses, and other arms of government." Viewed broadly as defined, the expected outcome of e-government would be less corruption, increased transparency, greater convenience, revenue growth, and cost reductions.

In Malaysia, the adoption of electronic government can be traced back to two decades ago when the then Prime Minister Mahathir Mohammad conceptualized the national "Vision 2020" which further inspired the Multimedia Super Corridor (MSC) project that frames e-government as one of the project's seven flagships [1]. Under this flagship, several key initiatives had been outlined and implemented, including the Generic Office Environment (GOE), Electronic Procurement Project, Human Resource Management Information System (HRIMS), Project Monitoring System (PMS), Electronic Delivery Services (e-Services), Electronic Labor Exchange (ELX) and E-Syariah for the development of Syariah court [2]. Additionally, the government administration in general has been further modernized and many agencies had planned, launched, or implemented digitization and computerization programs [1][2]. Based on the United Nations E-Government Survey in 2010,[2] Malaysia's global ranking is placed at 32 out of 184, an improvement from 34th rank in the 2008 UN global survey. This also places Malaysia at the top six among the developing countries.

In order to support those e-government initiatives, the Malaysian parliament had gradually introduced some legislation such as Computer Crimes Act 1997, Telemedicine Act 1997, Digital Signature Act 1997, Copyright (Amendment) Act 1997, Communications and Multimedia Act 1998, Electronic Commerce Act 2006, Electronic Government Activities Act 2007 and Personal Data Protection Act 2010 [2][3].

The ultimate objective of this legal framework is to convince the public to utilize what technology has to offer to the governance and business as well as to provide legal certainty on the validity of computer-mediated transactions, digital documents as well as the legality of information assets. The laws are also expected to remove the greatest barrier or participation in e-government initiatives, namely the lack of trust and uncertainty as to the security of transaction within e-government processes [2]. Nevertheless, none of these laws was enacted particularly to counter the information theft in general, what more on the e-government security. This is because information theft has transformed tremendously in the digital environment to a myriad of acts and abuses not anticipated by the current legal framework. On this background, this paper aims to relook and reassess some of these laws to see how they may help address the threat of information theft, especially in the domain of e-government.

[1] See, http://go.worldbank.org/M1JHE0Z280 (accessed 9 December, 2011)

[2] See, United Nations E-Governmetn Survey 2010 at http://unpan1.un.org/intradoc/groups/public/documents/un/unpan038851.pdf

II. THE PROBLEM OF INFORMATION THEFT

Information theft (occasionally referred to here as "data theft") arises inevitably because the use of information technology (IT) has created an abundance of limitless digital data which have now assumed a new role not only as a business process tools, but also as the commodity itself [4][5]. Meanwhile, the role of individuals in this digital economy has been tremendously improvised thus opens up chances of abuses [6].

Information theft which is an illegal acquisition of the information assets (confidential data, information systems, data processes, etc.) comes in a myriad of modes and methods that evolve with time. This problem, if left unattended would cost the Government in so many debilitating ways; monetary losses, degraded national reputation, diminishing consumer trust, proliferation of crime and even disruption of public order and national security can be within the longs list of the implications to the country.

The consequence, though mostly non-obvious, is hardly trivial. It was reported that the information theft costs nearly US$48 billion annual costs for the businesses and an additional five billion per year for consumers in the United States of America in 2003. Meanwhile, in the same year the UK Home Office reported that the British economy suffered an annual cost of £1.7 billion due to the information theft [7]. More recently in 2008, Verizon noted that the total losses suffered in the US due to data theft were US$361 million [8]. Meanwhile Symantec Global Internet Security Threat Report in 2008 revealed that the Government was the top sector exposed to identity leaks, amounting to 60% among all sectors.

In Malaysia, according to the CyberSecurity Malaysia, in the year 2008 alone, there was reported a total of 2123 security incidents including online fraud, hacking, malicious programs, denial of service and intrusion. This is a 100% increase from the 1038 incidents reported a year earlier [9]. The figure had significantly increased in 2011 as shown in the Fig. 1.

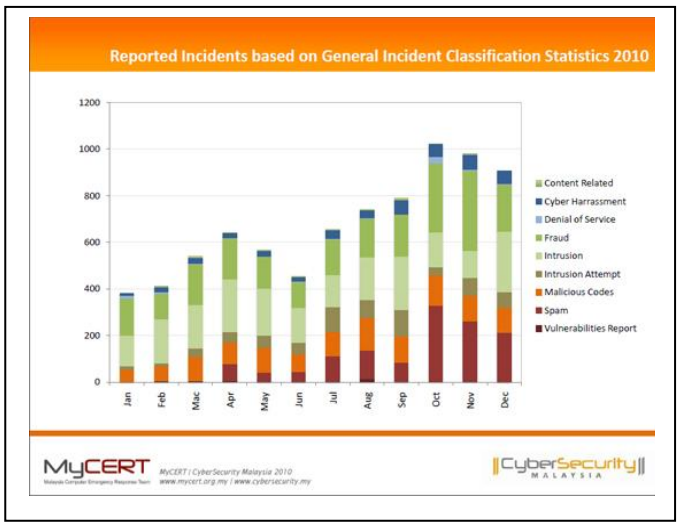

Figure 1. 2011 Information Security Incidents Report in Malaysia

III. E-GOVERNMENT AND THE CHALLENGES TO INFORMATION SECURITY

Information security is the protection of information and its critical elements, including the systems and hardware that use, store and transmit that information [10]. It involves three distinct but critical parameters in the form of confidentiality, integrity and availability objectives against threats that may come from internal and external sources in the form of, among others, inadvertent act, deliberate attack, technical failure, management failure as well as force of nature [10]. Based on this formula, this paper uses the framework in Fig. 2 to assess the requirements of e-government security.

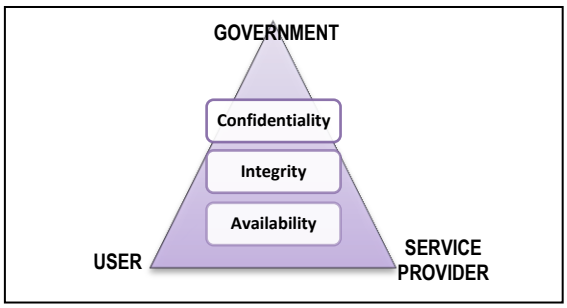

Figure 2. E-Government Security Framework

The threat of information theft mainly falls under such a 'deliberate attack' originating from either internal or external, though it is not rare that such attack is a consequence of an inadvertent incident such as the loss of laptops. This threat potentially compromises, weakens or defeats e-government initiatives. They can affect the users, i.e. citizens and the authority, who would grow doubts on the reliability of the system on which the e-government relies [11]. Unsurprisingly security breaches may become the weakest link in e-government processes as suggested by a study [12].

Based on its potential targets, information theft in the e-government activities can be categorized into at least three aspects: unauthorized intervention of information storage and processing devices; breach of official secret and confidential information; and theft of identity or personal data.

A. Intervention of Information Storage and Devices

E-government relies on the networked computers and devices for data processing as well as data storage. The security of these devices should therefore be protected. Under this category, it was revealed by the Symantec Global Internet Security Threat Report, that in 2007 the theft or loss of computer or other data-storage medium was the cause of most data breaches that could lead to identity theft, accounting for 57% of the total breaches as a result of high-profile case such as the data loss at the UK official revenue agency. Thus it is prevalent that the insecurity of e-government devices and computers can be the window for information theft and thus to the debilitation of e-government.

B. Breach of Official Secrets and Confidential Informaiton

Other than the security of devices, the integrity and confidentiality of the confidential data should be another point of concern. Apparently it is this confidential and valuable data

that would be the main target when people break e-government information system. An access to e-government information system may enable further acquisition of official data or secrets. The practice of stealing or disclosing secret documents and leaking the information contained in them to unauthorized persons is highly dangerous to the country. This is illustrated by the recent leaks of US secret cables through the Internet as solicited by the Wikileaks. Clearly any disclosure of those secrets may have a damaging impact to the government both at domestic politics and the international relations.

C. Theft of Personal Information (Identity Theft)

The threat to electronic government also comes from the theft of the personal information of individuals –which may include individual's credentials, passwords, social security numbers, credit card information, or other personal information. This is commonly known as identity theft. In the e-government processes, huge amount of personal data of the citizens are being gathered, stored, processed and disclosed. From national registry to taxation, from education to immigration, and from marriages and company registration, more and more personal data of individuals are processed – more increasingly in digital form. This is contentious issue in Malaysia recently as there were some incidents and allegations of identity theft implicating e-government process in Malaysia, including the individual information within the purview of the Ministry of Education, Land Registry Office as well as the National Registration Department [3].

IV. Reassessing E-Government Security Legal Framework in Malaysia

Given the challenges of the digital environment with the abundance of data as earlier noted, the role of legal framework becomes more prevalent. It is argued that government should ensure that adequate and effective legal infrastructure is in place. After all, e-government is not only a technical shift from the conventional way of running a government. Instead, it is a combination of technical, social as well as cultural shift and therefore technical control is not the only solution for e-government security [12]. Laws need to be strengthened to enable its enforceability in the digital environment thus to also secure the e-government processes. The development of a strong legal and regulatory framework on information security should facilitate the achievement of the objective of electronic governance and in securing official data and business processing. A significant success of e-government, despite the economy status, can be realized where there are enabling legal and regulatory frameworks in place, including specifically an e-government strategy [13].

Malaysia has in 2006 put forward its National Cyber Security Policy aiming for the protection of Malaysia's critical information infrastructure through the development of legal and regulatory frameworks. In line with this, continuous efforts need to be done to review, reformulate or reassess the adequacy of Malaysia's laws vis a vis threats to information security. This paper looks at the existing laws in three categories: (1) Electronic government functions and activities; (2) Criminal sanctions on information theft; and (3) privacy legal framework.

A. The E-Government Functions and Activities

The legality of functions, roles and activities of e-government in Malaysia is provided in the Electronic Government Activities Act ("EGAA") 2007. The Act seeks to provide for legal recognition of electronic messages in dealings between the Government and the public, the use of the electronic messages to fulfill legal requirements and to enable and facilitate the dealings through the use of electronic means and other matters connected therewith. Among others, it provides requirements of legal recognition of electronic message as well as its communication. The Act had come under criticism, among others, for being redundant and unnecessary [14]. This paper does not intend to debate on those articulate comments and analysis, but rather to assess it from a quite different angle, namely, information security.

One of the biggest break-through of the EGAA is the affirmation of a functional equivalence principle which seeks to accord legal recognition to certain new concepts pertinent to electronic transactions, so as to make them functioning equally as in the traditional concept of transaction. Such principle is evident from provisions dealing with the legal requirements of writing, signature, seal, witness, originality as well as electronic register. As an example, it is provided in section 10(1) that "Any information shall not be denied legal effect, validity or enforceability on the ground that it is wholly or partly in an electronic form." The break-through effect of this provision is certainly to instill the trust and confidence for any users of e-government that their transactions will be met by legal protection, and hence the peace of mind and security.

From information security perspective, it is noteworthy that many legal concepts of the functional equivalence in the EGAA are being *tied* with the requirement of system security. For example, section 10(2) provides that "Any information shall not be denied legal effect, validity or enforceability on the ground that the information is not contained in the electronic message that gives rise to such legal effect, but is merely referred to in that electronic message, *provided that the information being referred to is accessible to the person against whom the referred information might be used*." In other words, only when the data is accessible in its system, such data qualifies for the legal effect, validity and enforceability. In practice, a government agency would be able to rely on terms and conditions of e-government transaction stipulated in its electronic system if such information remains accessible to the user without alteration or modification. This 'accessibility' indicates that the purported user of the electronic message (i.e. the government agency) must make sure that there is in place and under his control a system from which an electronic message at issue can be accessed and available.

This "availability" is a crucial component of information security principles together with confidentiality and integrity [10]. Therefore in order to achieve the protection under many of the EGAA provisions, efforts must be made to ensure the information system is neither intruded nor compromised so that access not denied whenever it is required. The requirements of information confidentiality, integrity and availability can be found in other provisions of the EGAA dealing with various matters, as summed up in the Table 1.

TABLE I. SECURITY REQUIREMENTS IN THE EGAA 2007

Section	Matter	Security Requirements
10(2)	Legal recognition of electronic message	System availability
12	Requirement of electronic writing	System availability
13(2)	Requirement of electronic signature	System reliability, User confidentiality and data integrity
16(1)	Requirement of originality	System reliability, data integrity and availability

The requirements of system availability, system reliability as well as data integrity that are evident from some provisions of the EGAA seek to prevent information theft. This is because with such security requirements in place, the e-government system should be relatively safe, and anything less than that would amount to non-compliance. Although it is not conceivable to acquire hundred percent security at all time because security is a process rather than an outcome [15], at least the system is there to ensure a continuous effort and vigilance. Despite the loopholes, this EGAA could still provide certain safeguards for preventing or mitigating the threat of information theft in the e-government.

B. Penal Framework against Information Theft

In this section, the paper takes up what is left in the earlier. It was argued that the EGAA 2007 provides a good mitigating mechanism against information theft by ensuring the system is reliable, accessible and that the data remains unaltered. However, information theft is an attack that develops with the development of the technology itself. From time to time, we are bound to witness new ways to launch the attack. Recent reports had even showed that various computer intrusions can happen through enhanced deception or social engineering [16]. This means a preventive measure alone is not enough. There is a role to be played by law to punish the information theft and ensure the culprits do not come back to it. This role is to be played by cyber crime laws.

In Malaysia, the penal sanctions that deal with information security –but none on the crime of 'information theft' particularly– can be found mainly in the Computer Crimes Act ("CCA") 1997 and the Communications and Multimedia Act ("CMA") 1998. The following sections assess them in relation to the issue of information theft.

1) Computer Crimes Act 1997

The CCA 1997 is the first and main statute on computer crimes in Malaysia. It stipulates some computer-related offences, namely unauthorized access to computer material; unauthorized access with intent to commit or facilitate commission of further offence; unauthorized modification of the contents of any computer; wrongful communication of means of access; and abetments and attempts. Committing the above offences can trigger imprisonment, fines or both. The ultimate objective is to discourage, prevent and penalize any act or attempt of threatening and breaching the security of any given computer system (see, Table 2).

TABLE II. SECURITY OBJECTIVES IN THE CAA 1997

Section	Offences	Information Security Objectives
3(1)	Unauthorized access to computer material	Access security
4(1)	Unauthorized access with intent to commit or facilitate the commission of further offence	Access security
5(1)	Unauthorized modification to the contents of any computer	Data and content security
6(1)	Wrongful communication	Maintenance and operational security
7(1)	Abetments and attempts	Multiple aspects

As put up in Table 2, CCA deals with some crucial aspects of information security including the security of access to computer system under sections 3 and 4 and the secure maintenance of computer system as reflected in sections 5 to 7.

For an e-government system, this clearly mandates security management both on the users and system operators. Technologies need to be upgraded to restrict any unwarranted access and modification. Hence the need of managing passwords, identification numbers, encryption, access codes or any means of access. All these means of access are crucial to preserve the confidentiality and integrity of the information and the e-government system. One who maintains control over the means of access to his computer system is said to control the availability of an information asset. On the contrary, losing control over a means of access is equal to negating the availability of information and hence defeating the information security of the e-government.

2) Communications and Multimedia Act 1998

The Communications and Multimedia Act ("CMA") 1998 provides a regulatory framework to cater for the convergence of the telecommunications, broadcasting and computing industries. Unlike the CCA, this Act is more administrative than punitive. This law seeks to uphold the national policy objectives, namely among others, to ensure information security and network reliability and integrity. For this purpose, CMA criminalizes certain acts that pose threats to the information security, which is summed up in Table 3. Those penal sanctions serve some aspects of information security, namely: (i) network-related security; (ii) content-related security; (iii) communications security; and (iv) physical security.

TABLE III. SECURITY OBJECTIVES IN THE CMA 1998

Section	Offences	Information Security Objectives
232(1)	Fraudulent use of computer network facilities	Network security
233(1)	Improper use of computer network facilities	Content security
234(1)	Unlawful interception and disclosure of communications	Communications security
235	Damage to computer network facilities	Physical security
236(1)	Fraud and counterfeiting of access devices	Physical security

The fact that CMA addresses various security issues above is particularly useful to address the myriad threats of information theft in e-government. This is because information theft itself may take variety of forms and modus of operandi; ranging from network intrusion to sabotage, from fraud to impersonation, and from hacking to data interception.

C. Data Privacy Law

1) Introduction to Personal Data Protection Act 2010

Major legal issues on data privacy in Malaysia were resolved with the introduction of the Personal Data Protection Act (PDPA) 2010. Being the main legal framework for protecting data privacy of individuals, PDPA regulates the processing of personal data in commercial transactions and to provide for matters connected therewith.

Under section 4, "personal data" refers to any "data that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject." Meanwhile, "commercial transactions" mean "any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance."

The enactment of the PDPA is arguably a milestone for the development of e-commerce and e-government in Malaysia, considering that a massive and increasingly valuable amount of personal information are being stored, processed and exploited. However, there is a cause for concern here that the Parliament has expressly excluded the application of PDPA to the Federal Government and State Governments in section 3. Commentators opined that this exclusion would have a far-reaching implication in terms of the development of data protection law in Malaysia [17]. Nevertheless, it is argued that this law can still help protect the security of e-government in Malaysia in one way or another.

This paper argues that, based on its literal expression and the absence to any further qualification, the "exclusion" above concerns especially on the Government as an *entity*, but not on the e-government as an *activity*. It follows therefore, that if the e-government system and activities are operated directly by a government agency, the law does not apply. However, if such system is outsourced to any third party, notably and usually a private entity, such e-government system and activities shall be subject by the PDPA. Therefore, the PDPA still constitutes an important component in the legal framework to secure the Malaysian e-government.

2) Personal Data Protection Principles

At the heart of PDPA is a set of duties under the data protection principles from which stemming all the rights, duties and liabilities of each of data user and data subject ("data user" is those who use, collect, process, etc. the personal data that belong to certain individuals, i.e. the "data subject". There are generally seven categories of the duty spelled out in Table 4, whereas each of those principles contributes to the e-government security legal framework in Malaysia.

TABLE IV. PDP PRINCIPLES UNDER THE PDPA 2010

Section	Principle	Information Security Implications
6	General principle	No process of personal data which is excessive and/or without the consent of data subject.
7	Notice and Choice	Proper notification on the purpose of that data collection/processing
8	Disclosure	Prohibits unauthorized disclosure or sharing of personal data
9	Security	Imposes security measures by data users that commensurate the risk of security breach
10	Retention	Personal data shall not be kept unnecessarily
11	Data Integrity	Right of data subjects to correct and update their personal data
12	Data Access	Right of data subject to have an access to his own personal data the at the user's database

3) Offences of Information Theft under PDPA

While making contravention with any of the PDP principles above an offence punishable with a fine or imprisonment or with both, the PDPA also provides for several other offences directly related to the issues of information theft, though the phrase information theft itself is absent in the PDPA.

The most obvious provision under this heading would be the offence of unlawful collecting or disclosing of personal data (section 130). If any person is found to have knowingly or recklessly collected or disclosed personal data that is held by the data user without the consent of the latter commits an offence punishable with a fine of maximum MYR500,000 or with imprisonment for a maximum term of three years or with both. The same penalties await those who sell personal data under the same circumstances of the above. There is no specification as to the manner of such collection, disclosure or selling of the personal data. Instead PDPA leaves it open so as to be able to catch offenders in various ways or modus of operandi. In digital data environment such as the electronic government, fraud has used to cheat people so as to surrender their personal data. This provision, it is argued is useful in addressing those situations.

Another important provision of PDPA that can arguably help e-government security is the duty of data users such as those e-government service operators to conduct due diligence as to the reliability and security of their electronic system. This is because under section 133, board of director or any officer responsible for the management of the affairs in a body corporate may be charged for an offence by body corporate, unless if he can prove his absence of knowledge, and that he had taken all reasonable precautions and exercised due diligence to prevent the commission of the offence.

Given the above assessment, it can be said that the PDPA can lend a hand for the maintenance and protection of e-government security in Malaysia, albeit the fact that government will be excluded from its application.

V. CONCLUSION

The discussion above shows that information theft is popular due to the abundance of electronic and digital data created in the process of e-commerce and e-government. It arrives at some points; *firstly*, to ensure the sustainability and success of e-government in Malaysia (or any other country for that matter), it is paramount to put in place legal safeguards to protect its data and system from threats and attacks, especially the threat of information theft. *Secondly*, the role of law in addressing the issue of e-government security is enormous not only to prevent the threats, but also to provides incentives for the stakeholders to undertake those measures such as the due diligence duty under the PDPA.

This paper finds that the e-government security legal framework in Malaysia is still variably in the making with some significant provisions already in place, but yet under-utilized because they are largely untested in the court of law. Since the present paper focuses on the development of legal framework in terms of parliamentary statutes, the author recognizes there is a need to undertake further research in the future on how these laws have been variably applied and implemented in the courts, and what the challenges in their implementation are. Indeed, this legal framework as a whole needs a continuous assessment and reassessment because, after all, "security" is a continuous affair, not an end-state of things.

TABLE V. E-GOVERNMENT SECURITY LEGAL FRAMEWORK IN MALAYSIA

Statute	Main Features	Information Security Implications
EGAA 2007	The legality of electronic message and transactions in e-government	Requires confidentiality, data integrity and system accessibility as pre-requisite for the legality of transaction
CCA 1997	Criminalizes certain acts relating to the access and system maintenance	Safeguards access confidentiality, data integrity and system availability
CMA 1998	Criminalizes certain acts that pose a threat to information security	Declares information security, and network reliability& integrity as a national policy objective
PDPA 2010	Provides for the personal data protection principles and certain offences relating to personal data	Formulates sets of duties of data users in securing personal information that they collect and process

REFERENCES

[1] M. Ahmad and R. Othman, "Implementation of electronic government in Malaysia: The status and potential for better service to the public," Public Sector ICT Management Review, Vol 1(1), Oct 2006 - Mar 2007, pp.2–10.

[2] M. Rais Abdul Karim and N. M. Khalid, E-government in Malaysia. Kuala Lumpur: Pelanduk Publications, 2003.

[3] S. Zulhuda, "Information security in Malaysia: A legal framework for the protection of informaiotn assets," unpublished Ph.D. thesis, IIUM, 2010.

[4] J. H. Matsuura, A Manager's Guide to the Law and Economics of Data Network. Boston: Artech House, 2000.

[5] P. H. Rubin and T. M. Lenard, Privacy and the Commercial Use of Personal Information. Boston: Kluwer Academic Publisher, n.d.

[6] Yochai Benkler, The Wealth of Networks. New Haven: Yale University Press, 2006.

[7] K. Brimsted. "Data security breaches – Is Europe heading for US standards of openness?" Privacy and Data Protection, 1 Nov 2006 PDP 7 1(3).

[8] Verizon. "2011 data breach investigations report." <http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf>.

[9] Malaysia Computer Emergency Response Team (MyCert)'s official website at <http://www.mycert.org.my/en>.

[10] M. E. Whitman and H. J. Mattord, Principles of Information Security. Massachusetts: Course Technology, 2005.

[11] A. B. Munir and S. Zulhuda. "Becoming e-cities: Legal issues and challenges," Proceedings of the International Symposium on Knowledge Cities (2005), Madinah, KSA, pp.50-60.

[12] S. Kesar. "Is cybercrime one of the weakest links in electronic government? Journal of International Commercial Law and Technology, vol. 6(4), 2011.

[13] United Nations. "United Nations e-government survey 2010: Leveraging e-government at a time of financial and economic crisis," NY, 2010.

[14] A. B. Munir and S. H. M. Yasin, "Another law with flaws: Lesson never learnt," [2007] 4 CLJ xvii.

[15] B. Schneier, Beyond Fear: Thinking Sensibly about Security in An Uncertain World. New York: Copernicus Books, 2003.

[16] M. Jacobsson and S. Myers, Phishing and Counter Measures: Understanding the Increasing Problem of Electronic Identity Theft. New Jersey: John Wiley & Sons, Inc., 2007.

[17] A. B. Munir and S. H. M. Yasin, Personal Data Protection in Malaysia: Law and Practice. Petaling Jaya: Sweet & Maxwell Asia, 2010.