British Journal of Arts and Social Sciences
ISSN: 2046-9578, Vol.6 No.1 (2012)
©BritishJournal Publishing, Inc. 2012
http://www.bjournal.co.uk/BJASS.aspx

Information Security Awareness and Culture

Yasser Al-Shehri
Computer Science and Engineering Department , Yanbu University College, Yanbu, Saudi Arabia
e-mail: Yasser.alshehri@yuc.edu.sa

Abstract

Users from diverse background and culture are incredibly joining the Internet. At the same time, Internet threats have become sophisticated. Users' systems and Information must be kept protected from any kind of threats. However, the threat could be come from the user himself due to his practice with his system or information. Human factor is a crucial issue in the chain of the security and every part of the security chain must be strong because any weakness at any part will make the chain broken as a whole. Users must be aware of system threats and what practice must be adhered in order to keep the system and information protected. Therefore, measuring the awareness of end users from diverse backgrounds was one of the aims of this research. Another aim was to investigate if alerted users are practising their knowledge. In order to reach that, a questionnaire was designed and published online. The survey was opened for a month in duration and more than 200 persons contributed to the research and volunteer their answers. The main finding of this study is that users who had previously attended security course are more aware about information threats. Nevertheless, their practices with information are not differed from those who have no knowledge. Moreover, incompetent users are often unconscious of their needs. In addition, cultural factor is clearly present in the security practices especially in the confidential matters.

Keywords: Information Security, Information Security Awareness, Information Security Awareness and Cultur**e**

1. Introduction

Clearly, number of users joining the internet is increasing. As a consequence, the global network has been dramatically enlarged. In addition, internet applications have been facilitated for users in order to provide them with full connectivity text, voice, and video images. Users are spending more time on the internet doing more work than ever. Users nowadays are maintaining their bank accounts online, buying and selling using the internet. It is estimated that 20% of people in the UK are doing most of their banking operations through online banking (Online Identity theft, 2006). In addition, AOL reports (2005) that 72% of internet users use the internet for sensitive transactions such as banking or stock trading. These features encourage people to join the global network to remain in touch with family, friends worldwide. All these facilities have attracted users to come toward this global community and to remain connected longer or permanently. Although end users have adapted the technology, they often have a lack of awareness towards the right practice or they possess knowledge but they often do not practice it in proper ways.

To secure any systems, it is important to ensure the availability, integrity, and confidentiality of data inside this system. In order to do so, there are plenty of hardware, software, procedures implemented inside this system.

2. Background

Human interactions have been noted as an important area of the information security architecture. It is an important area which should concern by everybody not only home users. Furnell et al (2007) states that when home systems are compromised, the internet as a whole will be affected. Surely, raising the awareness will simultaneously reduce users fault (Siponen, 2000). As a consequence, it is essential to keep the public aware of the security threats and educate them towards using good practices in order to get greater security. Furthermore, human factors need be addressed beside the technical and management factors in information security. In this sense, Von Solms (2000) adds the third dimension in the information security waves which is called the institutionalization wave. This wave is described as building a security culture among users which should be practiced as daily activities. In addition, Siponen (2001) proposes the five dimensions of information security awareness. The first one is the organizational dimension which has been covered by much research (e.g. Siponen, 2000). The second dimension, on the other hand, is the general public dimension which has been touched by some other research (e.g. Furnell, 2007; 2008).

In order to measure human awareness, other areas need be measured. Kruger and Kearney (2006) suggest that the measurement should address three major areas: peoples’ behavior, feeling and knowledge. Based on this argument, they have developed a prototype to investigate three major questions: what do they know? How do they feel? And how do they behave? Some users could behave in a way that is against their belief or feeling. For example, a system forces a user to change his password every 30 days. This user has changed his password because he was forced to by the system not because he knows this practice can secure his account. This approach will investigate users’ knowledge and match it with their practice.

It is argued (Thomson et al 2006) that the level of awareness of this knowledge must be addressed first. The study proposes that users in the knowledge are either competent or incompetent. In addition, incompetent users are either conscious or unconscious of their needs. The worst level of awareness is the one when users are incompetent and unconscious. Therefore, in order to improve the skills level, users must be alerted of their needs.

3. Methodology

3.1The Chosen Method

The objectives of the research are to investigate the use of the internet among people of different cultural backgrounds. It will also investigate their practices and awareness towards information. Furthermore, the analysis expected differences between different cultures. In order to achieve these aims, several methods can be undertaken. For example, interviewing users and monitoring their practices with information. However, the most appropriate one to achieve diverse people is a questionnaire. With the help of the CISNR at the University of Plymouth, this survey was conducted and uploaded to the web server of the CISNR. An online survey is very cost effective since no papers are required to be distributed to all respondents. This can also maximise the number of respondents because it will be published online.

3.2The Survey Structure

This survey comprises 44 questions divided into four sections: Demographics, Computer General Practice, Security Practice, and Security Awareness. Firstly, the Demographics section will investigate the background that users are come from (Who are they?). Secondly, the survey will move on to investigate the practice of users with information (what do they really do?). This question will be addressed in two parts of the survey; the first part will ask them about their general practice with the computer, and the second part will be focused in specific to investigate their security practice. Thirdly, the security awareness section will check the level of awareness users have (What they know?).

4. Results and Analysis

The survey was conducted for one month, from the 4th of July2008 through 29th of July 2008. The total number of respondents was 245 users from thirty five countries all over the world. The survey was promoted through a published link. This link was sent to users through e-mails, and Internet forums. Users from 35 countries contributed and answered the survey. Four countries had the largest portions in terms of number. These countries are: Saudi Arabia, Pakistan, UK, and France.

4.1 Gender and Age of Participants

Females from all countries contributed in this survey in a small portion (20%). A majority of respondents (60%) are from the age group of 20-29 years of age. In terms of age, some differences were noticed in the use of the Internet applications and the use of technology. For example, social networks attract younger users. Fifty-three percent of users from the age group of 20-29 use social networks. The percentage drops down to 29% for the age group 30-39. The percentage also goes down to 9% for the age group 40-49. In addition, users in the middle ages have a low number of accounts in comparison to other users. For instance, all users from the age group 50-59 have few numbers of accounts (Maximum 5). Also, a majority of the users from the age group 40-49 have fewer than five accounts. In the security practice, users between the ages of 30 and 49 have been noticed to be more careful in their security practice. For example, 60% of the age group of 50-59 have never reused their passwords. Additionally, 60% of the same age group consider all of their accounts to be important.

4.2 Education

Without any doubt, education will influence extend knowledge, understanding of humans regardless of their field of study. The level of education or the level of degree earned is also crucial factor of the user’s knowledge. Users in general possess either graduate (41%) or post-graduate (40%) degrees. There was no noticeable difference in terms of the security practice or awareness between graduate or undergraduate students. However, all of the users who have attended security course show better understanding and awareness in many aspects of security. The survey could not reach users with low level of education or uneducated users due to the nature of the survey which was published online. Further research can involve such users by interviewing them.

4.3 Religion

The participants followed ten religions. Participates from some countries followed a single faith. For instance, Saudi and Pakistani users follow the Islamic faith. In the UK, users follow verities of faiths such as Anglicans, Catholicism, protestant, Islam and atheism. All the religions are illustrated in the following table 1.

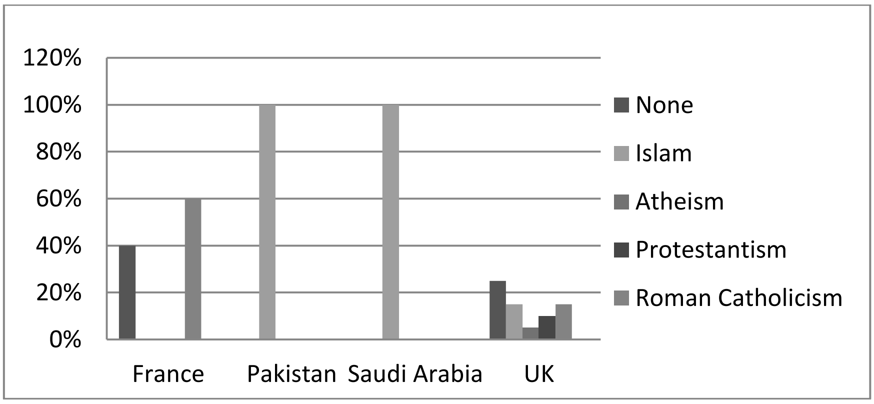


Table 1: Religions of the participants

4.4 The Use of the Internet

The survey questioned users about their use to assess the popularity of the applications, in one hand. On the other hand, this assesses the familiarity of end users towards the technology. As it is expected, some applications were used by many users such as e-mailing and web browsing with out noticeable differences between countries and religions. Other applications were quite new in the use of the Internet. Therefore, few users from every country were using them. For instance, telephony was used by Saudi (24%), Pakistani (26%), British (20%), French (60%), and Nigerian (50%). French and Nigerian respondents were students of IT in postgraduate level. So, their familiarities with technology were noticeably differed from other users. Online banking application was used more by British (75%) and French (70%) users. the reason could be due the application in industrial countries could be more mature and secure. Part of this also depends upon the trust between end users and their local banks. Also, what effort was made by local banks to introduce the service to their customers if the service is existed. In terms of age, some differences were noticed in the use of the Internet applications and the use of technology. For example, social networks attract younger users. As they get older, they lose the Internet in these types of application. Fifty-three percent of users from the age group of 20-29 use social networks. The percentage drops down to 29% for the age group 30-39. The percentage also goes down to 9% for the age group 40-49.

4.5 Authentication Practice and Awareness

Authentication is the process of ensuring that a system should be accessed by certain users. This study selected the password because it is one of the most common methods of authentication. First, the study evaluates the use of passwords and people's awareness for good password practices. Second, the study will assess whether users reuse their passwords in other systems. If so, the study will evaluate the extent of this behaviour. Third, the study will discuss the awareness of users towards password selection.

4.5.1 Reused Password

Almost all of the 245 participants revealed that they have more accounts than passwords. However, users reused different proportions of their passwords: 25%, 50%, 75% or all of them. Generally, a majority of all users have reused at least a small proportion (25%) of their passwords. Figure 4-1 shows the percentage of users from the five main countries who have reused 50% of passwords they have. Similarly, figure 4-2 and figure 4-3 illustrate percentage of users who have reused 75% or 100% of their passwords.

Figure 4-1.50% of their passwords have been reused

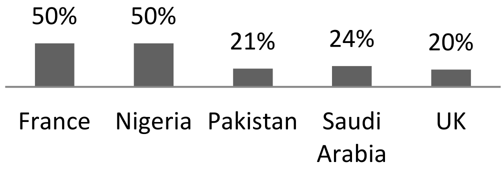


Figure 4-2. 75% of their passwords have been reused

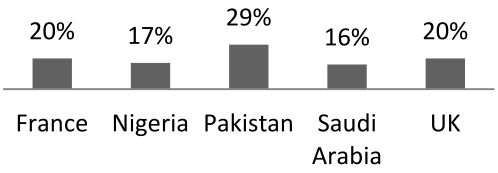
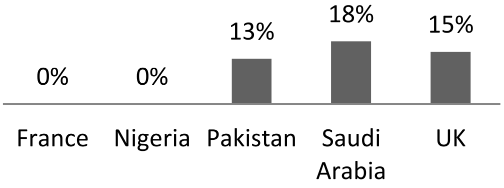


Figure 4-3. All of their passwords have been reused



4.5.2 Account Security Awareness

The awareness toward the necessity of having different types of accounts secure seems to be inadequate among all users in general. Every single account should be considered as crucial in users' thoughts. The reason for this is simply because every account could contain valuable information: financial, personal, and data belonging to work. Based on this, the participants were questioned about which accounts they think should be protected by using a strong authentication method. Five major accounts were listed: online banking, a login to work, a login to school, social networks, and mail servers. The results in general show that users agreed mostly about online banking as sensitive accounts. After online banking, the majority of every country thinks that mail servers are vital accounts. However, other accounts show that few users think that they are crucial accounts. As a result, the study breaks down four groups according to these answers.

SOC1	group of users who did not agree that social networks should be protected by strong passwords
LOG1	users did not appreciate work accounts
LOG2	did not appreciate accounts given by institutes or schools
BANK1	group of users who did not agree with the importance of online banking

Table 1: The four sample groups

First, the results of SOC1 are the most shocking results. First of all, all users in some countries have social network accounts, such as Pakistan and France. Seventy-eight percent of Saudi users and 69% of British users have access to these networks. In addition, they are happy to share real information such as names, dates of birth, family information, addresses, and telephone numbers. Second, the results of the second group, LOG1, demonstrate the low awareness level among quite a few users from Saudi Arabia, Pakistan, and the UK. The worst figure is shown in the Saudi users; 60% of them think the work login is unimportant. Also, 35% of them are workers and have access to computers from their work. British and Pakistani users share nearly the same level of awareness (20%). Third, LOG2 group shows a level of awareness that is the same as LOG1. The results find that quite a few users from every country did not agree with the necessity of the account while they are students. Fourth, BANK1 group joins users from Saudi Arabia (15%), Pakistan (8%) and the UK (15%). However, All British users from this group have no access to online banking. Even though, it is not an enough excuse. Seven percent of Saudi and 3% of Pakistani users have online banking, but they do not agree with the necessity of the account.

4.5.3 Password Understanding

The survey asked participants if they believe that "*David1984*" is a strong password. There were four possible answers and only one reflected good awarness and understanding of this issue. All other options would show that users are not aware of how passwords should be selected.The results found that a majority are conscious of this issue. Competent users will be the participants who selected the right answer. They will be joind under one group called **CompetentPass**. Their practice will be investigated individualy in order to find whether they practice what they understood or not. The study find that 40% from every of saudi, pakstani, and French users do not use complex passwords. Nigerian and British users have better practice when 20% of every country do not have complex passwords. The figure here does not look that bad. However, it is worthless having a complex password since this password is used in other systems as it is pointed in the previous section.

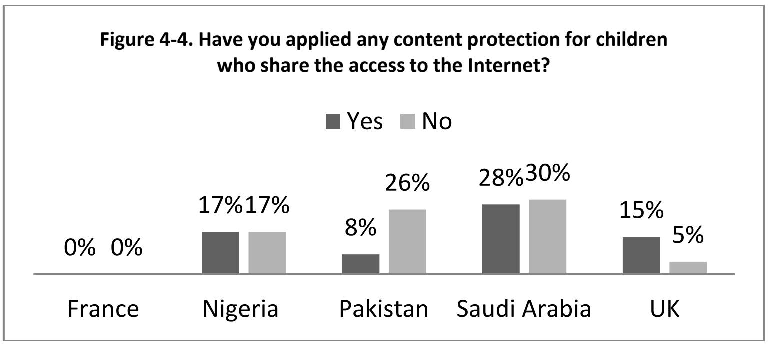
4.6 Access control, Practice and Awareness

Authorization is one of the main goals of system security. It helps to first authorize the right user to get access to a system. Secondly, it protects the user's own files, which are saved on the same physical disk with other users. Hence, it is important to have multiple IDs for a single computer that are accessed by multiple users. Having different accounts will protect data from being seen, lost or modified by unauthorized persons. Users prefer the easier option of opening a computer for anyone at any time. Or, they prefer to assign one user name for everyone using the system. Table 3 below show that users who share access with others are more likely to use a single account set for everyone except the Nigerian users, who either do not share access or set up the right security configuration. In the UK, one in every two users use the right practice; Pakistan is somewhat similar to the UK. In Saudi Arabia, one in every four users uses the right security configuration.

	France	Nigeria	Pakistan	Saudi Arabia	UK
Single account	30%	0%	26%	38%	25%
Several accounts	0%	17%	11%	10%	15%

Table 3: Access control practice

Child protection has been regarded as one of the main aspect of Internet content. Since the Internet is an open network, it is impossible to regulate what is inside the Internet. The respondents were questioned if they have applied a content protection for children who share the access. The following figure illustrates percentage of users who share the Internet with their children and weather they apply content protection or not. In this issue, British users show more care than other users as it seen in the figure below. The worst figure is shown with the Pakistani users. Almost one in every four users from Pakistan applies protection for children.



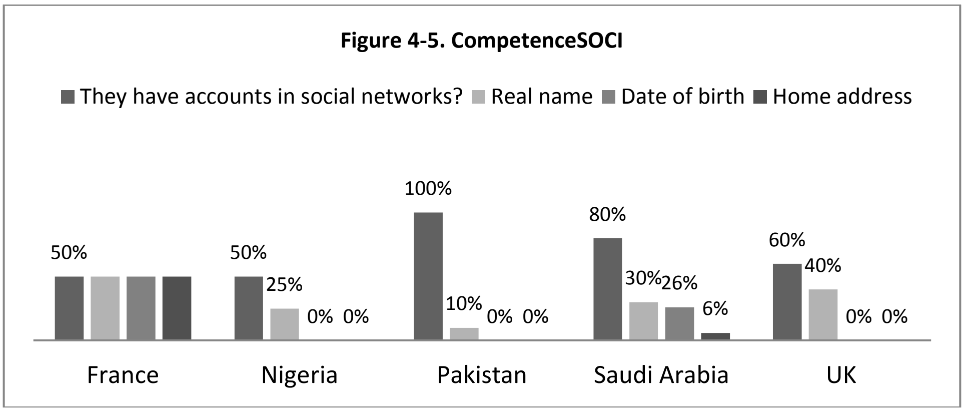
4.7 Social Network Awareness and Practice

First, the survey questioned users on what they think of having an account in a social networking web site. The answers are illustrated in the table below (4). The lowest level of understanding appeared in the first row which show that a majority of British users (70%), French users (70%) and Pakistani users (66%) did not understand the problem of social networks. Saudi users are not far better because 20% of them prefer to be anonymous. The best understanding is clearly represented in Nigerian users since 66% understood that the information in socail network could be misused. The last row of the table will be taken as a sample called **ComptenceSOCI**. The study assessed the knowledge of this group in regard to the social network understanding. It will now evaluate their practice and demonstrate whether their practice match their knowledge or not.

	France	Pakistan	Saudi Arabia	UK
I agree to expose my real information	70%	66%	32%	70%
I want to be anonymous	10%	8%	20%	10%
I don't agree because my real information could be misused	20%	26%	48%	20%

Table 4: Social Network Awareness

CompetenceSOCI was analysed in order to assess if the users of this group have social network accounts. If yes, what information they are happy to expose. Figure 4-5 illustrates the competent group and their use of social networks. Fifty percent of users from France have social network accoutns and all of them expose their real names, dates of birth and home adresses. All coompetent users from pakistan have social network accounts. However, only 10% of them exposed their real name only. Eighty percent of saudi users have social network accounts. It was found that 30% of them have exposed their real names, 26% disclosed their dats of birth and 6% revealed their home addreses. The figure also shows that 40% of the british users have share their real names in social networks.



4.8 Identity Theft Awareness

This survey questioned users if they have ever been victims of identity theft. A group of users (IDT1) answered “yes” and another group (IDT2) answered “no.” Both groups were evaluated in their practices towards physical documents (e.g. bank statements and bills) and digital information (e.g. social networks), which also can be used for ID fraud (National Identity Fraud, 2007). The results of the participants show that 35% of the British users, 30% of French users, 18% of Pakistani users, 17% of Nigerian users and 17% of Saudi users have been victims of identity theft. Also, it is important to note that people might not realise that they have been victims. Therefore, users of group IDT2 might be victims without their knowledge.

Seventy percent of British users (from IDT1 and IDT2 groups) have never thrown any of the physical documents. This show the best practice among other nationalities. This good practice might be due to the awareness programmes which are promoted by the government in the Internet and the media. Other users from both groups have thrown their physical papers without destroying them. Phone and utility bills were the most common papers which usually users do not care about them. Bank statements come after bills with average 20% of every country. However, social networks seem to be a serious problem for both groups. Some identity theft victims claim that they have never thrown documents into trash bins without first destroying them. However, the same users who claim that have social network accounts and have exposed some of their real information. So, if this was not the first reason, it might be due to the second reason. On the other hand, IDT2 users showed very poor practices that make it very likely that they will become victims. Figure 4-6 illustrates the percentage of information has been exposed in social networks from every country. It is clear that Saudi and Pakistani users have a high percentage in social networks. However, the percentage of the real information exposed is low in comparison to the number of accounts they have. In other words, they are likely to prefer to be anonymous. Table 4 indicates that 20% of Saudi users prefer to be anonymous rather than share their real information. So, this result here is not due to the security awareness.

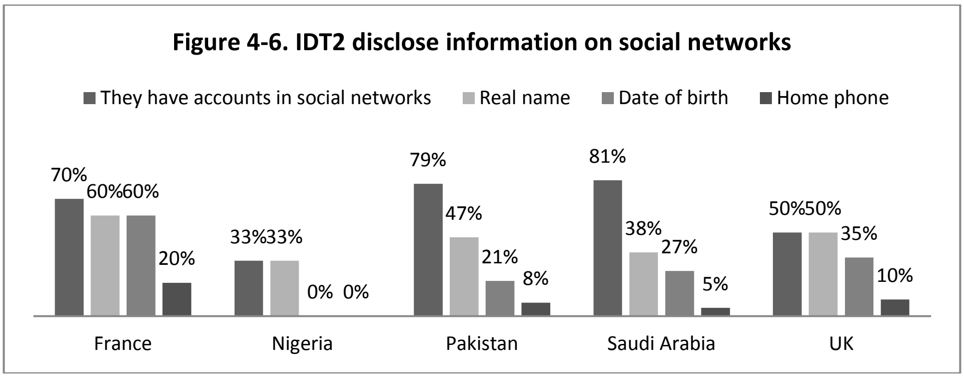


Figure 4-6. IDT2 disclose information on social networks

4.9 Competence and Consciousness

It is a good level of awareness when users are competent and conscious. In other words, users have the knowledge of particular skills. At the same time, they are aware of their needs and of their developing areas (Thomson et al 2006). However, they might be competent and conscious but not practicing what they know and what they believe in. Therefore, it is important for competent users to use the skills that they have. In other words, are they really practice what they believe in? (Kruger and Kearney 2006). From the two arguments, the study comes out with the level which all security awareness programmes much seek. This level can be called Conscious Competent Practised.

The results, in some places, clearly indicate the fact that users often practice differently than their understanding. There are two examples from this study that prove this argument. The first is the example of the password understanding, when a majority of the participants have a good understanding. However, their password practices are different than what they believe as it is pointed in the password understanding section. The second example is about social network understanding. Quite a few users understood that information in social networks could be misused. In spite of this, a large proportion of this group have posted their real information in social networks as it is pointed in the social network awareness and practice section. In addition, the results indicated there is a lack of consciousness among quite a large number of users. For example, their understanding is poor in some security aspects. In spite of this, they claim their professional level of computer security. In this sense, they were classified in the incompetence unconscious level.

5. Conclusion

It is important for this kind of research to be continued. Also, it will be useful to reach diverse backgrounds such as different levels of education, and ages. For instance, only 20% of the responses were female. Moreover, 81% of the participants hold graduate or postgraduate certificates. Also, the highest portion of the respondents was in the age group of 20-29 years of age. It will be very useful to find various answers which can lead to better analysis.

To sum up, this paper introduced the topic and gave a brief background of the topic. It explained methodology of this research. Then, the topic illustrated some of the key findings. It analysed and discussed the major findings of this study. At the end, the topic was concluded by explaining some limitation of this work which can be avoid in the future.

References

AOL/NCSA.2005. AOL/NCSA Online Safety Study [Online] Available at: http://staysafeonline.org/pdf/safety_study_2005.pdf [accessed 15 Jan 2008]

Furnell, S. Bryant, P. Phippen, A.2007. "*Assessing the security perceptions of personal Internet users*". Computer and Security. http://www.sciencedirect.com/science/journal/01674048Volume 26, Issue 5, August 2007, Pages 410-417

Furnell, S.2008. "End user security culture: A lesson that will never be learnt?" Computer Fraud and Security. http://www.sciencedirect.com/science/journal/01674048 Volume 2008, Issue 4, April, pp6-9, 2008

Kruger, H. Kearney, W. 2006. "*A prototype for assessing information security awareness*". Sience Direct. Vol.25, Issue 4, Pages 289-296

National Identity Fraud. 2007."How ID fraud Occurs". [Online] available at: http://www.stop-idfraud.co.uk/How_IDF_Occurs.htm [accessed 5 August 2008]

Online Identity Theft.2006. "Security Report: Online Identity Theft". [Online] Available at: http://www.btplc.com/onlineidtheft/onlineidtheft.pdf [accessed 10 July 2008]

Siponen, M.2000. *"A conceptual foundation for organizational information security awareness"*. Information Management and Computer Security. Vol.8/1, Pages: 31-41

Siponen, M.2001. *"Five Dimensions of Information Security Awareness"*. Computer and Society. Pages: 24-29

Thomson, K. Von Solms, R. Louw, L.2006." *Cultivating an organizational information security culture*". Computer Fraud & Security. Vol. 2006, Issue 10,Pages 7-11

Von Solms, B.2000."*Information Security- The Third Wave?*" Computer & Security. Vol. 19, Issue 7, Pages 615-620