5-2012

Information Security Awareness in Saudi Arabia

Abdulaziz ALArifi
University of Wollongong, aaa296@uowmail.edu.au

H. Tootell
University of Wollongong, holly@uow.edu.au

Peter Hyland
University of Wollongong, phyland@uow.edu.au

Information Security Awareness in Saudi Arabia

Abdulaziz ALArifi
University of Wollongong
aaa296@uowmail.edu.au

Holly Tootell
University of Wollongong
holly@uow.edu.au

Peter Hyland
University of Wollongong
phyland@uow.edu.au

Abstract

While the Web, cell phone 'apps' and cloud computing put a world of information at our fingertips, that information is under constant threat from cyber vandals and hackers. Although awareness of information threats is growing in the Western world, in places like Saudi Arabia, information security is very poor. Unlike Western pluralistic democracies, Saudi Arabia is a highly-censored country, with a patriarchical and tribal culture, which may influence its poor information security rating. This paper examines the level of information security awareness (ISA) among the general public in Saudi Arabia, using an anonymous online survey, based on instruments produced by the Malaysian Cyber Security Organization and KPMG. The survey attracted 462 respondents and the results confirmed that ISA in Saudi Arabia is extremely low. Several of the areas of weakness in ISA appear to be related to the level of censorship or the patriarchical and tribal nature of Saudi culture.

Keywords

Information security, Information security awareness, Information systems, Information security management

1. Introduction

The World Wide Web, mobile computing, and Cloud Computing provide a wide range of information, anytime, anywhere (Afyouni 2006). However, such technologies also allow new opportunities for "cyber vandals" to misuse or destroy information (Bragg et al. 2004) using techniques such as viruses, hacking or denial of service (DoS) attacks (Easttom 2006).

To overcome these threats, it is essential for both information providers and information users to have good Information Security practices, which ensure the availability, integrity and confidentiality of information (Turban et al. 1996; Stallings & Brown 2008; Whitman & Mattord 2008). However, before Information Security practices become routine, there must be an appropriate level of Information Security Awareness (ISA), in which information users are aware of the information risks, and understand the power of both physical and non-physical information security (Siponen 2000; Kruger et al. 2010). It has been demonstrated that a high-level of ISA can reduce information risks and increase information security performance (Siponen 2000).

Although this is generally well-understood, some countries, for example, China, Russia and Saudi Arabia, have incredibly high levels Information Security attacks. Unfortunately, high levels of Information Security attacks in these countries create increased risks for those countries with better security practices because weaknesses in security anywhere lead to faster rates of disseminations of viruses and provide 'easy targets' from which to launch DOS attacks on businesses around the world. So, it is important for information security throughout the world to understand what causes the high level of attacks in these countries. This paper focuses on Saudi Arabia and has two aims: i) to determine if there is a relationship between the high risk levels in Saudi Arabia and the level of ISA among the general population and ii) to identify mechanisms that could improve ISA.

2. Background of study

Information is now regarded as a valuable if not vital commodity. However, this valuable commodity is under constant threat. Information threats can be broadly categorised as natural disasters or human attacks, such as virus attacks, hacking or other intrusions, and denial of service (DoS) attacks (Easttom 2006). The risk of natural disasters can be mitigated by storing redundant copies of information in widely dispersed locations so that the risk of all copies being destroyed or damaged is incredibly low.

It is the human attacks that pose the greatest risk because these attacks are intentional and the mechanisms for conducting such attacks become more sophisticated every day. Moreover, human attacks typically rely on some other unsuspecting human agent allowing the attack. Virus attacks rely on people opening email attachments or using contaminated portable devices on multiple computers. Hackers rely on people leaving computers with inadequate passwords. DoS attacks use computers unprotected by firewalls as intermediaries to send billions of bogus transactions to a targeted computer, thereby making it unable to carry out its intended purpose.

To reduce the incidence and severity of human attacks, it is necessary to raise the level of ISA within a specific organisation or in the general public. Information Security policies and procedures are commonplace in most organisations, and seek to give employees clear guidelines on what they should or should not do to ensure the security of corporate information. The general public, too, is becoming more aware of many information security threats. However, that is not the case throughout the world. In 2010 and 2011, the Kaspersky Lab, a highly-respected Information Security specialist, reported the following statistics about the top 20 targeted countries around the world which had Information Security attacks. Table 1 represents 86.3% of the known information attacks by country in 2009 and 82% in 2010.
To understand these statistics we must realise that the number of attacks, to some extent, depend on the number of people using computers and the Internet. Thus, Italy has more than double the attacks that Thailand does, even although they have similar populations. However, Italy has nearly double the rate of Internet use that Thailand does, and so more attacks.
Once the rate of computer/Internet use is considered, three countries stand out: China, Russia and Saudi Arabia, all of which have far higher rates of attack than their level of computer/Internet use would suggest. While the cases of China and Russia are fascinating, their sheer size and, in the case of China, multiple languages makes it difficult to study, so this paper focuses only on the reasons that Saudi Arabia is so prone to information attack. Saudi Arabia has around 9,600,000 internet and computer users in 2009 and around 11,400,000 users in 2010. Saudi Arabia received 1.81% of the attacks in 2009. So, Saudi Arabia accounts for only 0.002 % of the internet users in the world, which is far less than the

percentage of attacks they experienced. In 2010 Saudi Arabia has nearly the same percentage of attacks 1.77% which prompts questioning regarding the reasons for this.

2009			2010		
No.	Countries	Attack %	No.	Countries	Attack %
1	*China*	*46.75%*	*1*	*China*	*19.05%*
2	*USA*	*6.64%*	*2*	*Russia*	*17.52%*
3	*Russia*	*5.83%*	*3*	*USA*	*10.54%*
4	*India*	*4.54%*	*4*	*India*	*5.56%*
5	*Germany*	*2.53%*	*5*	*Germany*	*3.16%*
6	*Great Britain*	*2.25%*	*6*	*Ukraine*	*2.66%*
7	*Saudi Arabia*	*1.81%*	*7*	*Vietnam*	*2.60%*
8	*Brazil*	*1.78%*	*8*	*Great Britain*	*2.56%*
9	*Italy*	*1.74%*	*9*	*France*	*2.55%*
10	*Vietnam*	*1.64%*	*10*	*Italy*	*2.39%*
11	*Mexico*	*1.58%*	*11*	*Spain*	*2.06%*
12	*France*	*1.49%*	*12*	*Saudi Arabia*	*1.77%*
13	*Egypt*	*1.37%*	*13*	*Malaysia*	*1.62%*
14	*Turkey*	*1.23%*	*14*	*Turkey*	*1.60%*
15	*Spain*	*1.2%*	*15*	*Brazil*	*1.49%*
16	*Ukraine*	*0.91%*	*16*	*Mexico*	*1.47%*
17	*Canada*	*0.81%*	*17*	*Canada*	*1.31%*
18	*Malaysia*	*0.8%*	*18*	*Thailand*	*1.15%*
19	*Thailand*	*0.76%*	*19*	*Poland*	*1.09%*
20	*Kazakhstan*	*0.71%*	*20*	*Egypt*	*1.02%*
	Total	*86.37%*		*Total*	*82%*

Table 1: Incidence of Information Attacks – the Highest 20 Countries (Kaspersky Lab 2010, 2011)

Initially, it might be thought that some aspects of Saudi Arabian culture could explain the high level of Information Security attacks.

Saudi Arabia is a highly-censored society. Both China and Saudi Arabia are subject to all three of the major types of filtering (Deibert et al. 2008), namely, political, social and security/conflict filtering. However, censorship alone cannot explain the large number of attacks in Saudi Arabia because Iran has the same types of censorship and a far higher rate of Internet use than either Saudi Arabia but it doesn't even rate in the top twenty countries for information attack. Perhaps it is some combination of culture and censorship that makes Saudi Arabia prone to attack.

Given our focus on Saudi Arabia, it is necessary to know a little about the country and its people. Saudi Arabia is one of largest countries in the Middle East with 26 million

inhabitants, 99% of whom are Muslims. It is an oil rich country and the income from oil subsidises a welfare state controlled by the government, which is dominated by the royal family, which numbers many thousands and controls most of the kingdom's important posts (Library of Congress 2006). The Islamic religion plays a huge part in Saudi life and politics, and all the decisions made by the king must be consistent with Islamic law. Saudis consider religion as the most important element of their identity (Moaddel 2006). The Saudi's interpretation of Islamic law severely constrains the roles of women, and the mixing of the sexes is actually prohibited outside the family. The country is also strongly patriarchical. Hofstede (2009) describes Saudi Arabia as:

"highly rule-oriented with laws, rules, regulations, and controls in order to reduce the amount of uncertainty"

Tribes are one of the most influential factors in Arab life especially in the Arabian Peninsula. Reflecting their Bedouin heritage, a person's tribe offers protection from other hostile tribes or foreigners. While the tribes within Saudi Arabia are no longer hostile to one another, a person's tribe is still seen as a source of security (Alhagil 2001; Alothimin 2009). This strong tribalism may also have a direct effect on the level of ISA. Hofstede (2009) observed of collectivisit cultures like Saudi Arabia have:

"close, long-term commitment to the member 'group', [i.e.] a family, extended family, or extended relationships. Loyalty … is paramount, and over-rides most other societal rules."

However, there is little or no evidence in the literature of any previous studies of the level or causes of ISA among the Saudi general public. So, this research addresses the questions: i) is there a relationship between the high risk levels in Saudi Arabia and the level of ISA among the general population? ii) does the level of ISA depend on Saudi Arabia's highly-censored, patriarchical, tribal culture? iii) what mechanisms might help address low levels of ISA?

3. Methodology

While our understanding of ISA in Saudi Arabia is very poor, the concept of ISA is well-defined in the literature and several excellent survey instruments exist for assessing ISA. Since this study seeks to gather data from as large a sample of the Saudis as possible, a survey is an ideal data gathering technique (Creswell 2003; Hancock & Algozzine 2006). An online survey is particularly effective over long distances and is well-suited to Saudi culture because women in Saudi Arabia can not speak to men who are not relatives. Consequently, an online survey can gather a large sample of both men and women in a short time without any ethical problems.

The survey questions were selected from instruments developed by the Cyber Security Organization in Malaysia and Klynveld Peat Marwick Goerdeler (KPMG). All of the survey questions from either survey were included unless they would have been inappropriate for the Saudi culture.

The questions in this research were 32 semi-closed questions that combine the advantages of closed-ended questions and open-ended questions. The survey was translated into the Arabic language because the participants are all from Saudi Arabia. The initial survey was subjected to pilot testing by Saudis who were fluent English speakers to ensure both the validity of the questions and the accuracy of their translation into Arabic. Pilot test participants strongly recommended making all questions optional as they believed that many Saudis would simply stop answering the questions if they encountered a compulsory question that they did not want to answer. The survey questions were then uploaded to Survey Monkey with all questions being optional. The survey was accessible via online links placed on popular Saudi

educational and business websites and forums with a letter that informs potential participants about this study with a clear announcement that it is to be completed by "only Saudi Arabian people". This worked well, resulting in 462 responses from adults.

4. Results

Although there were 462 respondents in total, the number of responses to each question varied significantly because all of the questions were optional (see above). An inspection of the data suggests that there is no systemic reason for non-completion i.e. no particular group of respondents chose not to answer particular sets of questions. Even although the non-response rate was sometimes as high as 50%, there were still over 300 respondents for every question, which is sufficient for the purposes of this research. However, the non-response rate itself is interesting; given the high level of censorship of the Internet in Saudi Arabia, it is possible that Saudis are not familiar with online surveys or the expectation that all questions should be answered.

Responses were in 2 main groups: information security issues, and preferences for information dissemination.

4.1 Information security issues

The first question asked if respondents physically secured their portable computer devices (e.g. laptops, mobile phones etc). Only 29% of 458 respondents indicated that they kept their portable devices in secure places all the time. A further 43.1% of respondents sometimes secure their devices, and 22.7% of respondents never secure their devices. So there is a surprising lack of care for these devices or the information they contain.

The second question asked if respondents secured their devices using login passwords. 55.2% of 458 respondents used passwords to login into their devices but 39.7% do not.

Hackers have a range of techniques for guessing or cracking passwords. Short or weak passwords or passwords containing personal identification, such as name or date of birth, allow hackers to crack passwords easily. However, strong passwords composed of more than 8 characters including a mixture of numbers, upper and lower case letters and special characters are far more difficult to crack.

Table 2 indicates how secure the respondents' passwords are. 45% (N=159) of 352 respondents have passwords less than 5 characters and 49% (N=173) between 5 and 8 characters. Neither of these is very secure. Conversely, 111 respondents have passwords of more than 8 characters. The multi-part nature of the question allowed respondents to indicate specific characteristics of their passwords e.g. use of capital letters etc. Table 2 shows that the use of capital letters (N=91, 25%) and special characters (N=105, 29%) is significantly less than those using small letters (N=145, 41%) or numbers (N= 272, 77%). This is unfortunate as the use of capital letters or special characters significantly improves password strength. At first, the use of numbers in passwords seems positive, as the inclusion of numbers greatly strengthens a password. However, anecdotal evidence suggests that many Saudis use **only** numbers, specifically their mobile phone numbers or date of birth. The structure of this question does not allow us to say definitively, but it appears that many of the numerical passwords up to 8 characters (N= 210, 59%) are mobile numbers or birthdays and therefore are among the most ineffectual passwords.

In addition to having a strong password, passwords should be changed regularly. Amazingly, 65.7% of 353 respondents have never changed their passwords. This is a major security risk.

In comparison, a South Africa study, reported that only 27.3% of respondents have never changed their passwords (Kruger et al. 2010).

How secure is your password? (Select more than one column if applicable) (N = 352)					
	Capital letters	Small letters	Numbers	Special Characters	Count (N)
Less than 5 characters	*17*	*27*	*113*	*26*	*159*
5 to 8 characters	*34*	*78*	*97*	*40*	*173*
more than 8 characters	*40*	*40*	*62*	*39*	*111*

Table 2: Strength and Characteristics of Participants' Passwords

It appears that Saudis are either unaware of the value of strong passwords that are changed regularly or simply don't see it as their responsibility. This abrogation of responsibility is reflected in later responses and may be associated with a patriarchical society in which "those in charge" are responsible and individuals are not. In either case it indicates a low level of ISA. Even more alarming is that systems administrators in Saudi Arabia do not appear to be aware of this problem either; otherwise systems would automatically force users to select strong passwords and to change passwords regularly.

Responses showed that 35.8% of 363 respondents shared their access passwords with family members. In comparison, one South Africa ISA study (Kruger et al. 2010) found that password sharing is close to 0%. Kruger et al. (2010) also reported that 22.7% of respondents would share a password with a system administrator. In Saudi Arabia, this value was only 0.6%, which raises the question, why share with family members but not with other responsible people outside the family. The high level intra-familial password sharing may be linked to the Saudi's tribal culture in which members of the tribe are seen as trustworthy but those outside the tribe are not. Regardless of the association with tribal culture, the security risk associated with password sharing is serious. Indeed, it hardly matters how strong your password is or how often you change it if you give it away to others. Table 3 shows the respondents' awareness of some of the main information threats and, as might be expected, awareness of virus attack and spam emails was high. However, only 7.4% of 462 respondents are aware of DoS. Coincidentally, the threats of vulnerability probing, harassment, cyber bullying, and cyber stalking were only familiar to about 19% of respondents, while awareness of system intrusion was slightly higher (20.8%). Only 25.5% of respondents were aware of the risk of identity theft.

Have you heard of and are aware of the existence of the following threats? (N = 462)					
	Percent	Count (N)		Percent	Count (N)
Virus or malware	*87.2%*	*403*	*System intrusion*	*20.8%*	*96*
Spam emails	*57.8%*	*267*	*Cyber stalking*	*19.7%*	*91*
Phishing	*29.7%*	*137*	*Vulnerability probing*	*18.8%*	*87*
Fraud and forgery	*28.8%*	*133*	*Harassment or cyber bullying*	*18.6%*	*86*
Identity theft	*25.5%*	*118*	*Denials of services (DoS)*	*7.4%*	*34*

Table 3: Respondents' Awareness of Information Threats

Faced with a number of different information security threats, a wise computer user has a number of security mechanisms at hand. The following question asked participants which type of security mechanism they used. Given the high level of awareness of viruses shown in Table 3, it is not surprising that over 86% of 452 respondents use antivirus software. However, probably because they are unaware of the other potential threats, the use of all other protection mechanisms is far lower. From 452 respondents only 16.2% use internet security software, 13.9% use anti-spam and 10.4% use anti-spy software. It is interesting to note that the use of protection is in all cases lower than the awareness of threats. For example, over 25% of respondents in Table 3 are aware of fraud and identity theft but only 16.2% of respondents use internet security. It appears that we have two related problems: lack of awareness of the threat and lack of appropriate response. It is still unclear whether the lack of response is because Saudis do not know what the correct response is or whether they simply don't think the response is warranted.

Of course, it is not enough simply to install protection software; one must also keep it up to date. The next question asked about the frequency with which either freeware and licensed protection software was updated.

Amazingly, over 53% of 462 respondents of either freeware or licensed protection software have not upgraded their software in more than 3 months. Possibly the cost of upgrades is a contributing factor. However, upgrades to freeware are free, but participants still did not upgrade that software either.

ISA also requires people to be aware of their own role in the propagation of risks. Sometimes this is done via email, especially when people have a private email account which they use for both private and work purposes, thereby seriously increasing the risk to an employer's organizational network. Responses indicate that 67.7% of 462 respondents use their private web mail for professional purposes at least sometimes and 21% use private mail for business purposes frequently or everyday. This represents a serious security risk to most Saudi businesses.

Should an information attack damage or destroy data, one can often use a backup to restore the lost data. So, even if Saudi's are not good at protecting their data, perhaps their backup procedures will provide a fall-back position. Unfortunately, Table 4 clearly shows that 43.9% of respondents have never done a backup of their data. Only 17.8% do a backup frequently or everyday, so over 80% of participants have an ineffective backup procedure which places them enormously at risk.

How often do you back up your sensitive / critical data? (N = 462)					
	Percent	Count (N)		Percent	Count (N)
Never	*43.9%*	*203*	*Frequently*	*15.2%*	*70*
Sometimes	*38.3%*	*177*	*Everyday*	*2.6%*	*12*

Table 4: Data Backup Use

Reporting security incidents is important as it allows users to find better protection solutions, and also allows security providers to reduce the likelihood of similar Information Security incidents in the future. Unfortunately, responses show that 80.5% of 462 respondents are not aware how or where they can report security incidents. This low awareness of appropriate responses, would reduce the speed with which threats could be dealt with and hamper overall Information Security across the country.

The final question in this section asked if participants felt that privacy was important when online. Protecting online privacy is important in itself but it is also vital in avoiding identity theft. Given that Saudi culture emphasises the idea that a person is only safe within a family or tribe and that women in particular are required to maintain a high level of physical "privacy" e.g. the wearing the veil and only being able to travel if accompanied by a male family member, we might expect that privacy would be a big issue for Saudis. Indeed, it is, with the vast majority (91%) of respondents either agreeing or strongly agreeing that online privacy is important. Unfortunately, although it is important, much of the previous data suggests that Saudis do not know how to ensure their online privacy.

While much of the previous data suggests that lack of knowledge gives rise to Information Security risks, another explanation might be that the Saudi's patriarchical culture does not encourage Saudis to take responsibility for themselves. Participants were asked who was responsible for their digital privacy and were allowed to nominate more than one person or agency. Responses show that 67.6% of 429 respondents believed that they were responsible for their own privacy. However, 22.8% also believed that the government was responsible, reflecting their patriarchical culture. Similarly, 35.2% of respondents believed that the company that had their digital information was responsible for its security. It is possible that the tribal nature of Saudi culture assumes that other trusted parties should take responsibility, rather than individuals themselves. In comparison, in a South African study, (Kruger et al. 2010) less than 10% of respondents said that information security was not their responsibility.

4.2 Preferences for information dissemination

From the data presented so far, there is a clear need to increase the level of ISA. The final two questions related to the mechanisms by which ISA could be raised i.e.: how should information about ISA be disseminated. The Web is, by far, the most popular source of Information Security information (69.2%) of 412 respondents. The Web is also particularly appropriate for Saudi culture for two reasons. Firstly, the country is very large and much of the population lives in relatively remote locations. The Web provides distance education which addresses this problem. Secondly, the Web is particularly suited to Saudi women who could not go unaccompanied by a male relative to attend seminars or courses. The article is second with 17.2%, nearly 12% of respondents use books, 8.3% use courses, 4.4% use exhibitions or seminars and 21.8% chose other.

Table 5 shows the list of communication mechanisms that respondents believed could effectively promote ISA. Respondents were asked to indicate their three most preferred options. 75% of 412 respondents prefer the Web but over 50.7% also thought that newspapers would be effective.

Which of the following mechanisms would be effective for learning about information security (N=412)					
	Percent	Count (N)		Percent	Count (N)
Web portals	*75.0%*	*309*	*Books*	*16.3%*	*67*
Newspapers	*50.7%*	*209*	*Cartoon series*	*14.8%*	*61*
Documentaries	*35.2%*	*145*	*Exhibitions*	*14.1%*	*58*
Advertisements	*30.3%*	*125*	*Talks*	*13.1%*	*54*
E-Books/ e-Magazines	*29.1%*	*120*	*Magazines*	*12.1%*	*50*
Billboard/ Posters	*28.9%*	*119*	*Web based games*	*8.7%*	*36*
Seminars	*21.1%*	*87*	*Other*	*0.7%*	*3*

Table 5: Communication Mechanisms that can be Effective in Promoting ISA

There are a number of interesting observations that can be made about these two Tables. Firstly, the number of respondents who used the "Other" option in the previous question which was about the sources that have been used to learn about information security is only 21.8%. This means that, apart from the 5 listed options, most respondents had not used many other methods to find out about Information Security. However, when presented with a larger set of information dissemination methods (Table 5) respondents found many of them useful. For example, 50.7% nominated newspapers as an effective medium (Table 5) but very few included newspapers as an "Other" mechanism that they had already used in the sources of learning about Information Security question. The most likely reason for this discrepancy is that respondents believed that newspapers could be effective but that they had not previously found the information they required in newspapers. This is not surprising as Saudi newspapers are highly conservative and highly censored, so newspapers have probably paid scant attention to a problem that only affects the Web, which is a major competitor to print media. Similarly, documentaries and billboard posters were far better represented in Table 5 (35.2% and 28.9%, respectively) than the 21.8% "Other" in the sources of learning about Information Security question. Once again, the print and television media in Saudi Arabia are not concerned about threats to online information.

5. Conclusions and future research

Saudi Arabia had the ninth highest incidence of Information Security attacks in the world in 2008 and the seventh highest in 2009 and twelfth in 2010 according to Kaspersky Lab. This is unusual, given its relatively small population and level of Internet adoption. Poor information security in countries like Saudi Arabia increase the rate of dissemination of viruses and provide 'easy targets' for Denial of Service attacks against businesses around the world. It is important to understand why countries like China, Russia and Saudi Arabia have such high levels of attacks, and to devise strategies to help them improve their situation, and, thereby, improve overall information security around the world.

This paper has suggested that the level of attacks may be due to a lack of ISA among the Saudi general public. It has also been suggested that the lack of ISA may be due to the highly-censored, patriarchical and tribal nature of Saudi culture. A survey of 462 Saudis indicates that ISA is in fact very low and that a number of information security risks may be related to Saudi culture. These include the sharing of passwords which can be explained in the context of the tribe. Similarly, the expectation that the government or other information providers are responsible for Information Security reflects the patriarchical Saudi culture. The frequency with which passwords were changed and the strength of passwords themselves supported the conclusion that the general public either does not know about recommended security procedures or simply chooses not to follow them.

So, the paper has indicated that ISA is low in Saudi Arabia and this is almost certainly one of the causes of the high level of Information Security attacks in that country. The next phase of this research will examine the IT practices in Saudi Arabia to determine if Saudi IT departments are aware of recommended practices and standards, if Saudi organisations have specialist IT security staff and if Saudi IT practitioners are sufficiently qualified in information security.

The study has also shown that the most appropriate methods of disseminating information about Information Security to the general public is via Web portals or via newspapers. Both of these mechanisms address the problems of distance and strict cultural controls that apply to women.

References

Afyouni, H. (2006) Database Security and Auditing: Protecting Data Integrity and Accessibility, Thomson Course, Canada.

Alhagil, H. (2001) Treasure lineage and Arts Complex, Saudi National House, Riyadh.

Alothimin, A. (2009) History of Saudi Arabia, Obekan Ltd., Riyadh.

Bragg, R., M. Ousley and K. Strassberg (2004) Network Security: The Complete Reference, Coral Ventura, United States of America.

Creswell, J. (2003) Research design: Qualitative, quantitative, and mixed method approaches, Sage Publications, California.

Deibert, R., J. Palfrey, R. Rohozinski, and J. Zittrain (eds.) (2008) Access Denied: The Practice Policy of Global Internet Filtering, London, The MIT Press.

Easttom, C. (2006) Computer Security Fundamentals, Pearson Prentice Hall, United States of America.

Hancock, D. and B. Algozzine (2006) Doing Case Study Research, Teachers College Press, New York.

Hofstede G. (2009) "National and organisational culture: Arab world", http://geert-hofstede.com/arab-world-egiqkwlblysa.html, accessed 09/02/2010.

Kaspersky Lab (2010) http://www.securelist.com/en/analysis/204792101/Kaspersky_Security_Bulletin_2009_Statistics_2009, accessed 29/02/2010.

Kaspersky Lab (2011) http://www.securelist.com/en/analysis/204792162/Kaspersky_Security_Bulletin_2010_Statistics_2010, accessed 14/05/2011.

Kruger, H. , L. Drvein, and T. Steyn (2010) "A vocabulary test to assess information security awareness", Information Management & Computer Security, 18 (5), pp.316-327.

Library of Congress – Federal Research Division (2006) Country Profile: Saudi Arabia, September 2006.

Moaddel, M. (2006) The Saudi public speaks: religion, gender, and politics, International Journal of Middle East Studies, 38, 79-108.

Siponen, M. (2000) "A conceptual foundation for organizational: information security awareness", Information Management & Computer Security, 8 (1), pp. 31-41.

Stallings, W. and L. Brown (2008) Computer Security Principles and Practice, Pearson Education, United States of America.

Turban, E. , J. Wetherbe, and E. McLean (1996) Information Security Technology for Management: Improving Quality and Productivity, 3rd Edition, Wiley, United State of America.

Whitman, M. and H. Mattord (2008) Management of Information Security, Thomson Course Technology, Canada.