Adherence to ICT Security and Privacy Policies in Saudi Arabia

Khalid Almarhabi
Umm Alqura University
Makkah, Saudi Arabia

ABSTRACT
There is general agreement that 2015/2016 has been the period when major successful attacks on both private and public sector information systems have reached intolerable levels and response at the governmental and private sectors has become imperative. This study outlines how public enterprises can adopt effective, relevant and efficient security and privacy policies to meet citizens', legal, and government expectations and to comply with appropriate cybersecurity standards. This paper provides those involved in planning, designing, managing and implementing security and privacy policies with guidance for security issues relevant to their national situation. This study undertook a qualitative analysis of policies and strategy documents published in the selected countries to investigate and contrasts the various methodologies utilized to adhere to security and privacy policies. The situation in Saudi Arabia was analyzed in comparison to Australia and the United Kingdom. The primary result shows that public enterprises in Saudi Arabia needs to increase their efforts to adhere to security and privacy policies by ensuring the policies' readiness to be put into action, and they need to establish appropriate rewards and sanctions principles.

General Terms
Security and Privacy policies, Public enterprises, Saudi Arabia.

Keywords
Adhering, Security, Privacy.

1. INTRODUCTION
It is generally accepted that the period 2014/2015 has seen the most successful number of attacks on both private and public sector information systems; indeed it is now agreed that these attacks have reached intolerable levels, being up 200% compared to the previous year [1]. US President Obama has apparently recognised the importance of government systems and has allocated $14 billion to enhance the security and resilience of American government information systems. This paper addresses several problems: the increased level of information security attacks on Saudi Arabia that sees them in the top 20 of 213 countries being attacked [2, 3] and the lack of practicable security and privacy policies [4] in those nations. The paper reviews research done on this issue in those countries along with violations and abuse by some internal staff against these policies in Saudi Arabia.

In response to the government-sponsored enterprises security and privacy requirements for contemporary government information systems as described, for example, in the Developing National Information Security Strategy for the Kingdom of Saudi Arabia [5], the overall goal of this paper is to propose a feasible, practicable and sustainable solution to meet today's security needs and to protect public enterprises by using effective and efficient strategies to adhere to those security and privacy policies and international security standards. This paper provides those involved in planning, designing, managing and implementing security and privacy policies with guidance to adhere to relevant security and privacy policies.

This study undertook a qualitative analysis of policies and strategy documents published by selected countries, investigating the various methodologies utilised to adhere to security and privacy policies in Saudi Arabia and compared them with those of Australia and the United Kingdom. Saudi Arabia government cover critical infrastructures such as power, water and telecommunications even when they are private, government or mixed ownership organizations because they are all controlled by to government ministries. The limitation of this paper is that while it considers current versions of public documents available on the Internet to investigate and analyse security and privacy policies as well as how government-sponsored enterprises implement these policies, some countries may have security and privacy policies classified as secret/confidential documents that are not published. These are therefore beyond the scope of the study.

This research considers different types of security and privacy policies in Saudi Arabia. The term 'Policies' is described in the [6] as 'a way of doing something that has been officially agreed and chosen by a political party, business, or other organization'. However, Saudi Arabia does not have specific published laws or rules in this area and this caused difficulty for the research. These rules can be found in a range of sources such as Law of Government states, royal decree, the Ministry of the Civil Service and the Ministry of Communications and Information Technology.

The remainder of this paper is organized as follows: Section 2 describes cultural and societal differences; Section 3 compares citizens' expectations and how government-sponsored enterprises adhere to security and privacy policies; Section 4 presents the gaps and missteps in implementing policies in Saudi Arabia.

2. CULTURAL AND SOCIETAL DIFFERENCES
The purpose of this section is to give a general overview of Saudi Arabia, and how people and public enterprises define privacy. It is difficult to interpret the term "privacy" and give it a global definition because every country's understanding of it differs depending on customs, traditions, cultures, and the economic and social climate [7].

2.1 General Background about Saudi Arabia
Saudi Arabia, officially known as the 'Kingdom of Saudi Arabia (KSA)', is one of Gulf Region countries situated

in Western Asia. It is absolute monarchies, governed by large family. Arabic and Islam are the main language and religion of this country. From an economic perspective, along with the other countries in the Gulf Region, Saudi Arabia rely heavily on oil and provide two-thirds of the world's oil [8]. Thus, government security in relation to the world's biggest wellspring of crude oil resources is extremely important.

2.2 The Meaning of Privacy

Defining privacy is difficult. Various studies have attempted to offer a general definition of privacy. Westin [9], for example, defines it as 'the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behaviour to others'. Brandeis and Warren [10], on the other hand, defined privacy as 'the right to be let alone'. The concept of privacy in Saudi Arabia, where does not differ substantially from the intention of these definitions and also gives careful consideration to information privacy, which Westin [9] defines as 'the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'. As defined by Saudi Arabia's Ministry of Interior in its 'Basic principles of information security' document,'[Information is all] about the private life of the person and their identity, nationality, trends, tendencies, beliefs and banking and financial dealings; all of these data linked to specific person or person can be identified by definable information' [11]. The concept of privacy in Saudi Arabia has a meaning similar to other perspectives.

2.3 People's Perspectives

Saudi Arabian people care greatly about their personal physical privacy. This type of privacy can be defined as the individual's right to possess any physical thing that is considered to be confidential and that nobody has a right to see without the individual's permission; for example, people's bodies and anything in their houses. The focus in this paper is particularly on information privacy, about which many Saudi Arabian people seem to have few concerns. Al-senaidy et al. [12] state that almost three-quarters (74%) of Saudi Arabian respondents were not worried about their information privacy and generally did not change their default privacy settings on social network websites. Conversely, 68.8 per cent of United Kingdom respondents and 66 per cent of Australian respondents were quite worried about their information privacy [13, 14]. These statistics indicate a significant problem with Saudi Arabian people that could expose them to risk, unless their respective governments solve this issue by developing and adhering to security and privacy policies. Governments need to ensure that they adhere to security policies and laws to protect data and to comply with citizens' expectations. Very few studies have been done on this issue in Saudi Arabia [4], but a study indicated that three-quarters of government-sponsored enterprises in Saudi Arabia have security policies to secure citizen data [15]. This statistic suggests that the government's awareness with respect to citizen data is greater than that of the Saudi Arabian people themselves. In summary, Saudi Arabian people showed little concern about information privacy. As such this may readily extend to the actual integrity of that data but this aspect of overall security has apparently not been studied in the context of this paper.

3. COMPARISON OF ADHERENCE STRATEGIES

This section discusses and compares citizens' expectations about the privacy of their information as hosted by government-sponsored enterprises, as well as how government-sponsored enterprises adhere to policies governing the security of citizen data. This research focuses on some of the significant strategies that are published by selected countries to adhere to security and privacy policies. Saudi Arabia is compared to Australia and the United Kingdom in order to determine the gaps in adhering to security and privacy policies. To begin with, knowing the levels to which Saudi Arabia has progressed in digitising the public sector is essential for comparing their progress with that of developed countries, as is knowing the technical environment and status of all countries concerned.

3.1 Digitizing the Public Sector

One of the most important resources concerning the status of digitisation of government in each country is the United Nations E-Government Survey 2014. According to that report, Australia scored 'very high' (more than 0.75) on the E-Government Development Index (EGDI), with a score of 0.9103, and had the second highest rank after the Republic of Korea. The United Kingdom, with a very high EGDI score of 0.8695, was ranked eighth. Saudi Arabia scored 'high' (between 0.50 and 0.75), with EGDI scores of 0.6900. Saudi Arabia ranked thirty-sixth, out of 193 countries. Ranking for Saudi Arabia has increased slightly since 2012, by five places respectively [16]. An example of the progress made in these developing countries is that of Saudi Arabia, where the process to renew a passport can now be done online and the document obtained the next day in non-peak time. All other services can be accessed online through the Saudi portal website. Saudi Arabia has good positions in digitisation of governments; comparing them with the top countries will enhance the adhering of security and privacy policies in public enterprises

3.2 Citizen's Expectations

Citizens have several expectations concerning data hosting in government databases. With the proliferation of the Internet and the increase of cyber attacks through viruses, worms and other malware that bring so much risk to the privacy and security of citizens' data [17], citizens expect their data to be secure, accessible only by authorised people [18]. When government uses their data, citizens expect that it will be used in a right way according to the regulatory requirements of that country. Citizens expect that their data will be kept at all times in a secure place with high quality IT infrastructure, with regular maintenance [19]. In addition, citizen expectations may include that consideration that government could use novel and effective technologies in different fields to secure citizen data. From a legal perspective, citizens expect that laws and regulations spread across electronic government channels will contribute to protecting their data [20]. In short, whatever their nationality, citizens instinctively aim to protect their data and keep it secure, but, just as customs, traditions, and cultures differ, so do interpretations of the meaning of privacy and what it includes.

The next section will consider how government-sponsored enterprises ensure that they adhere to the rules surrounding citizen data security as citizens expect in Saudi Arabia, in comparison to those of Australia and the United Kingdom.

3.3 Government-Sponsored Enterprises Adherence

Adhering to security and privacy policies while meeting citizens' increased expectations means governments must have procedures which keep to the rules surrounding citizen

data security. Comparing countries will highlight the gaps. This comparison is made difficult when all three countries have different methods for implementing their security and privacy policies. Therefore, this comparison is organized according to readiness of policies, putting policies into actions, rewards and sanctions, and use of a computer emergency response team (CERT).

3.3.1 Readiness of Policies

Since this study is concerned with the problem of how to adhere to security and privacy policies, one of the most important steps is to prepare the policies; in other words, policies should be documented, accessible, updated and written clearly so that employees can follow the instructions they contain [21]. Otherwise, there is no way to adhere to such security and privacy policies. A search for policies in selected countries revealed that the privacy and security policies of Australia and the United Kingdom are easily accessible, updated regularly and available to all, which is the first step in adhering to privacy and security policies. For example, Australia has published privacy acts on the Office of the Australian Information Commissioner's website, which was last updated on the 30 October 2014 at the time of writing this paper [22]. This information is public and easy to find.

Continuous training of all staff on security and privacy policies is necessary for implementing and maintaining policies compliance, especially in the case of new staff [23]. Security and privacy policies should be updated periodically, and procedures should be in place for educating staff so that public enterprises do not fall behind and risk non-compliance. Saudi Arabia could benefit from developing the degree of readiness of Australian and the United Kingdom policies. It is a challenge to gather the information security and privacy policies in Saudi Arabia, regardless of adherence to them. The policies found were scattered, overly broad and not up to date. For example, some policies were collected from Law of Government statements, through royal decree, from the Ministry of the Civil Service and from the Ministry of Communications and Information Technology. Policies that employees are largely unaware of result from lack of readiness, with one study showing that almost half of the staff members in a particular Saudi Arabian department were unaware of the privacy policies relating to their own department [4]. This large percentage confirms that policies must be documented, accessible, updated and written clearly, and with training of staff in these countries.

3.3.2 Putting Policies into Action

One of the most important steps after providing policies is to convert those policies into measurable actions. Australia and the United Kingdom apply a particular process for implementing security and privacy policies, as shown on the websites of the Australian and the United Kingdom governments [24, 25]. This process is carried out by assigning each article of the policies to the relevant government department and then converting the articles to actions to be carried out by the staff [26]. These actions should be measurable, and there should be indicators to check the level of policy implementation. In this way, gaps in the policies' implementation can be ascertained and evaluated, and a responsible party assigned to deal with them. In addition, the establishment of a follow-up committee to check action implementation is also important. Such committees should be formed within each department, alongside a neutral external committee within government-sponsored enterprises. However, Alsulaiman and Alrodhan [4] have indicated that Saudi Arabian policies are not assigned to a specific department and are not linked with particular actions. Policies in Saudi Arabia are often considered in judicial proceedings by the Bureau of Investigation and Public Prosecution, but this method is not sufficient to implement those policies as required. Converting policies into measurable actions is one of the methods used by other countries to effect compliance with such policies.

3.3.3 Rewards and Sanctions

This implementation mechanism involves the principle of rewards and sanctions, a way of adhering to policies in public enterprises through effective liaison, punishing those who make mistakes and encouraging those who perform well. The 'rewards principle' has been defined as 'tangible or intangible compensation that an organization gives to an employee in return for compliance with the requirements of the information security policies' [27]. Australia and the United Kingdom use this principle, for example, as contained in the ACT Government Evaluation Policies and Guidelines [24]. One of the benefits of evaluation for public servants is that it improves their performance through rewards given when satisfactory levels of policies implementation have been achieved as described previously. This is difficult to assess without indicators to measure achievement levels.

Sanctions, on the other hand, is a way to curb the abuse and violation of policies that some people may be motivated to commit. The United Kingdom government's website, for example, lists penalties in its documentation on the 'Let property campaign', which also covers data protection [28]. Sanctions results from violation of this policies or low levels of policies implementation. Saudi Arabia is also working with this principle. Penalties are associated with many of their policies: for example, in Saudi Arabian anti-cyber crime law [29]. The principle of rewards works, but it is less practised than sanctions and perhaps this is due to gaps in the measurement of policy implementation in public enterprises. The principle of rewards and sanctions is one of the methods used to achieve compliance with security and privacy policies.

3.3.4 Computer Emergency Response Team (CERT)

Another practice aimed at adherence to privacy and security policies is the development of a computer emergency response team (CERT). This is the final step in protecting the data of citizens and responding in the case of a disaster or attack, or when something goes wrong in a department. It is vital for predicting the occurrence of disasters, developing emergency plans and training special response teams to protect data in order to adhere to policies and meet citizens' expectations. The IT emergency response team is tasked with ensuring that appropriate steps will be taken in order to recover any data that may have been lost in the disaster [30]. Each department should have an internal CERT, linked with a super external CERT, to deal with small issues very quickly. All the countries chosen for this study have taken positive steps to establish a CERT. The United Kingdom has a CERT and it is a member of the FIRST organisation which is 'a premier organization and recognized global leader in incident response' [31]. Membership in FIRST enables incident response teams to more effectively respond to security incidents by providing access to best practices, tools, and trusted communication with member teams'. Australia is also a member of FIRST and has two CERTs, CERTAustralia, own by government, and AusCERT for private and non-critical organisations. The response team is contacted every time there is a security breach within a department, in compliance with privacy and security policies.

4. STRATEGIES USE TO FACILITATE

The previous section explained some of the significant ways an enterprise can properly adhere to security and privacy policies in public enterprises. This research has found that Saudi Arabia government has a lack of readiness policies, putting such policies into action, and implementing principle of rewards and sanctions. This section proposes some main strategies to help Saudi Arabia government to solve gaps and missteps in implementing policies. Therefore, this section is organized according to budget and human resources, awareness and training program, trust supply chain, and evaluation of policies.

4.1 Budget and Human Resources

Government should support public enterprises with a budget, a basic management tool for creating, implementing, and evaluating security and privacy policies. The budget, includes staffing, training, and meeting all requirements for adherence to the policies, strengthens cyber security in each public enterprise. Knowing the number of employees and their abilities helps enterprises achieve objectives [32]. The most important roles in the implementation of security and privacy policies are those of the Chief Information Officer (CIO) or Chief Information Security Officer (CISO); these roles entail responsibility for information security, technology, and computer systems that support public enterprise goals. These roles are also vital for planning information and communications technology (ICT), managing resources, and ensuring overall implementation of security and privacy policies. According to De Borchgrave [33], CIOs are 'responsible for formulating an extensive corporate policies on information security issues. This officer would procure state-of-the-art technology, oversee employee training, compartmentalise employee access to various types of information based on the need to know, devise incentives, and hold "threat awareness" programs.' Results of a study done on CIO status show a low number of CIOs in a department in Saudi Arabia [34]. However, to provide the necessary tools for adherence to security and privacy policies, budgets, including staff, are required for every department.

4.2 Awareness and Training Program

IT people who work for the government, especially top managers such as CISOs, may lack any background in dealing with security threats. The level of awareness of information security in the governments of Saudi Arabia is very low [35, 36]. IT, technical and managerial staff who do not comply with today's security and privacy needs are a serious danger to public enterprises because they could expose them to risk. Education and training of employees is one of the best approaches to preserving security and privacy [37, 38]. Governments can adopt three solutions to resolve the problem. First, governments should support universities in providing some security courses and professional education for those involved in planning, designing, managing and implementing security and privacy policies in public enterprises. Second, each government position should have some policies related to qualifications and certifications to identify the requirements for that particular job. Third, each public enterprise should have an office or committee to provide training and ensure staff members adhere to security and privacy policies. The governments must increase the level of security and privacy awareness of their employees by providing education and training opportunities for them.

4.3 Trust Supply Chain

Policies specific to buying products through a supply chain are largely missing in security and privacy policies. The New South Wales government in Australia states that, in their Digital Information Security Policies, 'Security must be an integral consideration in information systems purchasing and maintenance'[39]. Parts of the supply chain could be used in attack, intruding on enterprises through supplied products. Risk from both such internal and external supply chains must be controlled by policies and agreement. Policies should include all procurement steps, starting with a plan to identify needs and followed by choosing a method of procurement. These steps are then reviewed for internal approval by evaluation criteria before moving to implementation, which includes the agreement. The final step is analysis, which involves evaluation and monitoring of the entire process and all products. Agreement can be forged through different avenues such as contract negotiation and diplomatic procedures to achieve trust with the supply chain. The ISO/IEC 27002 contains the required aspects for an agreement with the supply chain concerning security and privacy. The most important aspect is defining information security and privacy requirements that apply to supply chain products. Another aspect is implementing an auditing process for the accepted method of delivery when products are found to be compatible with security and privacy requirements. Implementing this process is vital for identifying each component of that product and ensuring there are no unwanted or unexpected features. The final aspect is implementing a security risk management plan for each component of that product [40]. If the policies does not reflect an acceptable design document in reality, there will be no benefit from its use. Public enterprises in Saudi Arabia need security and privacy policies to ensure trust in the supply chain prior to buying products. In Saudi Arabia, for example, the Government Tenders and Procurement Law does not include security and privacy issues [41], which constitutes a threat to government-sponsored enterprises. While there are some discretionary instructions within some ministries about security of suppliers, they do not adhere to strict policies. Public enterprises must have security and privacy policies in place to be able to trust the supply chain through all steps of procurement.

4.4 Evaluation of Policies

Another missing step to ensure implementation of security and privacy policies is proper evaluation of these policies. Evaluation refers to 'the process of measuring and assessing the impacts and merits of government policies, strategies, and programs. It is a means of determining the appropriateness, effectiveness, and efficiency of government policies and programs and contributing to policies improvements and innovation' [24]. This basic component of the policies implementation cycle is required to benefit governments and citizens. Evaluation can assist decision making, improve quality of policies and performance, increase trust in government, achieve government goals, and more. The first step involved in evaluation, as shown in The Magenta Book: Guidance for Evaluation [25], is defining policies goals, intended outcomes, audience, and evaluation objectives. After identifying the evaluation techniques and data requirements, the basic resources and government arrangements need to be determined before doing the evaluation. The final step in the process is assessing the evaluation and using its findings. Measurable results by indicators that change the theory to numbers as practised are fundamental by any approach and techniques. However, when parliamentary authorities in Saudi

Arabia has previously enacted policies, they have made judicial authorities the reference in case of non-implementation, rather than adhering to a scientific principle to measure results, such as with the Anti-Cyber Crime Law in Saudi Arabia [29]. This step was good, but not good enough to evaluate and implement security and privacy policies; however, it should provide indicators for measuring implementation. For example, Article Four in the Anti-Cyber Crime Law in Saudi Arabia refers to 'Illegally accessing bank or credit data or data pertaining to ownership of securities with the intention of obtaining data, information, funds or services offered' [29]. The needed measurements can be procured by reviewing the number of complaints received by the police or the bank, or by 'impact,' such as an overall decrease in the number of complaints in a year versus the previous year. This example makes the article measurable, increases knowledge at the level of implementation, and sets guidelines for applying the principles of sanctions for abuse or rewards for achievement. For example, a bank may increase its level of safety because it helps reduce the crime rate. Evaluation and measurable results are essential steps for implementing security and privacy policies in public enterprises.

5. CONCLUSION

This paper has explained how public enterprises in Saudi Arabia can ensure adherence to relevant security and privacy policies to meet citizen, legal, and government expectations and to secure data from prospective opponents by comparing their methods of adherence with those of Australia and the United Kingdom. This paper provided guidance on security issues for those involved in planning, designing, purchasing, managing, and implementing security and privacy policies. The primary result of the study confirms that the security and privacy policies of public enterprises in Saudi Arabia should be documented, accessible, updated, and written clearly so that employees can properly follow the instructions they contain. Saudi Arabia public enterprises must convert those policies into measurable actions by assigning each article of the policies to the relevant government department and then converting the articles to actions to be carried out by the staff. The principles of rewards and sanctions should also be applied for proper adherence to security and privacy policies. The government should support public enterprises with budgets that include staffing, training, and other variables needed to meet all their requirements. Evaluation is another important concept to ensure proper implementation of security and privacy policies, including all procurement steps.

6. REFERENCES

[1] Patel, A., Network performance without compromising security. Network Security, 2015. 2015(1): p. 9-12.

[2] Kaspersky Website. Kaspersky security bulletin 2014. 2014; Available from: http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2014/12/Kaspersky-Security-Bulletin-2014.-Overall-statistics-for-2014.pdf.

[3] Mcafee Website. Estimating the global cost of cybercrime. 2014; Available from: http://www.mcafee.com/au/resources/reports/rp-economic-impact-cybercrime2.pdf.

[4] Alsulaiman, L.A. and W.A. Alrodhan, Information privacy status in Saudi Arabia. Computer and Information Science, 2014. 7(3): p. p102.

[5] Ministry Of Communications and Information Technology, Developing national information security strategy for the kingdom of Saudi Arabia, Editor. 2011.

[6] Longman Dictionary. Policy definition,. Available from: http://www.ldoceonline.com/dictionary/policy.

[7] The United Nations Educational Scientific and Cultural Organization. What is privacy. in The right to privacy. 1970. Paris.

[8] Appenzeller, T., The End of Cheap Oil. 2004, National Geographic Society: Washington. p. 80.

[9] Westin, A.F., Privacy and freedom. 1967.

[10] Brandeis, L. and S. Warren, The right to privacy. 2014: RL Van Bruggen.

[11] Ministry of Interior, The basic principles of information security, Ministry of Interior in Saudi Arabia, Editor. 2001. p. 7.

[12] Al-senaidy, A.M., T. Ahmad, and M.M. Shafi, Privacy and security concerns in SNS: a Saudi Arabian users point of view. International Journal of Computer Applications, 2012. 49(14).

[13] Virkki, J. and R. Aggarwal, Privacy of wearable electronics in the healthcare and childcare sectors: a survey of personal perspectives from Finland and the United Kingdom. Journal of Information Security, 2014. 2014.

[14] King, T., L. Brankovic, and P. Gillard, Perspectives of Australian adults about protecting the privacy of their health information in statistical databases. International Journal of Medical Informatics, 2012. 81(4): p. 279-289.

[15] Alqathbar, K. and A. Alsubah, Information security status in kingdom of Saudi Arabia. Information Studies, 2012. 14: p. 195.

[16] The United Nations, United Nations e-government survey. 2014: New York. p. 15 - 33.

[17] Kearns, I., Public value and e-government. 2004: Institute for Public Policy Research.

[18] Jorgensen, T.B. and B. Bozeman, Public values an inventory. Administration and Society, 2007. 39(3): p. 354-381.

[19] Karunasena, K., An investigation of the public value of e-government in Sri Lanka. 2012, RMIT University Melbourne, Australia.

[20] Karunasena, K. and H. Deng, A revised framework for evaluating the public value of e-government. 2011.

[21] Wood, C.C. and D. Lineman, Information security policies made easy version 11. 2009: Information Shield, Inc.

[22] Office of Australian Information Commission, Privacy act 1988. 2013. p. 1.

[23] Pahnila, S., M. Siponen, and A. Mahmood. Employees' behavior towards IS security policy compliance. in 40th Annual Hawaii International Conference on System Sciences. 2007. IEEE.

[24] Australian Capital Territory Chief Minister's Department, ACT government evaluation policy and

guidelines, Australian Capital Territory Chief Minister's Department, Editor. 2010: Canberra.

[25] Her Majesty's Treasury, The magenta book: Guidance for evaluation. 2011.

[26] Hallsworth, M., S. Parker, and J. Rutter, Policy making in the real world. London: Institute for Government, 2011.

[27] Bulgurcu, B., H. Cavusoglu, and I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 2010. 34(3): p. 523-548.

[28] Her Majesty's Revenue and Customs. Guidance let property campaign: your guide to making a disclosure. 2013; Available from: https://www.gov.uk/government/publications/let-property-campaign-your-guide-to-making-a-disclosure/let-property-campaign-your-guide-to-making-a-disclosure.

[29] Bureau of Experts at the Council of Ministers, Anti-cyber crime law, Official Translation Department, Editor. 2007. p. 4.

[30] Bada, M., et al., Computer Emergency Response Teams (CERTs) an overview. 2014.

[31] The FIRST Steering Committee. FIRST vision and mission statement. 2003; Available from: http://www.first.org/about/mission.

[32] Berke, P., et al., What makes plan implementation successful? An evaluation of local plans and implementation practices in New Zealand. Environment and Planning B Planning and Design, 2006. 33(4): p. 581.

[33] De Borchgrave, A., Transnational crime the new empire of evil. Strategy & Leadership, 1996. 24(6): p. 27-31.

[34] Altameem, T.A., The critical factors of e-government adoption: an empirical study in the Saudi Arabia public sectors. 2007.

[35] ALArifi, A., H. Tootell, and P. Hyland. A study of information security awareness and practices in Saudi Arabia. International Conference in Communications and Information Technology (ICCIT), 2012. IEEE.

[36] El-Haddadeh, R., et al., E-government implementation challenges: a case study. 2010.

[37] Puhakainen, P. and M. Siponen, Improving employees' compliance through information systems security training: an action research study. Mis Quarterly, 2010. 34(4): p. 757-778.

[38] Yoo, J., Comparison of information security controls by leadership of top management. Journal of Society for e-Business Studies, 2014. 19(1).

[39] The Department of Premier and Cabinet, Digital information security policy. 2012. p. 5.

[40] The International Organization for Standardization, ISO/IEC 27002: Information technology -- Security techniques -- Code of practice for information security controls. 2013.

[41] Bureau of Experts at the Council of Ministers, Government tenders and procurement law minister of finance, Editor. 2009.