



Title: Strategic framework to minimise information security risks in the UAE

Name: Ahmed AlKaabi

This is a digitised version of a dissertation submitted to the University of Bedfordshire.

It is available to view only.

This item is subject to copyright.



**STRATEGIC FRAMEWORK TO MINIMISE
INFORMATION SECURITY RISKS IN THE UAE**

**A thesis submitted to the University of Bedfordshire in partial fulfilment
of the requirements for the PhD degree**

By

Ahmed AlKaabi

June 2014

Acknowledgment

It is my pleasure to express my deepest gratitude to the following individuals and organisations for their help and support over the PhD period:

My supervisor and director of studies Professor Carsten Maple: Only with your guidance, encouragement and continuous support was this work completed. You have inspired me with your insight and numerous research skills, which was reflected in my work. Thank you very much.

My second supervisor Professor Yong Yue: Although face to face meetings could be counted on one hand, your guidance was invaluable. Thank you for your time and effort.

The General Director of Abu Dhabi General Headquarters (ADGHQ) affairs Brigadier Ali Aldaheri: Your encouragement and support is unforgettable. You have a significant role in my professional success and always encourage me to learn and improve especially in the field of information security.

Staff at the Abu Dhabi Educational Council (ADEC): Your help and support in the studies of this research contributed substantially to attained results. Thank you very much.

Staff at the Abu Dhabi System and Information Centre (ADSIC): Your provided material on local information security standards was a strong basis for my PhD project.

Father, mother and family: Thank you very much for your continuous support, patience and honest advice whenever needed.

Friends and colleagues: Thank you all for your support and advice over the PhD journey. Special thanks to Rashid Alneadi, Sobhi and Monika.

Dedication

This thesis is dedicated to HH Lt. General Sheikh Saif bin Zayed Al Nahyan, Deputy Prime minister and Minister of Interior.

Declaration

I declare that this thesis is my own unaided work. It is being submitted in partial fulfilment of the degree of PhD at the University of Bedfordshire. It has not been submitted before for any degree or examination in any other University.

Signed:

Date:

(Candidate)

Abstract

The transition process to ICT (Information and Communication Technology) has had significant influence on different aspects of society. Although the computerisation process has motivated the alignment of different technical and human factors with the expansion process, the technical pace of the transition surpasses the human adaptation to change. Much research on ICT development has shown that ICT security is essentially a political and a managerial act that must not disregard the importance of the relevant cultural characteristics of a society.

Information sharing is a necessary action in society to exchange knowledge and to enable and facilitate communication. However, certain information should be shared only with selected parties or even kept private. Information sharing by humans forms the main obstacle to security measure undertaken by organisations to protect their assets. Moreover, certain cultural traits play a major role in thwarting information security measures. Arab culture of the United Arab Emirates is one of those cultures with strong collectivism featuring strong ties among individuals. Sharing sensitive information including passwords of online accounts can be found in some settings in some cultures, but with reason and generally on a small scale. However, this research includes a study on 3 main Gulf Cooperation Council (GCC) countries, namely, Saudi Arabia (KSA), United Arab Emirates (UAE) and Oman, showing that there is similar a significant level of sensitive information sharing among employees in the region. This is proven to highly contribute to compromising user digital authentication, eventually, putting users' accounts at risk. The research continued by carrying out a comparison between the United Kingdom (UK) and the Gulf Cooperation Council (GCC) countries in terms of attitudes and behaviour towards information sharing. It was evident that there is a significant difference between GCC Arab culture and the UK culture in terms of information sharing. Respondents from the GCC countries were more inclined to share sensitive information with their families and friends than the UK respondents were. However, UK respondents still revealed behaviour in some contexts, which may lead potential threats to the authentication mechanism and consequently to other digital accounts that require a credential pass.

It was shown that the lack of awareness and the cultural impact are the main issues for sensitive information sharing among family members and friends in the GCC. The research hence investigated channels and measures of reducing the prevalence of social

engineering attacks, such as legislative measures, technological measures, and education and awareness. The found out that cultural change is necessary to remedy sensitive information sharing as a cultural trait. Education and awareness are perhaps the best defence to cultural change and should be designed effectively. Accordingly, the work critically analysed three national cybersecurity strategies of the United Kingdom (UK), the United States (U.S.) and Australia (AUS) in order to identify any information security awareness education designed to educate online users about the risk of sharing sensitive information including passwords. The analysis aimed to assess possible adoption of certain elements, if any, of these strategies by the UAE. The strategies discussed only user awareness to reduce information sharing. However, awareness in itself may not achieve the required result of reducing information sharing among family members and friends. Rather, computer users should be educated about the risks of such behaviour in order to realise and change. As a result, the research conducted an intervention study that proposed a UAE-focused strategy designed to promote information security education for the younger generation to mitigate the risk of sensitive information sharing. The results obtained from the intervention study of school children formed a basis for the information security education framework also proposed in this work.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION	16
1.1 Problem Statement	17
1.1.1 The Cultural Aspect	18
1.1.2 The Contextual Development	18
1.2 Motivation	18
1.3 Research Aim and Objectives	20
1.3.1 Aim	20
1.3.2 Objectives	20
1.4 Scope	20
1.5 Research Process/Methodology	21
1.6 Thesis Contributions	22
1.7 Thesis Structure	24
1.8 Related Publications	25
CHAPTER 2: HUMAN BEHAVIOUR IN ICT SERVICES.....	26
2.1 Information Security	26
2.1.1 Vulnerability of Information Security	28
2.1.1.1 CIA Loss.....	31
2.1.1.2 Social Engineering Attacks	33
2.1.2 Human Factors in Information Security	35
2.1.3 Insider Threats	35
2.1.4 Privacy Issues in ICT.....	37
2.1.4.1 Sensitive Information Disclosure	38
2.1.4.2 Password Sharing	40
2.1.4.3 Impact of Sharing Sensitive Information	42
2.1.4.3.1 Spam.....	42

2.1.4.3.2	Fraud.....	42
2.1.4.3.3	Scam	43
2.1.4.4	Law Enforcement	43
2.1.4.5	Information Security Standards and Guidelines.....	44
2.1.4.5.1	GAISP	45
2.1.4.5.2	COBIT	45
2.1.4.5.3	ISO 27000.....	46
2.2	Discussion	47
2.3	Conclusion	48
CHAPTER 3: THE ROLE OF CULTURE IN ICT SERVICES		49
3.1	Culture and ICT	49
3.1.2	The United States.....	51
3.1.3	The United Kingdom	52
3.1.4	Australia.....	54
3.1.5	The Arab World.....	57
3.1.5.1	Arab Culture	58
3.1.5.2	Sharing of Private Information.....	59
3.1.5.3	History of ICT adoption in the Arab World.....	59
3.1.5.4	Internet Revolution in the Arab world	62
3.2	Organisational Culture	63
3.2.1	Information Security Culture.....	63
3.2.2	Cultural Impact on Information Security.....	64
3.3	Conclusion	66
CHAPTER 4: CULTURE AND INFORMATION SECURITY.....		67
4.1.	Methodology	67
4.1.1	Phase One - Pilot Study	68
4.1.1.1	Quantitative Approach	68

4.1.1.1.1	Results	69
4.1.1.2	Qualitative Approach	74
4.1.1.2.1	Summary of Key Issues.....	76
4.1.2	Phase Two - Further Study	77
4.1.2.1	Questionnaire Design	77
4.1.2.2	Hypothesis 1: Users' attitudes in Oman, KSA and UAE.....	81
4.1.2.2.1	Data Summary	82
4.1.2.2.2	Descriptive Analysis (Aggregation).....	85
4.1.1.1.1	Inferential Analysis	91
4.1.1.2	Discussion	92
4.1.1.3	Hypothesis 2: Users' attitudes in GCC Countries and the UK.....	94
4.1.1.3.1	Results and analysis (GCC and UK)	94
4.1.1.4	Discussion	100
4.2.	Conclusion	102
CHAPTER 5: SOCIAL ENGINEERING ATTACK MITIGATION		104
5.1.	Legislation Measures	104
5.2.	Technological Measures	107
5.1.3	Restricting Data Access	108
5.1.4	Encrypting data.....	108
5.1.5	Data Hiding.....	109
5.1.6	Controlling System Access.....	109
5.1.7	Updating Software	110
5.3.	Education and Awareness	110
5.4.	Cultural Change	113
5.5.	Conclusion	114
CHAPTER 6: NATIONAL CYBERSECURITY STRATEGIES: RESPONSE TO PASSWORD SHARING		115
6.1	Research Strategy.....	115

6.2	Information Security Strategy in the GCC.....	117
6.2.1	Saudi Arabia (KSA).....	117
6.2.2	Oman.....	118
6.2.3	Bahrain.....	118
6.2.4	Qatar	118
6.2.5	Kuwait.....	118
6.2.6	United Arab Emirates (UAE)	119
6.3	National cybersecurity Strategies for the U.S., the UK and Australia.....	119
6.2.7	United States (U.S.)	119
6.2.8	United Kingdom (UK).....	122
6.2.9	Australia (AUS).....	123
6.4	Analysis and Discussion	125
6.5	Conclusion	126
CHAPTER 7: STRATEGIC INFORMATION SHARING SECURITY FRAMEWORK.....		128
7.1	The Intervention Study: Information Security Awareness Education	128
7.1.1	The Education Programme	130
7.1.2	The Structured Approach.....	130
7.2	Quantitative Study	133
7.2.1	Method: Likert Scale Questions	133
7.2.2	Initial Assessment.....	134
7.2.3	Post-teaching Assessment.....	137
7.2.4	Results and analysis	140
7.3	Qualitative Study	144
7.3.1	Questionnaire Design.....	144
7.3.1.1	Password Sharing	144

7.3.1.2	Device/Account Access Sharing	144
7.3.1.3	Personal/Confidential Information Sharing.....	144
7.3.1.4	Others	145
7.3.2	Method: Questionnaires Based On Yes/No Questions	145
7.3.3	Grounded Theory.....	146
7.3.4	Results and Analysis.....	148
7.3.4.1	Password Sharing	149
7.3.4.2	Device/Account Access Sharing	151
7.3.4.3	Personal/Confidential Information Sharing.....	152
7.3.4.4	Others	154
7.3.5	Summary of the results	155
7.4	Discussion	156
7.5	Sensitive Information Sharing Security Framework.....	158
7.5.1	Sharing Environments	158
7.5.2	Information Security Design Structure.....	159
7.5.3	Information Security Education Model	160
7.5.4	Information Security Education guidelines	160
7.5.4.1	Password Sharing	160
7.5.4.2	Devices/Accounts Access Sharing:.....	161
7.5.4.3	Personal/Confidential Information Sharing:	162
7.5.4.4	Others (can have an impact on sharing):.....	163
7.6	Conclusion	163
CHAPTER 8: CONCLUSION AND FUTURE WORK		165
8.1	Conclusion	165
8.2	Further Work.....	172
REFERENCES		175

APPENDIX 1.....	199
APPENDIX 2.....	202
APPENDIX 3.....	207
APPENDIX 4.....	219
APPENDIX 5.....	227
APPENDIX 6.....	238

LIST OF FIGURES

Figure 1: Password sharing threats against information security	32
Figure 2: Potential risk exploitations and impacts when information is shared	34
Figure 3: Arabs willingness to share information.....	69
Figure 4: Sharing information which may lead to information security breach GCC.....	84
Figure 5: Sharing information which may lead to information security breach (Oman) ..	86
Figure 6: Sharing information which may lead to information security breach (UAE)....	90
Figure 7: Sharing information which may lead to information security breach (UK)	96
Figure 8: Inferential analysis of the differences between the two regions (GCC and the UK)	98
Figure 9: Hierarchy of the investigation and the applicability to the UAE cybersecurity threats.....	116
Figure 10: The strategic responses of the UK, the U.S. and Australia to sharing sensitive information compared to the UAE's CERT	125
Figure 11: The proposed strategy	129
Figure 12: Results of the initial test in a colour-coded diagram.....	136
Figure 13: Results of the second test in a colour-coded diagram	139
Figure 14: Results and analysis	141
Figure 15: Sensitive Information Sharing Security Framework.....	158
Figure 16: Teaching as a method of reducing information security risks	171

LIST OF TABLES

Table 1 - Applying a framework for responding to insider threats (Pfleeger &Stolfo, 2009).....	37
Table 2: U.S. employees are less willing than their Arab counterparts to share information with others	71
Table 3: The willingness of workers in the UAE to share information.....	73
Table 4: Nature of information sharing and vulnerabilities to personal and work assets..	78
Table 5: Sensitive information-sharing in 3 GCC countries	82
Table 6: Sensitive information sharing in Oman.....	85
Table 7: Sensitive information sharing in the KSA.....	87
Table 8: Sensitive information sharing in UAE	89
Table 9: The Kruskal-Wallis One-Way ANOVA test results	92
Table 10 - Results of Mann-Whitney U One-Way ANOVA	99
Table 11: GCC countries governmental initiatives to cybersecurity.....	119
Table 12: Likert Scales	133
Table 13: Age Groups.....	133
Table 14: Information security areas covered by the questions and their codes	134
Table 15: Results of the initial assessment organised in age and gender	135
Table 16: Results of the initial test	137
Table 17: Results of the second assessment organised in age and gender	138
Table 18: Results of the second test	140
Table 19: The Mann-Whitney U Test.....	142
Table 20: Experiment group	146
Table 21: Control group.....	146
Table 22: categories established from answers obtained from the two groups	149
Table 23: Password Sharing	149
Table 24: Device/Account Access Sharing	151
Table 25: Personal/Confidential Information Sharing.....	153
Table 26: Others	155

CHAPTER 1: INTRODUCTION

The proliferation of ICT systems pose high demands on availability, confidentiality and integrity when extensive data sets are stored and transacted, including sensitive data remotely accessed at any time over the Internet. With information security being virtually at the heart of all core ICT (Werner 2004), it must complement technical and organisational measures by providing new and customised security solutions.

The Internet transcends any time and location boundaries; this feature has attracted an ever growing number of online users to form communities and this constitutes an additional aspect of ICT. This results in difficulty in introducing trusted online identity and achieving global security standards, leading to an increasing number of e-crimes and phishing attacks in almost every IT sector (GTIC 2009).

Setting aside the technical details of the security measures needed to protect valuable information resources, one can perceive the human factor as a major contributor of data exposure to unauthorised access. This argument is borne out by the increasing number of social engineering attacks and internal threats in organisations. Social engineering is a technique that aims to compromise a system by which the attacker manipulates people instead of technology to bypass security mechanisms (Hahnagy, 2010).

Culture has an influential impact on people's conduct and behaviour and certain cultures are more vulnerable to information security threats than others. This vulnerability is based on several factors including openness and sharing. In cultural studies, these cultures are referred to as collectivist. According to Hofstede (2003), the Arab World is a collectivist society as compared to individualist culture and is manifested in a close long-term commitment to the member group, that being a family, extended family, or extended relationships. Loyalty in a collectivist culture is paramount, and overrides most other societal rules. Hence, adopting an information security standard without cultural customisation is unlikely to yield the intended results.

Information security education is one of the main approaches that have been suggested to increase user awareness. Different studies present information security education in different contexts such as public awareness, industry awareness and academic awareness. For example, Aloul's (2012) research on information security in the UAE maintains that users should be educated against the risk of information sharing which can be exploited

by social engineering attacks. Aloul (2012) also asserts that schools should offer security awareness courses as part of their computer course curriculum. Bishop (2000) asserts that educating the public is a primary procedure and should focus on making the public aware of the threats associated with activities on the Internet. Another reason why information security is a concern particularly for the academic field is due to the breaches rising from cultural backgrounds and lack of security awareness among university students (for example Rezgui & Marks, 2008; Hjelmås & Wolthusen, 2006; Shaikh, 2004; Kruger et al., 2011; and Bogolea & Wijekumar, 2004). Studies have been limited however to alerting to the importance of increasing information security awareness by education. Designing appropriate material and adopting suitable learning methods is another area of concern. For example, Logan & Clarkson (2005) assert that teaching hacking activities is one approach to improving a graduate's employability as a network administrator charged with protecting valuable corporate assets. Similarly, to address national needs for computer security education many universities targeting undergraduate and graduate students have incorporated computer and security courses in their curricula (Sharma & Sefchek, 2007).

As opposed to common studies in information security education, which incorporate education in university courses or in employee training programmes, this study argues that school education is more relevant especially in the cultural context of the study. The study targets school students in the UAE and assesses their information security awareness based on course material designed to raise awareness of information security risks arising from cultural-based behaviour of Arab people.

1.1 Problem Statement

The United Arab Emirates comprises seven emirates: Ajman, Dubai, Fujairah, Ras Al Khaimah, Sharjah Umm Al Quwain and the capital Abu Dhabi. The authorities in Abu Dhabi recognise the importance of developing an eGovernment strategy that conforms to information security standards which can ensure smooth and safe transactions between the government and its citizens. However, this has not yet been achieved to a satisfactory standard, as the sources cited below indicate. This work claims that neither a single standard nor a group of customised standards, if adopted by Abu Dhabi, can sufficiently satisfy the security requirements of the unique nature of the Emirate. While there has been development of international standards and guidelines, it is important to recognise that implementations are often in a local context. In order to be effective, standards,

policies and guidelines should be sensitive to local culture and context. This thesis involves the development of standards, policies and guidelines for Abu Dhabi Emirate and considers two aspects: cultural and developmental (Höne & Eloff, 2002).

1.1.1 The Cultural Aspect

The Arab culture is of a special nature, where privacy is something that Arabs share. In certain circumstances, individual privacy may take second place to the needs of the community or family (Chadwick, 2002). Furthermore, Arab culture respects elders and seniority (Koocher, 2009); private details may be divulged in circumstances involving seniority requests for these details.

1.1.2 The Contextual Development

Abu Dhabi is still under the development phase of its IT infrastructure and has not reached an advanced level of maturity to implement standards that may have worked with other countries.

1.2 Motivation

The General Secretariat of the Executive Council of Abu Dhabi is committed to establishing a service-oriented government. Through its end-user focus it aims to deliver systems that provide a high degree of performance, offering services on a global level for the benefit of all customers (UAE E-Council, 2010).

In order to create an environment of trust between the government and users of its systems, the Government of Abu Dhabi has made efforts to educate users about safe ways to use the Internet and data provided through its web sites (UAE E-Council, 2010).

In Abu Dhabi, international standards and global best practices, most notably ISO 27001:2005 and ISO 27002:2005, have been customised to develop national policies for security (ADSIC [1], 2010). These policies have been developed by the Abu Dhabi Systems and Information Centre (ADSIC). In particular, ADSIC has developed guidance and documentation including:

- An Information Security Policy Programme;
- Unified Information Security Standards;
- A series of Procedural and Technical Manuals;
- An e-literacy programme that aims to identify the digital gap and improve the capacity of ICT in all segments of society (ADSIC [2], 2010).

One of the problems that concern the UAE government is cybercrime. There have been a number of incidents reported in the past years for example:

- 402 cybercrimes in Dubai and Abu Dhabi in 2009 according to the Ministry of the Interior (Alkhaleej News, 2010);
- 62 cybercrimes in the UAE within a period of two months targeting security bodies, ministries, government bodies and private sector companies (Emarat Alyoum [1], 2010);
- 80% of all cyber-attacks on UAE organisations are launched from within the organisation itself (Emarat Alyoum [2], 2010).

The government has undertaken a number of initiatives to combat the problem including:

- Launching official calls for establishing a cybercrime court (ITP, 2009);
- Establishing a new department under the federal courts to combat cybercrimes becoming a significant security threat to public and private institutions (UAE Interact, 2009);
- Launching the Salim initiative for protection against the risks of electronic information threats and working towards attaining a culture of safety in the UAE (CERT, 2009).

The Telecommunications Regulatory Authority (TRA) is responsible for the management of every aspect of the telecommunications and information technology industries within the UAE. The TRA established a Computer Emergency Response Team (AECERT) to act as the cybersecurity coordination centre in the UAE and on 21 October 2010 AECERT obtained the ISO (ISO 27001:2005) standard for establishing a system for managing information security. The team has been, and will be, using the standard to develop internal procedures and to access global best practices that ensure business continuity and minimise threats (Zawaya, 2010).

However, standards alone are ineffective in preventing specific attacks. This inability to prevent attacks is discussed by Madan & Madan (2010), who stress that a single standard or a combination of standards fail to address vulnerability to attacks, which knowledgeable attackers can exploit with great effect. Additionally, Cheremushkin & Lyubimov (2010) have identified weaknesses in ISO/IEC 27000 series concerning Risk management, Asset, Information security policy and Certification documents.

1.3 Research Aim and Objectives

1.3.1 Aim

This research investigates culture as a key factor in ICT development, particularly in information security. The aim of the work is to *develop a strategic framework to minimise information security risks in the UAE*. This strategy is to be implemented in the long-term by targeting the younger generation, beginning with school students. The study provides the decision makers with a strategic information security framework, accompanied by guidelines, in order to have a comprehensive program relating to implementing information security education with effective outcomes.

1.3.2 Objectives

The following objectives are put forward:

1. Conduct a comprehensive literature review on Arab culture (GCC countries) and its current ICT practices, security standards and policies;
2. Investigate behaviour particular to Arab culture that could be pertinent to privacy sharing (surveys, literature review) in the UAE;
3. Investigate behaviour and attitudes towards information security in GCC countries;
4. Investigate behaviour and attitudes towards information security in a different culture other than the Arab Culture;
5. Investigate and critically analyse information security strategy initiatives taken by the UAE authorities to minimise the risk of sharing sensitive information;
6. Devise a strategy for privacy sharing in Arab culture, which comprises a solution or a set of solutions to reduce the overall information security risks;
7. Implement the strategy (taught material) on samples of students in different schools and of different age groups (11-17) and sex groups;
8. Conduct a series of surveys to test applicability and assess the results of the implementation before and after the taught material is delivered

1.4 Scope

The scope of the research covers three main topics: information security, culture and strategic security awareness to minimise the risk of sharing sensitive information. The

cultural aspect is used to investigate certain behaviour within a country in order to differentiate the selected countries. The type of culture (collectivist, individualist, etc.) is the only basis used in the research to compare people's behaviour and attitudes towards information security. Analysis of the cultural norms and psychological attributes and their potential impacts are beyond the scope of this research.

Statistical analysis tests are used to compare and analyse people's behaviour and attitudes towards information security. Other countries' cybersecurity strategies contribute to designing the sensitive information sharing security framework. According to best practices around the world, the guidelines recommend educating online users about the safe ways to use internet services.

1.5 Research Process/Methodology

In order to achieve the aim and objectives of this research, the author used both quantitative and qualitative methods (Likert scale and open ended questionnaire) in order to cover the target area. Likert scale measures were used as a quantitative approach to people's perceptions towards information security. The qualitative approach was used to reveal computer users' knowledge of information security awareness and how to respond to some scenarios and incidents.

The developed questionnaires targeted both adults and children. Details of the ethical form for the adults' survey are found in the appendices (2 & 3). Further requirements were considered in the ethical approval for the children's survey. The following are the additional points added to the ethical form for the children's survey:

- Neither your teachers, nor your parents or your classmates will have access to your answers;
- Your answers are very valuable to the researcher for further studies;
- Your answer is protected and secured;
- The researcher will not obtain any information about you (your personal information, your school name, etc.);
- If you do not wish to participate in the research study, please decline participation by clicking on the "disagree" button.

The research process was conducted in a number of stages as follows:

Stage one: Extensive work was conducted throughout the research period to identify information security best practices worldwide which have been designed to reduce the

impact of culture on information security. Information security best practices were targeted in this thesis to analyse initiatives to reduce the cultural attributes that are considered a hurdle to information security compliance.

Stage two: A cultural investigation process was instigated to identify the social contribution to computer user behaviour towards information security. The investigation process considered different countries with different attitudes to the phenomenon of sharing sensitive information.

Stage three: Different information security initiatives were analysed in order to minimise the risk of security and privacy attacks that are inherent due to the cultural attributes identified in this research.

Stage four: Cybersecurity strategies for several countries that consider information security awareness and education were critically analysed in order to find an effective solution that contributes to reducing the effect of cultural behaviour in information security.

Finally, in order to design a strategic information security education framework that considers cultural background, an intervention study was conducted to cover certain aspects that contribute to minimising the information security risks in the digital world.

1.6 Thesis Contributions

The main contribution of the research is the development of a framework for information security education that can be utilised as a strategy for the UAE for reducing the information security risk arising from cultural and social relationships among family members and friends. The framework also includes information security education guidelines that provide different scenarios of information sharing and the impact of these activities followed by some mitigation and education strategies.

Secondary contributions of the thesis are:

- A critical analysis of the human factor in information security systems and the limitations and weaknesses of the current practices for reducing information security risks;
- A detailed analysis of the role of culture in human behaviour and its impact on information security and identification of the risks of sharing sensitive information;

- Design of a questionnaire to investigate the impact of sharing sensitive information among family members and friends on information security. This questionnaire was designed to focus on areas such as: personal belongings, work belongings, and trust and social influences of family members and friends. The design also reflects the risk and impact of such activities and the relationship between the work and home environments;
- A critical assessment based on a quantitative approach of school students before and after being taught on information security. The analysis test revealed a significant difference between the two assessments;
- A critical assessment based on a qualitative approach to analyse the differences between a group before and after being taught on information security.
- A comparative study of sharing sensitive information among friends and relatives between the UAE and other GCC countries (KSA, Oman). The study revealed cultural similarities of sharing sensitive information with friends and family members, which can lead to compromising digital authentication;
- A comparative study of sharing sensitive information among friends and relatives between GCC countries and the UK. The study revealed a significant difference between the two groups.

Based on an analysis of information security strategies for the U.S., the UK and Australia, the thesis also arrived at the following recommendations:

- In the U.S. advising the end user not to share their access control with anyone is not sufficient. Rather, educating the end user about the risks and impact of sharing sensitive information in all environments (home, work, school, etc.) is necessary for a national security;
- Although sensitive information sharing happens in the UK on a smaller scale in comparison to the GCC countries, the UK cybersecurity strategy 2011 may also need to consider the education of sharing preferences of citizens among their friends and family members;
- The Australian cybersecurity strategy 2009 should focus on the design of security awareness tools and consider the sharing of sensitive information

among family members and friends in both home and work environments. It is also worth investigating the sharing phenomenon and how it is related to the cultural norms, behaviour, attitudes and trust;

1.7 Thesis Structure

Chapter One: Introduction

This chapter provides a brief introduction to information security and the cultural influence on ICT. The chapter also provides a background of the United Arab Emirates' information security and security initiatives towards local cybercrime incidents. The aim, objectives and scope of the thesis are clearly presented in this chapter.

Chapter Two: Human Behaviour in ICT Services

This chapter provides an introduction to information security as part of Information and Communication Technology (ICT) services as well as the security controls used to secure data. The chapter also covers information security issues worldwide and the protection initiatives developed to reduce the impact of human behaviour.

Chapter Three: The Role of Culture in ICT Services

This chapter presents some elements of culture in ICT in several countries. It also provides analysis of the organisational culture and its role in creating an information security culture that aims to enhance information security awareness.

Chapter Four: Culture and Information Security

This chapter consists of two parts. The first part contains the pilot study of this research that investigates the privacy sharing preferences among family members and friends. This part also aims to build a further understanding of the cultural impact on information security in the UAE. The second part considers three other countries: Saudi Arabia (KSA), Oman and the UK and aims to establish the extent to which cultural attitudes and behaviour can impact information security. The overall aim of the chapter is to present a clear picture of the cultural influence on sharing sensitive information among family members and friends.

Chapter Five: Social Engineering Attack Mitigation

This chapter considers several potential mitigation measures for further implementation that respond to both issues of cultural influence and lack of information security

awareness.

Chapter Six: National cybersecurity Strategies: Response to Password Sharing

This chapter provides a critical analysis of the cybersecurity strategies of several countries with a particular consideration given to password sharing. The aim of this chapter is to find a possible solution to the problem of sharing sensitive information among family members and friends. The chapter also analyses the governmental initiatives of the GCC countries to respond to sharing of sensitive information.

Chapter Seven: Strategic Information Sharing Security Framework

This chapter covers the intervention study that has been designed to reduce the impact of sharing sensitive information amongst others. The intervention study considered several aspects in its design, such as devising taught material to address sensitive information sharing, the implementation of the taught material and a series of surveys to test applicability and assess the results of the implementation. The chapter further provides a strategic framework based on the intervention study.

Chapter Eight: Conclusion and Further Work

This chapter provides a summary of the results obtained from this research. It also includes the information security education framework designed to reduce the likelihood of sharing sensitive information with family members, friends, employees, and even with strangers. The chapter includes recommendations based on the findings and aspects of further work.

1.8 Related Publications

1. Alkaabi, A., Maple, C., Yue, Y. (2014). User Attitude and Behaviour towards Information Security. *Social Influence in the Information Age Conference*, February 2014, King's College.
2. Alkaabi, A., & Maple, C. (2013). Cultural impact on user authentication systems. *International Journal of Business Continuity and Risk Management*, 4(4), 323-343.
3. Al-Kaabi, A. & Maple, C. (2012). Cultural Impact on Information Security: The Case of Arab Culture. In *IADIS International Conference e-Society*, 2011 (p. 391).

CHAPTER 2: HUMAN BEHAVIOUR IN ICT SERVICES

This chapter provides an introduction to information security and the security controls that are used to secure data. The chapter also covers information security issues worldwide and the protection initiatives developed to reduce the impact of human behaviour.

Sharing sensitive information with others is an end user issue in ICT. This chapter includes a detailed analysis of the issues with sharing sensitive information and the associated threats and impacts on both individuals and organisations.

2.1 Information Security

Throughout history information has always been a valuable commodity. It ensures the security of nation-states, empowers people, spreads education and advances businesses around the world. In today's society, information must be properly secured to prevent it from becoming vulnerable to criminals and hackers via the Internet. The spread of information technology and the corresponding security of that information are critical to governments, businesses and cultures around the world. The influx of information and communication technology to developing areas of the world increases literacy rates, women's education, and political stability and helps the economy.

Societies have attempted to secure information for thousands of years. The first attempts to secure information involved basic cryptography to obscure a message so it could be passed from originator to receiver without fear of interception. The first attempts involved a simple substitution system; other letters, numbers or symbols replaced a counterpart letter. With the key, or some critical thinking and time, one could decipher the message easily. As time progressed, the methods of information security grew in complexity. Perhaps the most famous encryption device is the Enigma Machine used by the Germans during World War II. The machine worked by an advanced three to five rotor scrambler. After a message was typed, the rotors would be set to a three to five letter code and then the message would be scrambled. The recipient of the message would set their machine to the same three to five letter code and decrypt the message (BBC, 2014). The methods are similar to those used today to encrypt information, trade secrets and military information (SANS, 2001).

Our modern system is much more advanced than the early methods of encryption and has a language all of its own. Definitions are broad but information technology can encompass anything from educational information to the most critical national security information. Information and Communication Technology is generally considered to be technologies that provide access to information through technology. This includes the Internet, wireless technologies, telephony technologies and other communication mediums. Information Security is any method used to restrict access to information.

Information security is present in almost every aspect of daily life. Passwords are the most common method of security but they do present problems. Poorly selected passwords, reusing passwords, incorporating easy to identify or guess elements in passwords, as well as not changing passwords frequently enough, result in reduced security (OUCH, 2013).

The most extreme method of information security is the use of an “air gap” between a computer or a computer network and the Internet. This lack of connection means information is less susceptible to information attacks or theft via the Internet. The system is, however, not fool-proof, as the Iranian nuclear programme at Natanz was infected with the Stuxnet virus without a connection to the Internet. The advanced virus code was able to replicate itself through emails, USB devices and computers that were then taken into the standalone system. The virus mostly operated on its own with the first sign of success being the shutting down of the reactors in the Natanz facility (Lagner, 2013).

Information can be protected in a number of ways beyond encryption methods. Physical security is arguably as important. Physical security can be anything from separate rooms with keyed or biometric access, restricted facilities or guards.

Many systems rely on passwords to gain access but passwords can be broken or stolen, allowing unauthorised users access to the information. One method of verifying the user is genuine is utilising unique biological signatures of users by way of biometric security systems. Biometric systems are those that rely on a biological signature to allow access to information. This could include DNA, ear, face, fingerprint, gait, body motion, hand geometry, vein pattern, iris, retina and odour. Biometric data could also include non-DNA based information such as keystroke patterns or signatures. Since the biological signatures of a human are fairly unique, this can provide a good measure of security.

Fingerprint scanners are the most common biometric device available. Outside of

computer technology, fingerprints have been used as identification since the turn of the 20th century, when fingerprints were first used to gain a conviction in a murder case (History.com, 1905). Nowadays, the process of comparing fingerprints is done automatically by scanners. The technology has become increasingly common even for consumer electronics such as the iPhone 5 (Apple, 2014). Fingerprint scanners do present some security problems, however, as they can be easily spoofed. A simple photocopy of a fingerprint which was enhanced only by using a magic marker to make the finger impression lines dark enough for the scanner to read was enough to fool a high-end fingerprint scanner (Boneh & Shaw, 1998; Shubinsky & Sobel, 2013).

Iris scanners identify and compare over 200 points on the iris and are one of the fastest and most secure biometric systems available. In high-stakes businesses such as banking or government, iris scanners are gaining popularity and will continue to do so as eye scanners become more affordable and integrated into hardware (Havenetidis, 2013).

Given the ability for any of the biometric systems to fail through one of their weaknesses, there is a good argument for combining methods to achieve enhanced security. This would achieve higher security although it would come at a price, both financially as well as the time needed for a user to pass multiple authentication procedures.

Authentication tokens are another, less high-tech, method for identity verification and controlling access to information. It is a physical object the user must have to verify their identity for the system. It could be a key fob, magnetic strip card or USB stick. Often, it is paired with a pin number, much like an ATM card used at a bank (Rouse 2005). These are often used as they are both secure and inexpensive to make for employees or others who need to access the materials.

2.1.1 Vulnerability of Information Security

Information technology is penetrating the entire value chain in each of its points, transforming the way activities are performed and the nature of the interconnections between them. It is also affecting the competitive landscape and reshaping the way products and services meet customer needs. These effects explain why Information and Communication Technology has acquired strategic significance and why it differs from many other technologies.

ICT is well known for being increasingly linked to technological advancement. Advances in technology, while necessary, often need to focus on a particular area of expertise to

meet the specialised needs of different industries, whereas ICT is concerned with every aspect of organisational behaviour. Moreover, this new emphasis on the specialisation of different industries has led to the creation of new positions in the IT field.

As we move forward, the need for and dependence on ICT grows tremendously. This tendency toward the omnipresence of ICT is elevating the necessity, yet difficulty, of information security. There are more threats than ever before; the main aim of information systems is to be secure rather any other functionality. Although information security is growing, the number of websites with information and tools that can be used even by novices to attack systems and their information is also increasing (Denning, 2003).

A security breach that has been in the news most is the theft of information from Target. It is estimated that 70 million customers were affected. There were early indications of a breach from the FireEye security system used to monitor the network (Finkle, 2014). These warnings were not acted upon by those in charge of Target's information security because it was only one of hundreds of alerts received by the team and the information trail left behind was negligible. A US Senate report on the investigation of the breach was not forgiving of the Target information security department. The corporate offices of Target have apologised and attempted to gain back the trust of its customers by offering credit monitoring services at no charge to customers (Reuters, 2014).

Banks are particularly vulnerable to information security attacks. There has been a long history of bank breaches which bring a high cost to the industry and consumers. In 2012, Citibank's UCard system was attacked and information about its users was stolen. The personal information of 465,000 users was compromised. This type of information can be used for identity theft or manipulating the information to steal directly from the banks in a scheme similar to the one perpetrated by a network of hackers targeting ATMs. The hackers were able to find vulnerabilities in the security practices of credit card processing companies, remove the limits, and use reproduction cards to withdraw \$45 million in a matter of hours (JPMorgan Chase Cyber-attack, 2013).

Other banks have also been targeted with success. Barclay's investment branch was targeted by hackers who successfully stole entire customer dossiers in 2013. This included names, addresses, loan information, medical history, passport numbers and other critical information. With this wealth of information available to them, criminals would

have an easy task of stealing the identities of Barclay's clients (Van Doom, 2014).

As a result of these attacks, banks have taken precautionary measures in information security practices. Expanding the importance of security practices across the entire company culture rather than leaving the brunt of the effort focussed within the IT Department has been an important move. Making all employees aware of security practices and motivating them to become an active part of the information security of the company has led to faster identification of information security threats (Denver Business Journal, 2013).

Banks and private corporations are not the only targets for information security attacks. In 2006, the Department of State suffered a large-scale intrusion from an unknown source. The intrusion began as an email sent from a legitimate-looking email address. Upon opening the attachment, a programme was executed that allowed outside access to user accounts and passwords.

The intrusion was detected quickly and only the non-classified systems of the Department were compromised, but the resulting security measures did force restricted Internet access and required new accounts and passwords for many of the system's users (Wright, 2006). The Department also had to disable its Secure Socket Layer system which allowed the transmission of encrypted data (State Department Suffers Computer Break-in, 2006). At the same time, the Defense Department and other US agencies were also experiencing difficulties, attempts and intrusions. China was the most obvious suspect as they are focusing large efforts on hacking as part of their military programme; however, the source of the Department of State intrusions was never identified (Lagorio, 2006).

Technology has introduced complex capabilities for information sharing, yet has brought complexity in protecting that information (Anderson 2006). According to Ko & Dorantes (2006), information security breaches have been increasing in recent years. The impact of such breaches affects different prospects of the financial, reputational and private natures of an exposed organisation and may lead to further vulnerability issues (Anderson 2006). Cavusoglu et al (Cavusoglu 2005) also suggest that there have been dramatic increases in the number of IT security breaches in recent years, making ICT security a major concern in ICT management. Consequences may include data corruption, data loss, privacy loss, downtime, fraud and loss of public confidence (ITU, 2003).

A security risk occurs when a security vulnerability is associated with an exploit. For

example, buffer overflow in an operating system application is a vulnerability that can be associated with a hacker's knowledge strengthened by appropriate tools to generate access (i.e. an exploit to compromise a Web server) (ITU, 2003).

Associated with the growing threats, increased security measures have become the primary concern in the internal development of organisations over any other information technology related field (Luftman, 2004), triggering a set of preventive considerations that need considerable time and effort on the part of the organisation in order to protect its assets as much as possible.

According to NIST (NIST 2002) an effective risk management process should protect not only the organisation's ICT assets but also its ability to perform its mission. Although effective risk management and security processes should involve decision makers in information security management and operations, there is little research, as well as lack of best practice, on what aspects decision makers should base their security-related decisions (Schroeder, 2005). Accordingly, the risk management process must be treated primarily as an essential management function of the organisation rather than a technical function carried out by the IT experts who operate and manage the IT system in the organisation (Stoneburner, 2002).

After the numerous security breaches over the last decade, businesses are beginning to share cyber threat and other data security information but this has been met with some regulatory resistance. Regulators had a concern that cyber threat information would be similar to competitive information such as pricing and market strategy and would therefore violate antitrust regulations. However, the Justice Department recently ruled that the ability to share this information would not violate the regulations. Cyber threats and information security breaches are becoming more of a concern and allowing businesses to share such information should prevent and mitigate attacks and loss of information in the future (Wyatt, 2014).

There is a perception that information security is a task solely for the IT department in a major business or government but, with the growing importance of information and its parallel growth in importance, more focus needs to be placed on security at the larger organisational level.

2.1.1.1 CIA Loss

Information security triad Confidentiality, Integrity, Availability (CIA) loss is another

consequence of sharing sensitive information. Janczewski and Fu (2010) asserted that both organisations and individuals have suffered enormous loss from social engineering attacks. However, the threat is constantly overlooked because awareness about this loss is currently low. As a result, the password sharing problem can potentially lead to significant loss of assets for both organisations and individuals. The table below shows the potential damage to the information security triad for both organisations and individuals (Figure 1):

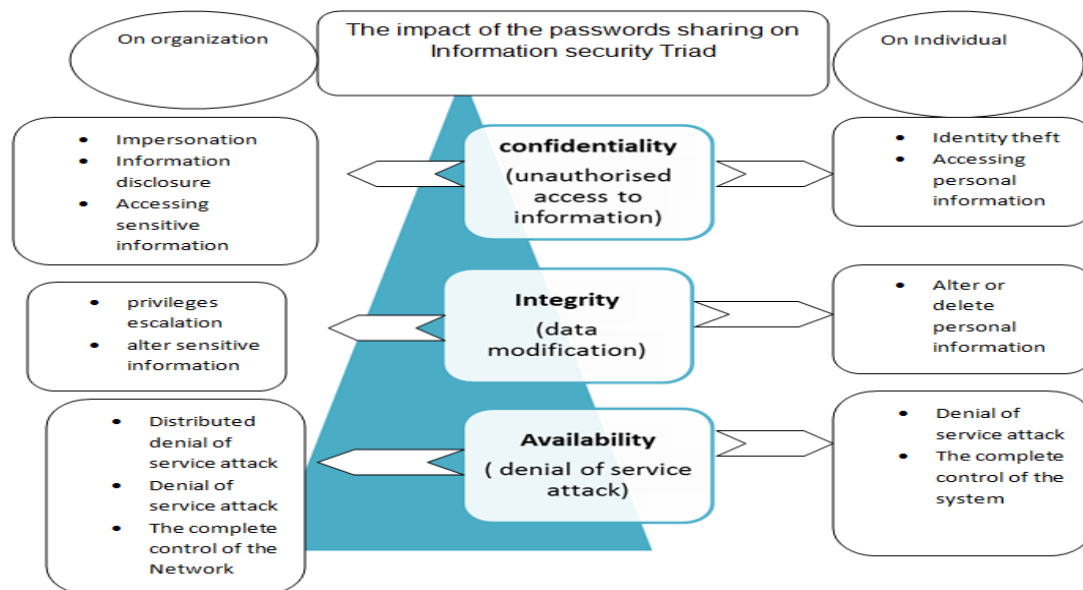


Figure 1: Password sharing threats against information security

Password sharing is considered a dangerous habit as it contributes greatly to information security violations specifically on confidentiality. The consequences that might result from breaching confidentiality are quite drastic and can take the form of identity theft, sensitive information disclosure and unauthorised access to confidential information. Identity theft is a serious crime that merits due consideration and adequate prevention and combating (Chawki and Wahab, 2006). Typically, performing identity theft attacks on individuals involves collecting information about the victims over the Internet. Aggregation is performed in the second stage and gaining access at the final stage. However, conducting social engineering attacks and obtaining the password of the targeted person does not require performing the above lengthy procedure in certain environments where password sharing is permitted. Similarly, counterfeit or stolen vendor or employee ID can give access to a secure location where the attacker can then obtain access to confidential information (Newman, 2006) and therefore confidentiality of the information security triad is compromised. As a result, people whose identities

have been stolen can spend months or years and a lot of money cleaning up the mess generated by the thieves' exploitation of their good name and credit record (Chawki and Wahab, 2006).

The term integrity in terms of information security means that data may be altered or modified only by an authorised user. Applying this definition to password sharing will demonstrate the huge threat that can result from integrity violation. This can be seen when someone with an admin account shares his password with his colleagues. The threat of having access privilege may result in the modification of sensitive information that should only be accessed by limited and authorised users. In addition, when only authorised users store information on some digital devices, that information should remain secure and preserved on its integrity, and if that information requires changes or modifications, changes are allowed to be done by only those authorised to do so.

Preventing legitimate users from accessing the system is another primary target for hackers. This hacking activity is known as a denial of service attack. Knowing the target system password can allow complete control over the system. This can increase the chance of changing the legitimate user's password and consequently prohibiting system access. Similarly, triggering the distributed denial of service attack on an organisational level could benefit the social vulnerability of sharing passwords. Such attacks, that attempt to deny computer and network resources to legitimate users, will have a significant impact on the information security triad (Newman, 2006).

2.1.1.2 Social Engineering Attacks

Social engineering is a technique that aims to break into a system and is where the attacker manipulates people instead of technology to bypass the security mechanism (Hadnagy, 2010). This can be illustrated by the ability of a social engineering attack to compromise authentication and consequently jeopardise the security triad.

Researchers suggest that every information system should have deterrence, prevention, detection, response, and recovery security measures in order to have a comprehensive protection of its assets and avoid cybercrime occurring. It is important, however, that security measures should include both social and technical measures (Mwakalinga & Kowalski, 2011). This is due to the fact that hackers use both social and technical measures in attacking or in gathering information before the attacks (Mwakalinga & Kowalski, 2011).

Sharing sensitive information, including passwords, is a social vulnerability to a system. Social engineering is a highly attractive method of gaining access to sensitive and valuable information. The ability to perform such an attack is relatively easy as opposed to the conventional methods such as technical vulnerabilities or system penetration methods (Hinson, 2008). The Phishing attack is one of the best known attacks in the field of social engineering. Phishing involves the use of emails or malicious websites for attacking purposes. There are some other attacks under the social engineering attacks' umbrella such as scareware, rogueware, and ransomware attacks (Koch et al, 2012). Due to the decrease in the effectiveness of technical-based attacks as technological security solutions are gradually being adopted by many users and organisations (Janczewski and Fu, 2010), the alternative social vulnerability threat will be further utilised by hackers who try to gain unauthorised access to the system.

Social engineering is a major concern for organisations due to its effective results in compromising a system by exploiting users (Newbould and Furnell, 2009). These are challenging not only to individuals and organisations but also to the law enforcement community. Social engineering attacks are more challenging to manage since they depend on human behaviour and involve taking advantage of vulnerable employees. Therefore, an exploit may lead to a major breach to an organisation whereby the social engineer can have complete control of the system, allowing privilege escalation or launching a denial of service attack (Liu and Cheng, 2009). Businesses today must utilise a combination of technology solutions and user awareness to help protect corporate information (Dimensional Research, 2011).

The figure below (Figure 2) depicts the potential risk of exploitations and the impacts when information is shared:

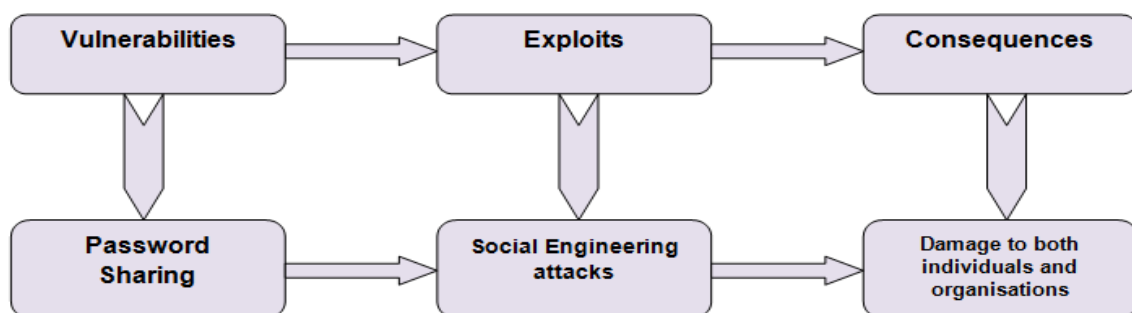


Figure 2: Potential risk exploitations and impacts when information is shared

2.1.2 Human Factors in Information Security

According to numerous studies in this field (CSFI, 2010), effective information security may be impeded by the so-called human factor. Deloitte (2005) maintains that employees are the main hindrance to effective information security policies and standards.

Woodhouse (2007) maintains that the better employees are at applying the controls, the more secure the organisation will be, as even the best designed technical controls and procedures will be of limited value if the staff involved do not understand why they have been implemented and what they aim to accomplish.

Staff-caused risk is recognised as being high on the list of security risks (CSI, 2006), for example in the form of unintentional or malicious misconduct or misconfiguration of the organisation's machines, resulting in mostly (73%) of the unsophisticated cyber-attacks according to a recent report by 7Safe UK (2010). Direct losses are usually large, in addition to immeasurable indirect damage.

According to ReedSmith (2010), employees are identified as a major source of identity theft risk in two major studies: Kroll Global Fraud Report - Annual Edition 2009/2010 and Verizon Business RISK Team, 2009 Data Breach Investigations Report. Furthermore, ReedSmith has advised on over 150 data breach incidents over the past 5 years and employees were players and/or victims in most incidents. ReedSmith showed that more than 20% of breaches were caused by employees, 50% of whom were IT administrators and 50% were end-users. About 2/3 of such breaches were deliberate whereas 1/3 were accidental, resulting in:

- Abuse of system access/privileges;
- Violation of PC/email/Web-use policies;
- Violation of other security policies;
- Embezzlement.

When the cause of a breach is internal, the number of records compromised almost triples, compared to that of external breaches. It also takes much longer and is harder to detect internal breaches. The consequences can range from service availability failures to leak or loss of confidential data (ReedSmith, 2010).

2.1.3 Insider Threats

Although every organisation defines its insider threat according to its own core business, the following are some definitions of the insider threat towards information security.

“An insider is a trusted entity that is given the power to violate one or more rules in a given security policy. Enforcement mechanisms are not applied against those trusted users. The insider threat occurs when a trusted entity abuses that power” (Bishop, 2005, p. 78).

“The threat is attributed to legitimate users who abuse their privileges, and given their familiarity and proximity to the computational environment, can easily cause significant damage or losses” (Chinchani, 2005, p. 1).

Insider threat is one of the biggest issues that information security systems face today. An organisation’s employees can pose a threat where they have almost a complete knowledge about the network design and security measures used, as well as the sensitive information that they access to accomplish their routine job. The threat is apparent and the security measures applied become weak as long as a human being is involved. The loss that results from the insider threat can have a big impact on the organisation in terms of finance, plans and strategies, disclosure, reputation, and sensitive information sharing (Munshi, 2012) but the insider threats remain inadequately addressed by organisations and hence it will be a growing concern over coming years (Potts, 2012).

Of course, information security can never be completely effective. Someone working from within the system has a unique opportunity to steal information from behind many of the security protocols. Edward Snowden is a prime example of this type of threat. Whether history will label him whistleblower or traitor remains to be seen but, regardless, he worked from behind NSA’s considerable security to take information and make it public. Due to his assignment to create backups of immense amounts of data, he had almost a free reign to make copies of the information and hand them over to the press. No amount of computer or physical security can safeguard information from someone who has a legitimate access to it. Developing better background check procedures and employee outreach has been put forward as the most effective method to deal with insiders (NPR, 2014).

Insider threat is differs from the outsider threat where the opportunity to access the network assets is legally authorised for the insider. However, the insider threat plays a significant role to build up the outsider threat by using its privileges to access any sensitive information that seem interesting to the outsider. The damage can also exist when an ex-employee has background knowledge about the network design which

increases the chances of a breach by an outsider (Li, 2005).

There are different approaches that can reduce the occurrence of the insider threat according to several researchers (Pfleeger &Stolfo, 2009), (Guido & Brooks, 2013), (Alawneh, 2012) and (Colwill, 2009). Those approaches vary according to domain and are shown in the table below (Pfleeger &Stolfo, 2009).

Table 1 - Applying a framework for responding to insider threats (Pfleeger &Stolfo, 2009)

	Organisation	System	Individual	Environment
Detection		Embedded decoys, Watchful Monitoring		
Prevention	Create organisational policy	Embed organisational policy	User training, incentives, reminders, access control	Remind users of legal implications of their actions and of costs to organisation
Mitigation	Update related policies			
Punishment				Apply legal punishments
Remediation	Update related policies			

One of the biggest issues that affect information security protection from the insider threat phenomena is the cultural behaviour background as it is difficult to mitigate this threat (Crossler et al, 2013). According to Colwill (2009) in order to examine the insider threat, national and regional culture should be taken into consideration as it is has an impact on attitudes and effectiveness of levels of information protection. This is apparent when conducting business since every region has its own style for doing business. He also asserts that practices prohibited in the Western world, for instance the giving of substantial gifts (namely bribes), may be a normal activity and accepted behaviour in some regions where the wheels of business have to be “oiled” (Colwill, 2009) As a result, culture can impede the security measures applied and hence can damage the organisation.

2.1.4 Privacy Issues in ICT

Advances in ICT infrastructures have opened up new dimensions in communication and virtual connectivity. It is now easy to access, share, store, replicate and even manipulate information and images using ICT. The technologies involved in ICT have reduced the effort and time needed to communicate, and this is no doubt a welcome development for many people. Yet, and as Olanreqaju et al. (2013) observe, authentication and protection

of much of the information shared through ICT services remain a concern not only to individuals but also to corporate bodies, non-governmental organisations and governments. The risk of hackers and intruders is ever lurking, and there is a possibility that they can access confidential information, use it, alter it or even delete vital information. The effectiveness of ICT services therefore calls for effective technology whose security and privacy can be guaranteed. Yet, in a world where any security issues are being challenged, it is unclear if absolute privacy in ICT services will ever be achieved. The absence of privacy guarantees is even worse considering the absence of a legal framework which would provide deterrent or punitive measures to perpetrators who breach people's privacy.

The concept of privacy has been defined variously as “an individual condition of life characterised by exclusion from publicity” (Britz, 1996); “the right to be let alone” (Moore, 2008), or “the state of possessing control over a realm of intimate decisions, which include decisions about intimate access, intimate information, and intimate actions” (Inness, 1992). A right to privacy, therefore, can be understood as a person's right to control inner spheres of their personal information, body, powers and capacities. As Moore (2008) indicates, “it is a right to limit public access to oneself and to information about oneself. In the United Kingdom (UK) today, the right to privacy is represented in the Human Rights Act (HRA) 1998, which has its basis in the European Convention on Human Rights (ECHR) article 8 (Equality and Human Rights Commission (EHRC), 2011). Despite the existence of the Human Rights Act (HRA), there have been concerns in the UK that the law has lagged behind, especially in the wake of changes and advancements in ICT services (EHRC, 2011). Consequently, it has been argued that the state, which has the mandate to uphold people's and organisation's right to privacy, is failing in fulfilling that mandate.

2.1.4.1 Sensitive Information Disclosure

People and institutions can share sensitive information either knowingly or unknowingly. The sharing of sensitive information (e.g. name, address, financial information, health records etc.) is commonplace, particularly when dealing with institutions such as banks, government agencies, hospitals, institutions of learning or insurance companies. Once a person gives out their confidential information, they do so with the expectation that the recipient body will not disclose such information to third parties. Yet, it has been seen that such institutions are prone to breaches of privacy, where some of the information

stored in their computer databases is lost, compromised, or altered. Olanrewaju et al (2013) for example note that Medical Identity Theft (MIDT) is one of the most common crimes in the healthcare sector. MIDT is defined as a specific type of identity theft that occurs when a person uses someone else's personal health identifiable information. Such identifiable information includes the names, addresses, birthdates, security numbers and healthcare providers of patients. MIDT (especially in the US) has been conducted by organised and sophisticated hacking groups who access electronic medical records stored in hospital or insurance company servers. The hackers then use MIDT to obtain prescription drugs and medical drugs, amongst other things, using patients' names and details (Olanrewaju et al, 2013).

Governments also lose confidential information entrusted to them by private citizens and organisations. In the UK, for example, in October 2007 HM Revenue and Customs lost two computer discs (EHRC, 2011). The discs contained names, addresses, bank details and national insurance numbers of families who had filed benefit claims. Unlike hacking, which is often an external criminal attack, the discs were lost through the negligent practice of officers who had sent the discs via a courier service to the National Audit Office. It later turned out that the officer was neither authorised to access the files nor send them. It was argued that the loss of data was not only negligence on the officer's part, but also by senior management (EHRC, 2011).

Ways through which involuntary revelation of information and passwords occur include theft or loss (where unsecured paper files, electronic media, portable electronic devices and computers are lost or stolen) or through unauthorised access to insecurely transmitted or stored personal identity information (PII) and sensitive information (this can happen if files are stored in a publicly accessible 'place'). Additionally, passwords can often be hacked because hackers are able to take advantage of missing operating system updates or security patches. In some cases, users make their passwords too simple thus making hacking an easier undertaking. Furthermore, virus infection on computers can make PII inaccessible, meaning that even important information about people stored in computer databases is rendered unusable. Additionally, insecure disposal of data-containing devices is also a major way through which people and institutions inadvertently share sensitive information (UC Santa Cruz, 2014). A case in point is when an institution of learning sold two hard drives on eBay without wiping the data. In the UK, cases of lost *Universal Serial Bus* (USB) discs containing sensitive information about people in

several institutions have been reported (EHRC, 2011). It is also possible that a compromise of contractors' computers can expose PII.

In addition to the involuntary disclosure of information and passwords, UC Santa Cruz (2014) observes that people unintentionally reveal their passwords by replying to phishing emails or clicking on links in emails. An example is when a faculty physician “unknowingly provided the user name and password of his email account in response to an email message that appeared to come from the university’s internal computer servers” (Miaoulis, 2009). Other scenarios that may involve sharing of sensitive information include online shopping (where the identity of the purchaser needs to be verified) and registering or subscribing to specific online services (usually a person’s email address and screen name are required). Some sites may also ask for personal information that includes age, nationality, gender, physical address, photos etc. There are also competitions that require the competitor to fill in their demographic details, personal interests and other types of personal data. Other examples include virtual worlds (including online games), which require a person to provide personal details during registration (Commonwealth of Australia, 2014).

2.1.4.2 Password Sharing

A study on banking and security (Singh et al, 2007), conducted in Australia, has shown that the practice of password sharing does not conform to standards. The study reveals that password sharing occurs in different scenarios, such as with family relationships as an expression of trust, remote indigenous populations as the only feasible way of getting banking services that are far from major population centres, and with people with disabilities who need the help of others with their banking. The authors recommended using user-centred security approaches and emerging work on security in the organisational context. They argue that security design should consider the social and cultural practice. Otherwise, users would have to be individually kept under surveillance in the workplace, which is not feasible. Ignoring the social and cultural design of security solutions may lead to a reduction in security.

In a similar study in the US by Stanton et al (2005), sharing account information with a friend is one of the ten most extreme end user behaviours. The same study showed that 23% of respondents sometimes reveal their passwords to members of their work groups, 7% share their passwords with someone in their company but outside their work group,

and 4.1% share their passwords with someone outside their company. Stanton et al (2005) considered that user behaviours are crucial for any user-related information security policy. The authors maintained that end user behaviours intertwine inextricably with the overall effectiveness of security. They therefore suggested having a systematic view of end user behaviour in order to allow accurate auditing and assessment of this behaviour in order to be considered in effective security.

A study in a Swedish public nursing centre (Harnesk and Lindström, 2011) showed that users at the nursing centre had a record of jeopardising privacy of care takers by sharing passwords. This eventually led to other users developing harmful security habits over a long period of time and avoided taking responsibility for their own user credentials; instead they used the competencies and skills of others to log on to domain-specific applications. The authors argued that discipline and ability control the main aspects of behaviour in an organisation as a result of the existing culture and the selected security management approach. They suggested that security managers better recognised how different security behaviours affect the outcome of inscribed security. They maintained, however, that further research into the domain of security behaviours was needed.

Chryssanthou et al (2011) propose that organisational culture may need to be addressed in security management procedures. The authors argued that an organisation with a culture that allows its staff to share confidential information amongst each other, without proper authorisation, would certainly find it extremely difficult to prevent its staff from sharing their usernames and passwords. The authors suggest making sanctions in order to prevent and control the information sharing issue in such organisations.

In a survey study, Alarifi et al (2012) showed that information security awareness in Saudi Arabia is relatively low, causing a high level of information security attacks in the country. The authors referred that to the tribal nature of Saudi culture. The study showed that the general public was either unaware of the recommended security procedures or deliberately chose not to abide by them. The study concluded that the most appropriate methods of disseminating information security awareness were through web portals and newspapers because these methods address the problems of distance and strict cultural controls.

Al-Hamar et al (2010) cites several incidents of Qatari citizens who fell victim to phishing attacks because of different factors such as culture, country-specific factors,

interests, beliefs, religion and personal characteristics. The author also asserts that information security awareness was imperative in order to mitigate the risk of a social engineering attack.

2.1.4.3 Impact of Sharing Sensitive Information

The impact of sharing sensitive information can range from harmless (but nevertheless disturbing), to costly consequences which may affect one's financial wellbeing, personal integrity, and some may even lead to criminal charges.

2.1.4.3.1 Spam

One of the most harmful consequences of sharing sensitive information is spam mail being delivered to one's inbox (Commonwealth of Australia, 2014). Spam is a generic name used to refer to electronic junk mail. This kind of mail can be delivered to one's email inbox, through instant messaging, Multimedia Messaging Service (MMS) or Short Message Service (SMS). The latter two are delivered to a person's mobile phone particularly in cases where their mobile phone numbers have been revealed to third parties. Spam messages can contain information related to marketing of products or services, while some may contain fraudulent or offensive material; others can contain computer viruses or phishing content (Commonwealth of Australia, 2014).

2.1.4.3.2 Fraud

Internet-based fraud is another consequence of sharing sensitive information. Fraudsters seek personal details from targets and those details are later used for deceptive undertakings, including obtaining money using their targets' PII. Closely related to Internet-based fraud is identity theft, which the Commonwealth of Australia (2014) defines as a "type of fraud that involves stealing money or gaining benefit by the perpetrator pretending to be someone else" (p. 6). The Organisation for Economic Co-operation and Development (OECD, 2008) defines ID theft as occurring when "a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an authorised manner, with the intent to commit, or in connection with, fraud or other crimes" (p. 2). Some of the ways through which ID theft is committed include the use of malware, spam, phishing and hacking. After obtaining PII, the perpetrators then misuse the victims' existing accounts (e.g. credit card accounts, Internet accounts such as email accounts, Facebook and other social networking sites), medical insurance accounts, bank accounts, and telephone accounts amongst others. The perpetrator could also open new

accounts using the victims' personal details. When this happens, all the billing for the new accounts are placed in the victims' account. That means that they lose money. It is also possible for perpetrators to use stolen identities to commit other frauds, which include obtaining government benefits, medical services or supplies, or even giving it to the police if stopped for a crime (OECD, 2008).

2.1.4.3.3 Scam

Another consequence of sharing sensitive information is that people can become a target of many scams. Scams are often disguised as lotteries, for example the targeted person receives an email stating that he or she has won a prize and, to claim the prize, they are required to pay a small fee. Scams can also be implemented as advance fee schemes (also known as Nigerian 419). Here, the scammer offers to leave a substantial amount of money to the target, but he or she is first required to pay some fee to transfer the claimed money from a foreign account. Another type of scam is mule, which is a form of money laundering activity where victims are involved in transferring huge amounts of money between accounts. The victim, if caught by the authorities, may face criminal charges. Perpetrators of such crimes also use phishing (emails sent from spoofed or falsified emails). Phishing is a major source of identity theft (Commonwealth of Australia, 2014). Industrial espionage is also a likely consequence of disclosure of sensitive information especially when the perpetrator is able to access trade secrets or competitive advantage information about a corporate entity (Granger, 2010).

2.1.4.4 Law Enforcement

The challenge of identity theft (which is assumed to be performed by exploiting the social vulnerability of passwords and sensitive information sharing) can be extended to law enforcement too. The investigator must provide rigorous evidence to prove beyond reasonable doubt that the suspect was the person who was in control of the device when the actions took place. This can be highly contestable, particularly when the case is related to passwords and tokens as they could have been obtained and used by someone else (Jones & Martin, 2010).

Although laws concerning digital security and authorised access to systems are available in the Gulf Cooperation Council (GCC) region, the difficulty arises from ability to apply these laws. This is based on that information-sharing leaves little evidence when associated with cybercrime. As an illustration, the UAE Federal Law No. (2) of 2006 on

The Prevention of Information Technology Crimes states that unauthorised access to a system results in imprisonment and a fine or either (UAE, 2006). However, Abu Dhabi Police Department has been recently faced by a case of fraud, theft and seizure of a police sergeant who was made redundant in 1999 after being diagnosed health-wise unfit to service. The prosecutors accused the former policeman of breaking into the electronic system of the Ministry of Interior as an official and promoting himself to captain and to major eight months after using the brigadier's password. Having no evidence of breaking into the system, the judge could not reach a verdict to accuse the policeman of being guilty on the grounds of the abovementioned law. The defence lawyer has pleaded the defendant not guilty and someone else set him up by tampering with his details in the system (Alkaabi & Maple, 2013).

Overall, the sharing of sensitive information makes people all the more prone to scams, fraud and other major security breaches on their person or the institutions they represent. It makes privacy harder to achieve because hackers and identity thieves are often on the lookout to find weaknesses that exist in ICT infrastructures or social weakness in their environments. The targeted population (albeit unknowingly or ignorantly) also share their information by replying to phishing emails, carelessly storing or discarding data, or simply not taking enough precautions. Organisations, charged with guarding people's private information, also have infrastructural weaknesses, which sometimes lead to the sharing of information belonging to thousands of people whose personal information is stored in their databases.

2.1.4.5 Information Security Standards and Guidelines

With the fast incorporation of technology comes the responsibility for the security of all of this data. Customer data is perhaps the most vulnerable as the risk of identity theft is a major concern for most individuals who entrust their information to a business.

Information security standards have been adopted by information technology professionals to provide uniform methods. This has become increasingly important as sharing information over the Internet has become more commonplace, as well as vital, for business and government. There are different information security standards and guidelines worldwide which have been developed to reduce information security risks and maintain acceptable levels of information security compliance. In order to provide an acceptable security level, security standards address the minimum mandatory rules that

should be followed by organisations (Al-Azazi, 2008). Below are some of these standards (these standards have been customised by ADSIC to develop national policy for the UAE) and their ability to secure the organisation's assets:

2.1.4.5.1 *GAISP*

The Generally Accepted Information Security Principles (GAISP) was developed after a 1990 report written by the National Research Council on computer vulnerability (GAISP, 2003). The report, entitled "Computers at Risk", suggested a Committee be formed to provide overarching guidance to public and private organisations and professionals akin to those provided by the Generally Accepted Accounting Principles. GAISP introduced three levels of information security principles: pervasive (few, rarely changing) such as those of ethics and awareness; broad functional (more detailed); and most detailed (Siponen & Willison, 2009). The GAISP consists of the following pervasive principles:

- Accountability Principle
- Awareness Principle
- Ethics Principle
- Multidisciplinary Principle
- Proportionality Principle
- Integration Principle
- Timeliness principle
- Reassessment Principle
- Democracy Principle

2.1.4.5.2 *COBIT*

The Control Objectives for Information and related Technology (COBIT) was another early Information Technology framework and was first developed in 1996. The focus of this set of rules was to fully integrate the overall business plans with the IT standards necessary (Hardy, 2006). This is primarily important for those businesses or government agencies which rely on up-to-date information on a consistent basis (FAQ, 2014). COBIT provides metrics and models by which to measure the effectiveness and security of the business goals (Von Solms, 2005). COBIT is used by a number of businesses including ORACLE, Sun Microsystems, and several US government agencies as well as governments around the world (Case Studies, 2014).

COBIT has 34 objectives, which have been arranged under four groups (Lainhart, 2001;

Hadden, 2002; Abu-Musa, 2009):

- Planning and Organisation
- Acquisition and Implementation
- Delivery and Support
- Monitoring

2.1.4.5.3 ISO 27000

ISO 27000 consists of several information security best practices such as: information security management, risks, controls etc. These are designed to reduce the information security risks based on global perspectives.

ISO 27001 consists of 11 domains (ISO/IEC-27001:2005) as follows:

- Security policy
- Organisation of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

The above domains are also listed in ISO/IEC 27002 code of practice, however, the ISO/IEC 27002 only provides guidance and uses words like “may” and “should”, whereas the ISO/IEC 27001 is a set of requirements of information security management systems (ISMS) and uses words such as “must” and “shall” (Calder, 2006).

ISO/IEC 27001 and ISO/IEC 27002 are designed for use in organisations of all sizes targeting the managerial parts of information security (Calder, 2009).

Many of the testing and auditing procedures measure the information security compliance against standards such as the ISO 27000 series. The most recent version, ISO 27002, recommends information security system designs. The goal is to prevent “gaps” in security. An assessment against ISO 27002 standards can help businesses identify and

plan for remediation steps to comply with the ISO standards (Layton, 2006).

2.2 Discussion

A general consideration of information security is the ability of organisations to protect their information. International information security standards such as ISO/IEC 27001 and ISO/IEC 27002 noticeably neglect the role of culture in information security and do not allude to any culture-related considerations. Furthermore, the ISO certification does not necessitate the implementation of the standard. The IT Baseline Protection Manual, a security standard for IT systems, also does not refer to culture in its descriptions of security measures. BITS (The Framework for Managing Technology Risk for IT Service Provider Relationships) does not scrutinise any cultural impact on information security (Glaser, 2009). Andrew Jaquith (2010) of Forrester Research asserts that successful protection of sensitive data cannot be accomplished only by following a standardised set of guidelines (Search Security, 2010). Moreover, the ISO standard (ISO 27005) does not offer any specific methodology for information security risk management but leaves the organisation to decide on the suitable approach to risk management depending on the scope of its industry sector, ISMS and context of risk management (ISO 27005). Ross (2010) recognised these weaknesses in risk management methodology of the ISO 27005 standard and suggested using fuzzy mathematics theory to overcome these weaknesses.

Siponen and Willison (2009) analysed BS7799, BS ISO/IEC17799: 2000, GASPP/GAISP, and the SSE-CMM. The paper claimed that BS7799, BS ISO/IEC17799: 2000, GASPP/GAISP and the SSE-CMM were too generic and they had universal scope. The authors proposed that these standards do not consider the differences between organisations as they normally have different security requirements.

Furthermore, although the availability of several standards provides organisations with a wider margin of choice, it brings difficulties to the organisations in understanding and selecting which one to use (Al-Azazi, 2008). Tejay (2005) asserted that having many standards and the need for the organisation to adopt a minimum set of standards to cover its maximum IS security needs, defies the concept of their efficiency.

Kluge and Sambasivam (2008) researched several IS standards, namely, the ISO 27000 family, COBIT, Information Security Forum and the IT Baseline Protection Manual by the German Federal Office for IT security. The authors claimed that ISO 27001 had a process approach to security that defined operational procedures instead of describing

security technology. Höne and Eloff (2002) stated that the organisation should not exclusively rely upon security standards for guidance because of their lack of comprehensive coverage and their tendency to address the processes needed for successfully implementing the information security policy.

2.3 Conclusion

Information security issues are manifold. The lack of information security awareness represented in end user behaviour and the cultural and social impact lead to a breach to both organisations and individuals.

Confidentiality of account details and the privacy of the users are significant for protecting against identity theft. Credential privacy is an integral part of authentication, and that should remain private to the account owner in order to remain secure and protected.

Privacy is considered one of the most important needs of people in the West (Feng & Hughes, 2009). However, it is given less importance in other cultures, such as Arab culture, which is characterised by trust and loyalty (Obeidat et al., 2012). Arab employees give more loyalty to their managers than to the organisational goals (Obeidat et al., 2012). A user might share his or her account password without even realising the threat.

Information security standards and guidelines have failed to consider the role of culture in information security, Therefore, a wider scope, which considers culture, is needed in order to recognise its importance.

CHAPTER 3: THE ROLE OF CULTURE IN ICT SERVICES

As seen in the previous chapter a wider consideration of culture is needed in order to realise its importance in information security. This chapter provides an overview of culture and ICT across different countries including the Arab World. The chapter also provides an analysis of the organisational culture and its role in creating an information security culture that aims to enhance information security awareness.

3.1 Culture and ICT

Security of information is meaningless without an understanding of how the information and communication technology (ICT) affects countries and cultures around the world. The United States and the West in general have been leading the adoption of information and communication technology for a long time but the rest of the world is catching up. Countries around the world are seeing extraordinary benefits in their culture from information and communication technology.

Global integration has been happening for years but the widespread use of information and communication technology, such as the Internet, has advanced this at a frenetic pace. Countries once separated by oceans are now instantly connected using wireless video conferences. Beyond the business and economic benefits, this interconnectedness has had a dramatic impact on society in general. Supporters of the increase in information and communication technology have called it a non-return economic pathway (Ramos & Ballel, 2008).

The growth of the Internet has had the greatest impact of all the information and communication technologies. Recently, social media has been the darling of the Internet and it shows no signs of disappearing anytime soon. Twitter, Facebook, and the other hundreds of social media websites now available estimate one out of every four people in the world are active users, leading to an 18% increase over the past year alone (Web Users in the Middle East Emphasize Social Networking, 2013).

Culture may impede IT growth, whereas inappropriate consideration of the cultural aspects may result in unfortunate outcomes of IT adoption (Glaser 2009). Dutta et al (2003) argue that IT development faces significant intangible challenges of cultural attributes. In this respect, studies have shown that countries with high information

dissemination capacities are those with high uncertainty avoidance, high collectivism, high future orientation, low in-group collectivism and low gender equality practices. In addition, national culture values seem more appropriate predictors of information dissemination capacity than national culture practices (Glaser 2009).

The powers of the Internet and the ability to crowdsource are not only used by law enforcement and business in the Western World. With a complex scam of promising people money to work from home or in the “import/export” business, criminals are able to dupe innocent victims in the United States and other western countries into doing one of the most dangerous aspects of the job—receiving stolen goods and laundering them back into the system through a legitimate service such as Western Union. Other reports of criminals using crowdsourcing techniques involve tricking unwitting accomplices in the United States, Britain and Europe to solve CAPTCHA puzzles in return for access to free pornographic material. The puzzles were presented as a type of contest but, in fact, the puzzles were being used to break into Yahoo email accounts (Goodman, 2011).

Criminals around the world are also taking advantage of the increasingly easy access to technology. The criminals send out countless emails to get a few respondents. The story is usually something along the lines of a wealthy family, politician, or businessperson is stuck in troubling circumstances and wishes to leave the country with as much money as possible. They need a partner outside the country and, if you are willing to help, they will give you a large portion of their wealth. Reports vary on how much the criminals are making but a recent article in the United Kingdom estimates some scammers are making up to £250,000 (about \$400,000) a year (Jones & Hill, 2010).

In February 2014, six British citizens were charged with a new version of the scam targeting dating services (Six charged in connection with alleged Internet dating scam, 2014). Scammers create fake profiles on dating services and develop relationships with targets. Once they have an established relationship, usually some type of tragedy happens - a medical bill, a sick relative or a serious accident that they cannot pay themselves. Or perhaps they simply need the money to book a trip to visit the target. The target sends the money willingly since they believe they are in a real relationship (Dating and Romance Scams, 2014). Only after the target has sent large sums of money and the relationship ends do they suspect a scam.

Information technology and security has become a major element of our daily life. We

shop online, email, pay bills and send other personal information over the Internet on a daily basis. We trust that the businesses on the other side of that transaction have embraced security measures that incorporate the international standards such as ISO 27000. However, this is not always the case and our information could be compromised.

3.1.2 The United States

The United States has seen tremendous growth in the use of technology over the last three decades. Computers went from a novelty item to an item that is present in most homes, with 76.5% of all households having at least one computer (File, 2013).

This growth in Internet connectivity in the United States has not been an even distribution. The discrepancies in computer ownership and Internet access reflect the racial and poverty level breakdown in the United States. In 2011, 76.2% of non-Hispanic White households, 82.7% of Asian, 58.3% of Hispanic, 56.9% of Black households reported accessing the Internet from home (File, 2013). The lack of infrastructure is the main hurdle to expanding Internet access in the United States. Broadband Internet access connects 2/3rds of Americans but the lack of infrastructure leaves just 10% of tribal lands connected and the high cost leaves those with household incomes of less than \$20,000 with low connectivity rate (Rosen, 2011).

The increasing use of social media has also had an impact on solving crime. Tip lines, to inform the police of a potential suspect or share information about a crime, have existed for years - even generating TV shows such as America's Most Wanted. In April 2012, an investigation into a fatal hit and run investigation hit a roadblock. The vehicle could not be identified and, without that piece of information, solving the crime was impossible. The police department released a photograph of the only piece of the vehicle that remained at the scene—a small piece of metal. A popular automotive blog wrote about the story and the contributors were able to identify the piece of metal as part of an early 2000's Ford F-150 pickup truck. The breakthrough was the key to law enforcement being able to identify the suspects who were later convicted (Glynn, 2013).

Such uses of social media reached a new level during the aftermath of the bombing at the 2013 Boston Marathon. With a greater scope of both information available from photos and videos taken by the crowd as well as a larger population from which to draw both time and talent, crowdsourcing was able to add valuable information to the criminal investigation. The appeal sent out to the public to send in videos and photographs of the

event garnered 13,000 videos and 120,000 photos (Pepitone, 2012). In addition to providing police with more evidence, websites like Reddit drew thousands of users to compare information presented in photographs of the scenes to identify the paths and activities of crowd members. With almost unlimited resources, every lead could be followed through the photographic trail (Glynn, 2013).

In addition to the ability of crowdsourcing to add to criminal investigations such as the Boston Marathon bombing, businesses have also turned to social media and crowdsourcing for new ideas. One company, Goldcorp, experienced immense benefits from allowing free access to its private information (Goodman, 2011).

The growth of communication technology has also had other societal benefits in the United States. The rise of online education has extended university education programmes to more non-traditional students than ever before (Moloney & Oakley, 2010). Enrolment on online courses continues to rise, albeit at a slowing rate for some degree programmes. The reputation of online courses and degree programmes is also on the rise as they gain a larger foothold in academia. Sixty-seven percent of academic professions stated that online courses were the same or superior to traditional classroom instruction and 65.5% of Chief Academic Officers see online education as critical to the long term strategy of their institution (Lytle, 2011).

3.1.3 The United Kingdom

Information and Communication technology has also strengthened its hold in the United Kingdom. Connectivity rates in the UK are slightly better than those in the United States with just 17% of homes without Internet access. The racial and poverty issues are less severe in the connectivity breakdown. A poll of those without access found that 59% of those without the Internet at home stated they simply did not feel the need: only 10% cited cost as the barrier to connection. The government is active in trying to expand coverage to all households, pledging to have at least 2 megabits per second in all homes by 2015 (BBC News, 2013). Even without such extension of Internet service, the UK still ranks as the eighth most connected country in the world according to the United Nations (Kelion, 2013).

Britons are using the Internet for much the same reasons as Americans. With close to one in five non-food items purchased online in the UK, a 19.2% growth in Internet purchases in a year (Record online sales over Christmas, 2014). Smartphones are leading the surge

in online purchases; there has been a 150% increase in shopping via iPhone and other smartphones in the UK. With same day delivery offered by many retailers, online food and grocery sales are growing. Twenty one percent of families in the UK have shopped online for groceries compared to less than 10% in the rest of the world (Poulter, 2013).

In 2013, Prime Minister David Cameron announced new plans to require a filtering system for those accessing the Internet from an Internet service provider in Britain. The system is an “opt-out” filter, which means the default option is for the filter to be implemented for all new subscribers. To remove the filter, you must actively opt out by calling your Internet service provider to regain full access. While the government has stated this was done for the safety of children on the Internet, some have argued this is government censorship of the Internet, especially with non-committal answers from government officials such as Cameron who stated that he “didn’t think” the filter would block access to *Fifty Shades of Grey* (Taylor, 2013).

The Internet and other communications technologies are not only used by shoppers in the UK, London boasts one of the most sophisticated surveillance systems anywhere in the world (Monahan, 2006). The reception to technology has not all been positive however. There has not been an appreciable change in crime rates around the city and privacy proponents fear the intrusion in the lives of innocent citizens. That being said, the CCTV system has aided in solving some crimes; the suicide bombers who struck London’s transit system were identified via the CCTV system which aided in the investigation (WSJ, 2014). It is estimated that the average Londoner is captured on closed circuit television 300 times per day but this is only an estimate as the total number of cameras in the city is unknown (Evans, 2012).

In the information and communication technology realm, is not only the Internet and closed circuit videos that have had a major impact on the United Kingdom. In 2006, the *News of the World*, a popular newspaper, came under investigation for illegally tapping and pinging the phones of citizens in order to gain information for printed stories. Celebrities, the Royal Family and politicians were all targeted via illegal means. As the investigation progressed into 2009-2011, even more victims came to light, the telephones of family members of fallen soldiers, high-profile news cases such as the murder of a young girl, as well as the victims of the London Bombings (discussed above). Telephones have, in the main, been considered to be secure—with access to them only given with proper warrants and legal paperwork but the evidence from the *News of the World*

scandal shows that stealing information from telephones or pinging a mobile phone to track an individual can be done by anyone. Some government officials have called for additional regulation but, as of yet, no new laws have been passed in the UK (Halliday, 2012).

3.1.4 Australia

Australia was a relative latecomer to the Internet. Geographical isolation kept the country without Internet until 1989 when a satellite connection linked the University of Melbourne and the University of Hawaii. Today, Internet connectivity has grown to almost universal access. A national survey showed 98% of respondents had Internet access and the majority of those people used the Internet on a daily basis. Social network usage has a strong foothold in the country with 78% of Australians visiting websites such as Facebook (Technology use in Australia, 2013).

To some degree, the geography of the nation influences the distribution and nature of the technology industry, with the majority of industrial production and service industries concentrated in the southwest. Agriculture takes place in the temperate zones and in the semi-arid regions bordering the large interior desert. Technological communications and transportation infrastructure is well developed in Australia, but has not resulted in the geographic dispersion of industry and workforce due to the relatively small population levels.

The technological systems that have developed in Australia are the result of management and cultural viewpoints inherited from the United Kingdom. In general, the primary business influence on Australia until recently was its connection with Britain, which remained its principal export market until the late twentieth century. The development of British derivative information security systems enhanced the nation's ability to form trade and other types of business relationships with the United States as recent improvements in security fostered the process of globalisation.

Despite the nation's geographic location, which is far closer to Asia than Europe, the technological culture retains primarily a European and American perspective. Until recently, there has been significant protectionist legislation to prevent competition in Australia from Asian markets. As a result, technological paradigms often focus on the perceived benefits of a controlled technological environment rather than on a full free-market model. In effect, the majority of Australian managers are reluctant to establish

ongoing trade and information exchange with Asian markets and businesses due to the belief that this will result in a long-term negative effect on their business operations. Recent government efforts to end this decades-old management perspective have resulted in increased technological contacts with Asia, but the majority of Australian managers continue to view Europe, the United States and New Zealand as their primary external markets.

Information security systems structures in Australia are analogous to those in Britain and the United States. To a large degree, the information systems that develop in various businesses are conditional on their structure, with closer supervisory control retained by managers in small businesses than in corporations. Australian corporate managers are somewhat responsive to shareholder demands for security in technology, but retain the general belief that their primary concern as managers is to ensure that the organisation makes a profit. Stakeholder theory, which requires managers to consider the social impact of their actions, has not taken hold in Australia, although government regulations often place a degree of limitation on managerial decisions when they involve a security concern regarding informational infrastructures. As in other industrialised free market nations, as businesses grow in size, they are often faced with the difficulty of legacy information systems that are inappropriate for the change in circumstances. In many of the long-established manufacturing businesses in Australia there is a higher degree of resistance to altering existing information systems than in the newer and more technologically oriented businesses. As a result, the newer industries, which incorporate more recent technologies into their business operations, often have more flexible management systems due to the lack of legacy management systems.

Australian management systems inherited the British operational paradigm of a hierarchical management structure, which was common throughout the British Commonwealth until the middle of the twentieth century. This model was applied to larger manufacturing operations such as mining and steel production, with operational departments for various tasks and centralised decision-making processes. In this model, upper management was responsible for making all decisions. Middle management acted as the supervisory intermediary between upper management and workers, and the general attitude toward workers was paternalistic. Due its geographic and cultural isolation, Australia has been slow to abandon this model in favour of more modern information security concepts.

In the past two decades, the organisational model of many businesses in Australia has started to shift away from vertical control towards a more horizontal system that provides a greater degree of lateral communication and more direct connections between upper management and workers. To some degree, this is in response to the management trends in the United Kingdom and the United States for industries using innovative technologies, which emphasise new types of organisational structures in order to enhance productivity. In this model, the workforce operates as task-oriented teams, with the teams participating in setting organisational goals based on their perceived capabilities and the resources available. The team leader largely replaces middle management as the supervisory and communications nexus between upper management and the workforce. The attitude towards workers is based on a partnership perspective, which assumes that all employees of a business, regardless of their position, share responsibility for the firm's success. While the majority of Australian managers are willing to embrace these types of fundamental management system changes, they are more often found in newer information-intensive businesses such as banking, communications and electronic commerce rather than in the more traditional types of manufacturing and production firms. To some degree, this is the result of inertia in the traditional production sectors, which are slow to respond to new management paradigms and perspectives.

Despite the slow pace of altering management systems, almost 90% of Australia's organisations have experienced significant internal restructuring since the mid-1980s (Light, 1999). The management perspective of the nation has shifted away from the centralised model of operations to a process that is described as "managed decentralisation." The intent of managed decentralisation is to increase productivity without having a negative effect on the workforce. It is the outcome of a combined effort of government and key industry leaders to alter management practices in order to make Australian business more competitive in the global marketplace.

In addition, the management system has developed various types of internal incentive and award programmes that involve recognition and sometimes merit pay increases or bonuses. In industry sectors that involve rapidly changing technologies such as IT, Australian businesses also focus on continuous retraining of personnel in order to ensure that their skills are commensurate with current technology, which research indicates is an important factor in retention. In the IT sector, personnel believe that the opportunity for ongoing training in new technologies is more important than a competitive salary. As a

result, it is commonplace for Australian management to emphasise training for the majority of their workforce, even those that are not deemed to be in critical positions (Brave, 1999).

While access in Australia has grown, Internet censorship has become more commonplace in the country. In 2010, plans were announced for a broad Internet filtering of all data coming into the country. The legislation would “introduce amendments to the Broadcasting Services Act, which will by 2011 require all ISPs to block refused classification-rated material hosted on overseas servers.” The “refused classification list” was still a work in progress at that time (Tung, 2009). These broad filtering plans were abandoned due to criticisms of Internet censorship. However, the idea has been transformed into a new “opt-out” Internet filtering system for all Internet service providers in the country—much like the one already adopted in the UK. The filtering will now be directed at blocking the Interpol list of the “worst of the worst” child abuse websites. There is still some tension in Australian politics however, as more conservative groups continue to push for mandatory filtering of all pornographic material (Taylor, 2012).

Another Internet issue gaining momentum in Australia is the “right to erasure” which would give citizens the ability to remove posts to social networks they have made or that others have made about them. However, most experts and critics note that unfeasibility of enforcement (Right to rub out embarrassing pictures and data posted online floated by The Australian Law Reform Commission, 2013).

3.1.5 The Arab World

Different aspects of ICT have been widely implemented in developing countries on different scales and in different areas. These implementations are mainly adoptions with no genuine adaptations to their new environments. These undertakings can be compared to the industrial revolution that began in Britain in the 18th century, which was later exported to developing countries but still couldn’t be regenerated (Thoburn, 2009). It is believed that there were a number of factors, such as population and working capitals, which had matured by that time, which contributed to the revolution’s success in the West. The same factors were not available to some other, then developing, countries including the Arab world, which settled with being industry exporters instead.

3.1.5.1 Arab Culture

It is important to consider the limitations of generalising about 21 states spanning over an area of 5.25 million square miles and inhabited by over a 200-million population. However, there are a number of characteristics that critical theorists in social sciences believe are inherent in Arab culture and society.

According to Barakat (1993), the apparent features of Arab cultures and society are as follows:

- Social diversity summarised as a three dimensional framework on a homogeneity-heterogeneity continuum, processes of conflict-accommodation-assimilation, and social class splits;
- Pyramidal class structure based on communal splits, socioeconomic structures, and lack of political power;
- Social complementarities, i.e. the "likeness" of Arab people, including the family, social class structure, religion, political behaviour, patterns of living.;
- Transition and the Arab renaissance, i.e. the perpetual change that has always been a characteristic of Arab society;
- Patriarchal relations, particularly in the family, which have been the basic economic and social unit for all three Arab patterns of living - Bedouin, rural, and urban;
- Primary group relations;
- Spontaneity and expressiveness in social interactions;
- Alienation and the lack of civil society for the masses;
- Continuing dependency and underdevelopment, which increases disparities between the rich and poor, creates marginal ruling families and classes, and a distorted development directed toward consumption rather than production.

Regardless of the level of development reached by a certain culture, it will comprise the following components: Language, Norms, Values, Religions and Beliefs, Social Collectives, Statuses and Roles, and Cultural Integration (Wingens et al, 2011). The more advanced the culture is, the more integrated these components are. Arab culture is one of the richest cultures in the world with a long history, during which Arabs have contributed to its development. The level of development of Arab culture can be based on the above components.

Religion is intrinsic in Arab culture and does not need to be changed or updated. This does not mean that the door to development has been closed, but it is needed at the level of interpretation which is supposed to be commensurate with the circumstances of the time and take into account the evolution that occurs in the elements of knowledge at the international level.

Historically, Arabs contributed a significant amount to the development of scientific knowledge. Although the scientific development attained by Arabs has benefited the civilised world on occasion, the circumstances witnessed by the Arab community contributed to the relative backwardness of it. This backwardness can be eliminated or decreased in theory, particularly after the wide spread of education. However, this is not happening for a number of reasons, including the core system and the components of the educational process, especially regarding the use of the Arabic language, adopting the scientific approach in thinking and the nature of the relationship with other cultures.

3.1.5.2 Sharing of Private Information

Arab culture is of a particular nature in which information is something that Arabs share and matters that should be considered private in other cultures are not so in Arab culture. A Lack of research can be seen in the literature on privacy in Arab culture. Chadwick (2002) conducted research on 9 communities in Australia, some of which were Arabic communities. This work involved a review of the literature on the subject of data privacy and attitudes towards the collection and storage of personal information. The author met leaders from three of the Arabic communities for round-table discussions of issues important to their communities and included their feedback in the research findings. Chadwick noticed that in certain circumstances, individual privacy may take second place to the needs of the community or family. Koocher (2009) presented research based on psychological investigations. He maintained that Arab culture respects elders and seniority. He further asserted that learning the background of a person can increase their cooperation; effective rapport flows from quid pro quo, commonalities, fairness, and mutual respect. Koocher alluded to the basis of social engineering and argued that private details may be divulged in circumstances involving seniority or friendship.

3.1.5.3 History of ICT adoption in the Arab World

According to Hamade (2009), the major problems negatively affecting the flourishing of ICT in most Arab countries are of two natures: Problems relating to basic infrastructure

and economy and problems relating to governmental policies and regulations.

Arab countries vary in their wealth, economic conditions and statute systems. For instance, some countries are oil producers and therefore have more wealth that positively contributes to their ICT development. However, there are several problems affecting these countries in different ways and at different levels, such as cost, education and language (2009).

It can be seen that Internet access in Arab countries seems to increase more slowly than that of the rest of the world due to the economic, political and social aspects in the region (Checchi et al, 2002) (Fergany et al, 2002). While the Internet has developed in the Western world, its presence as part of everyday life in the Arab World is relatively new. The first Internet connections in these countries date back to the early 1990s. Tunisia was the first Arab country to have an Internet connection in 1991, and Kuwait established its Internet services in 1992 as part of its reconstruction after the Iraqi invasion. In 1993, Egypt and UAE established Internet connection, while Jordan joined the Internet community in 1994. Other Arab countries did so in the late 1990s (Wheeler, 2004).

Most Arab countries have joined the World Trade Organization (WTO) and are adapting their legal and regulatory systems to accommodate trademark, patent and intellectual property rights (IPR) protection (Dutta & Coury, 2003). A recent study on Arab human development by the United Nations Development Programme (Fergany et al, 2002) reported that Arab countries generally lag behind other parts of the world in ICT, even when compared to other developing countries.

Although the Arab world is mainly constituted of developing countries, some Arab countries have already tried to move on from this characterisation.

Adopting a leadership position within the Arab world, Egypt began to pay attention to the importance of ICT policies in the early 1980s with the formation of the Cabinet-level Information and Decision Support Centre (IDSC). In 1999 the government established another ministry-level policy group, the Ministry of Communication and Information Technology (MCIT).

A crucial, high level research question emerges from contemplating such evolutionary processes in developing countries. Specifically, what bearing do culture, implementation factors, and government ICT policy have on the transfer of ICT and the associated diffusion of computing (e.g., hardware, software, telecommunications, applications) and

the Internet? A related issue is the benefit in social change and economic development afforded by such technology diffusion. In each case, the first challenge in studying such phenomena is developing an appropriate instrument of measurement that can capture the critical aspects of the phenomena (Checchi et al, 2002).

Mohamed Ali (2005) indicates 5 main causes of ICT lag in the Arab world, summarised in the following factors:

- **The belief that there is no urgent need to implement ICT (Abu Bakr, 2001):**

The impression is that the right environment for the application of ICT is the private sector because it seeks profit and works in an environment characterised by rapid changes and unpredictability. In addition, it is not subject to political constraints and social governing bodies which make it freer to move and change the direction of its areas of operation at any time. In government agencies however, it is a different story, as these agencies operate in a more stable environment where customers mostly seek its services, especially in developing countries. Therefore, the belief that there is no need or necessity for the application of the foundations and principles advocated by the information systems has prevailed in many Arab countries.

- **Lack of coordination and money and effort squandering (Yusuf, 2003):**

Most of the state bureaucracies in the Arab countries, concerned with the development of ICT and the application of information systems, ignore the importance of coordination with neighbouring countries and still implement their plans in isolation from their neighbours, despite the similarity of social and economic conditions. Some Arab countries have created centres of large scientific research, bringing together many technicians and specialists and have tried to achieve several accomplishments in the field of software inventions and information systems. These centres did not, however, coordinate with each other, resulting in a waste of money and effort due to conflicting projects. For example, several Arab companies worked at the same time on the completion of Arabic optical character recognition (OCR) system, but they did not benefit from each other's efforts, and ended up abandoning their attempts after Sakhr had achieved a leading step in this project.

- **Deficiencies in the government administrative bodies (Jaafari, 1983):**

The government administrative bodies in the Arab world face administrative challenges

especially in service-oriented organisations such as municipalities. The ancient city is the same city that must provide twenty-first century services and which is facing a steady increase in population and a rise in the needs of the different services. In addition, there is the industrial outskirts challenge, which adds to the environmental problems. Municipalities in the Arab world do not use the best information resources available to the best means to achieve the results they were intended for. They also do not benefit from the application of IT and information systems, as well as the scientific principles of modern management needed to face new challenges and obstacles in order to push forward the process of administrative development in these vital institutions.

3.1.5.4 Internet Revolution in the Arab world

In the Arab world, the Internet has been a revolutionising force. In terms of time online, although the region lags behind the worldwide average, the benefits of access are still astounding. The use of social media dominates time spent online at 29% of the total online time. In Bahrain, the average user spends 4.1 hours per day on social networks; the average for the region is 3.2 hours per day for users over 18 (Web Users in the Middle East Emphasize Social Networking, 2013).

The Arab world region has had a long history of disregarding the importance of women's rights but the spread of information and communication technology is helping to diminish the gender gap in some of the most conservative countries. Only 10% of all Internet entrepreneurs are women but that number changes drastically when focusing on the Arab world region. As of 2012, 40 start-ups had been launched by a small business incubator programme in Gaza—more than half of which were begun by women. In total, estimates put the percentage of women Internet entrepreneurs in the Middle East and North African region at 23%. The Gulf countries have an even better rate of 35% of start-ups created by women. The ability to work over the Internet affords well-educated women in conservative countries such as Saudi Arabia to begin a career without the social stigma of working outside the home (Rosbrow, 2014). With less community and family support, women entrepreneurs in the region are supporting each other and encouraging women to enter the information and communication technology field where they are able to more easily find equality with men (Rosbrow, 2014).

Another example of the spread of information and communication technology in the Arab world is the use of social media during the recent Egyptian revolution to oust President

Mubarak from power. Facebook and Twitter led the way, as protesters used them to organise and distribute messages and information and spread the word across the world about the conditions in the country. The use of social media was so important to the activists that some have termed the Arab Spring the “Facebook Revolution” (DW.DE, 2013).

Today, the use of social media continues but the protesters are no longer the only ones active. Government officials and agencies are also turning to social media to spread their own message. This could prove to have positive results by opening up debate and dialogue between the population and the government. This open political discourse could help maintain political stability in the country (DW.DE, 2013). On the other hand, social media has shown a darker side since the revolution, when it has occasionally been used to incite violence (Morrow, 2013).

3.2 Organisational Culture

Businesses and government are using technology like never before. Corporate culture has changed to embrace the convenience of technology. Executives of major corporations discuss the necessity of having video conferencing, team collaboration, cost savings, and more frequent meetings between team members who are located in different countries. The collection of data on consumers, markets, competitors, etc. is also important. All of this must be both stored and easily accessible (UT Dallas News, 2013).

In advanced countries, organisations resort to organisational culture to mitigate the impact of security threats and to support decision makers, by providing a framework of values and customs that executives can use when making their security-related decisions. Organisational culture governs the performance of businesses and individuals. Schein (2004) defines organisational culture as a set of basic shared assumptions learnt by the organisation’s endeavours to solve its internal integration and external adaptation problems, which have proven to work well and have been considered valid. These are taught to new members as the correct ways to perceive, feel and think in relation to these problems.

3.2.1 Information Security Culture

As part of organisation culture, information security culture represents the way an organisation reacts to information security problems and the way its people act towards information security. Experts have recognised that different approaches based on policy,

awareness, training and education assist organisations in establishing its information security culture (Lichtenstein & Swatman, 2001; Schlienger & Teufel, 2003; Furnell et al, 2000).

Security culture combines different sociocultural attributes that support the conventional technical security measures and aim to incorporate information security in the employees' professional aspect of practising daily tasks. The definition of information security culture given by Dhillon (1995) is widely accepted (Le Grand & Ozier 2000), namely "the totality of human attributes such as behaviours, attitudes, and values that contribute to the protection of all kinds of information in a given organisation".

The holistic or totality nature of information security is stressed in the literature by several authors (Connolly 2000), (Khalil, 2009), (Andress, 2000), (Koocher, 2009), (Ko & Dorantes, 2006) and (Ramachandran, 2008).

Information Security Culture (ISC) is therefore an intrinsic part of organisational culture that reflects the organisation's values and customs and includes training personnel, processes and communications (Ko & Dorantes 2006), suggesting that ISC is not a definite project but a sustained endeavour that must be constantly analysed, encouraged and adapted.

The qualitative nature of ISC yields an inability to directly and precisely measure it, yet it still has a significant effect on the behaviour of the workers, management style and the technological level. Organisations create and develop appropriate policies and adequate human and financial resources, effective management structures and control mechanisms to undertake the responsibility of establishing and sustaining ISC.

Although the positive impact of an effective information security culture is hardly disputable (Da Veiga 2007), Schlienger and Teufel (2003) considered that further research in the field of sociocultural security measures is still needed to improve the overall security level of an organisation, hinting at more intrinsic factors influencing information security. Woodhouse (2007) believed that achieving ISC required more than an annual awareness training initiative but involved an overall cultural awareness.

3.2.2 Cultural Impact on Information Security

Organisational culture does not often provide for the business requirements of information security which are reflected in confidentiality, integrity and availability. These can be related to a fundamental difference between the organisational information

security culture and the cultural impact on the organisation's information security. This was illustrated by Glaser (2009) where he argued that security culture is a measure of security used by managers to control human behaviour in their endeavour to attain a certain security level, whereas understanding the impact of human behaviour requires analysing the impact of culture on information security. Accordingly, implementing an organisational security culture needs a suitable understanding of the particular culture, as it exerts a powerful influence over information security. Sociology and cultural studies can provide further understanding of human behaviour which is necessary to implement effective and efficient security measures (NIST, 2002) and (Furnell 2000). Merely understanding employee behaviour and attempting to overcome major information security threats, only by cultivating organisational security culture and deploying technical measures, is unlikely to yield the desired results. Zhao et al (2010) referred to studies by Leidner and Kayworth (2006) which reviewed a wide range of literature on the relationship between IT and culture to highlight the significant impact of culture on IT at both the organisational and national levels. Chaula et al (2006) considered ICT security as being about people and their motivations to cause security breaches. They recommended examining culture as the main interpreter of people and motivations.

Both business and government would benefit from a more holistic approach to information security. There has been a long history of information security lapses over the last few decades and the lessons learned from these can be a powerful tool for the field of information security in the future. The biggest threats to information security in the United States are foreign government sponsored hacking attempts, terrorist/fundamentalist groups, as well as individual hackers.

Information security attacks are also posing a difficult legal situation for businesses. To combat this, information security professionals will be required to work closely with other departments in a company, particularly legal departments. Retailers who have been the victim of attacks are now facing large scale lawsuits from those whose information has been stolen. Litigation has been successful in the past; several banks were able to recover \$74.6 million dollars after a T.J. Maxx breach (Tracy, 2014). A lawsuit has already started in the Target case with banks attempting to recover the \$200 million expended on replacement cards (Bjorhus, 2014).

Increasing organisation preparedness through unifying the culture of security throughout an entire organisation is a critical step in increasing the overall preparedness. With rising

threats from state-sponsored hacking, corporate and organisational culture will have to place a greater emphasis on information security to keep pace with the increasing risk to sensitive data. On a similar note, information security specialists will need to work more closely with other corporate departments such as legal and public relations to obtain the best information on breaches and risks to the public as well as their business.

3.3 Conclusion

This chapter provided an overview of the cultural impact on ICT in developed countries as well as an insight into Arab culture and the history of ICT adoption in the Arab world.

Although this chapter showed that there exist security initiatives to raise awareness, the cultural impact on information security requires analysing human behaviour in practice. The need for analysing the cultural behaviour towards information security is essential to enable a solid understanding of security issues related to human behaviour. The practice of sharing sensitive information amongst family members and friends is addressed in the next chapter.

CHAPTER 4: CULTURE AND INFORMATION SECURITY

The aim of this chapter is to provide a build a deeper understanding of the cultural impact on information security, particularly in sharing sensitive information including passwords. For this aim, the chapter describes a pilot study conducted to investigate the preferences of sharing private information among family members and friends. The study aims to acquire knowledge of the role of culture in information security in the UAE. The pilot study is followed by further investigation to identify the extent to which cultural behaviour can have an impact on information security in other countries. The other countries considered are Saudi Arabia (KSA), Oman and the UK.

4.1. Methodology

The chapter discusses how data collection was carried out in the two phases of the study. *Phase One* was a pilot study conducted using two approaches: Questionnaires and interviews in major organisations the in Abu Dhabi Emirate. The aim of conducting this phase was to identify the extent that culture can have an impact on preferences of private information sharing, as well as establish how intense the issue of culture is present in information security in certain settings. *Phase Two* was a comparative study to investigate the role of culture in information security further. The study was conducted in several countries to identify user attitudes towards information sharing over digital services. A quantitative approach was used due to the research defined problem of targeting the public sharing preferences while using the digital resources and social media interactions. A quantitative evaluation was used to assess the privacy sharing preferences among family members and friends. The evaluation was conducted for the UAE, Oman, KSA and the UK to identify user attitudes towards sensitive information sharing. The analysis was based on t-test statistics. These types of tests have been used in earlier research studies to investigate cultural difference in terms of behaviour and attitudes towards Internet usage, as well as the mixed-method research (qualitative and quantitative) (for example Li & Kirkup, 2007 and Dinev et al., 2009). Furthermore, mixed-method research offers a number of advantages over the quantitative or qualitative approaches alone. For example, Creswell and Clark (2007) maintain that mixed-method research provides more evidence of investigating the research problems and answer

research questions that cannot be answered by either quantitative or qualitative research alone. Moreover, the mixed method bridges the gap between the sometimes adversarial divide between quantitative and qualitative researchers, and provides a more practical sense to the research as the researcher becomes free to use all methods possible to address the problem. Teddlie and Tashakkori (2009) highlight various benefits of using mixed research over individual quantitative or qualitative research for analysing human behaviour and attitudes. Similarly, Kelle (2006) argues that qualitative and quantitative methods should be combined in order to compensate for their mutual and overlapping weaknesses.

The questionnaires and interviews of both phases can be found in Appendix 1.

4.1.1 Phase One - Pilot Study

A large amount of research on ICT development claims that ICT security is essentially a political and a managerial act and the importance of the relevant cultural characteristics of a society should not be disregarded. Phase One's study investigates culture as a key factor in ICT development, particularly in information security and looks into organisational culture as a way of addressing cultural issues in information security. The pilot study consists of two approaches that have been used to provide a solid foundation about the cultural issue on information privacy in order to proceed to the next stages.

Based on the literature review, the pilot investigation strategy was focused on the following research hypotheses in order to commence with a rigorous research methodology that answers the research hypothesis:

Hypothesis 1: Arab culture is of a special nature where privacy is something that Arabs share

Hypothesis 2: There is a fundamental difference between organisational information security culture and the cultural impact on the organisation's information security

4.1.1.1 Quantitative Approach

In an attempt to determine the extent of privacy sharing within the Arab culture in Abu Dhabi Emirate, a survey questionnaire was used. The questionnaire was used by Olson et al. (2005) in the U.S. to capture respondents' views and willingness to share certain information with certain people.

The survey asked respondents to rank from 1 (least likely to share) to 5 (most likely to

share) information with certain people. The questionnaire was distributed to 90 people (49 male and 41 female) in different job positions and age categories (22-53) in major government institutions based in the UAE.

The pilot testing necessitated tailoring some questions from the original Olson questionnaire to better fit Arab culture. Given the number of questions (39) and the variety of options (19) to be ranked, respondents were allowed to take the questionnaire home and complete it later. The questionnaire was given in Arabic in order for respondents to clearly understand the questions and the corresponding options.

The answers were collected, tabulated and then rank for each question was averaged. These averages were included in a resultant table summarising the overall preferences of privacy sharing. The table utilises a visualisation colour-coded reflecting the likelihood of sharing information. The information most likely to be shared (3.5 to 5 inclusive) is coloured in white whereas the least likely to be shared (1 to 2.5 inclusive) is coloured in black. Cells ranging from greater than 2.5 to less than 3.5 reflect the ambiguous middle and are coloured in grey.

4.1.1.1.1 Results

Based on the calculated arithmetic means of the 90 participants for each question, the table below (Table 2) shows that Arabs are willing to share (in white) 69.91% of their information with certain people, while they preserve (in black) 24.97% to themselves. They are not sure about either sharing or preserving (grey) 5.13% of their information.

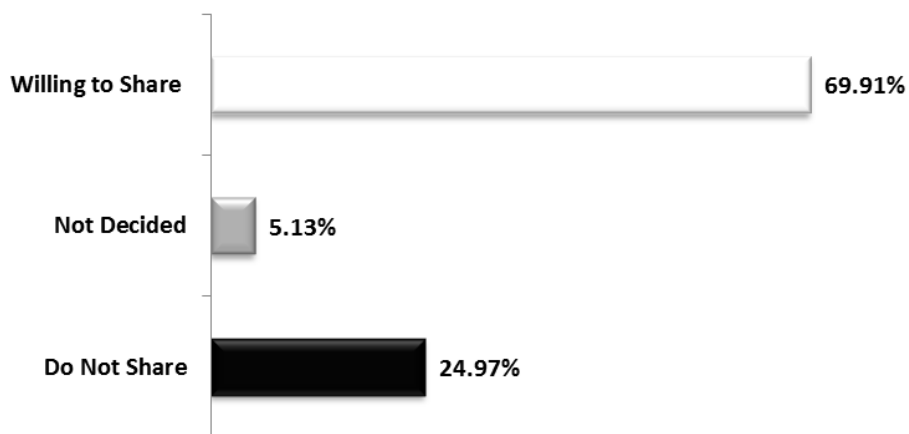


Figure 3: Arabs willingness to share information

Transgression is the only piece of information Arabs refrain from sharing with absolutely anyone. Examples of other presumably critical information that Arabs may share with

their family and close friends, are email content, credit card numbers or even a potential transgression. They are not sure, however, if they would share certain information, for example about salary or a significant personal failure, with extended family members. This is visually depicted as the small black region concentrated in the upper-left corner and which diminishes in the right and bottom, with very few grey cells in the middle.

However, Arabs may share most of the information regarded as private and non-sharable in other cultures, with almost anyone. These results reinforce an important point of privacy sharing as an intrinsic aspect of Arab culture; yet reflect a genuine vulnerability to be considered in information security measures applied in organisations operating in an environment where Arab culture prevails.

The collected results below can be compared to a similar study by Olson et al. (2005) on 30 people who worked at mid-sized companies in the USA and used computers as part of their jobs (Table 2).

Table 2: U.S. employees are less willing than their Arab counterparts to share information with others

	Salesperson (live or web-based)	Your personal website/blog	Potential or confirmed competitor	Company newsletter	People in an upcoming meeting	People you want to impress (e.g. hire, date)	Corporate lawyer	People in a project for whom it is relevant	People who work for me	Other team members	People in extended family	Young child of yours	Trusted colleague/team member	Sibling	My manager	Adult child of yours	Parent/grandparent	Best friend outside of work	Spouse	Average	Standard Deviation
Transgression that is well understood to be wrong (e.g. accessing pornographical images on a work computer)	1.07	1.50	1.04	1.16	1.17	1.10	1.32	1.23	1.26	1.20	1.34	1.63	1.57	1.61	1.60	1.79	1.82	2.17	2.55	1.48	0.40
All of my email content	1.07	1.17	1.11	1.20	1.30	1.24	1.64	1.50	1.47	1.43	1.66	1.94	1.73	1.68	2.00	1.57	1.89	2.00	3.10	1.62	0.47
Credit card number	1.57	1.06	1.00	1.00	1.10	1.10	1.40	1.17	1.40	1.27	1.59	1.59	1.43	1.75	1.47	2.43	2.32	1.83	4.38	1.62	0.78
Social Security Number	1.30	1.06	1.14	1.08	1.17	1.38	1.80	1.31	1.60	1.47	2.07	2.18	1.80	2.61	2.67	3.14	3.41	2.17	4.45	1.99	0.92
A potential transgression -- action not universally understood as wrong, more in a gray area (e.g. using your work computer for church activities)	1.10	1.61	1.14	1.36	1.33	1.41	1.68	1.67	1.65	1.80	1.97	2.12	2.30	2.46	2.40	2.93	2.68	2.90	3.69	2.01	0.70
Outside income	1.48	1.37	1.19	1.21	1.34	1.46	1.79	1.43	1.63	1.52	2.25	2.25	1.76	2.59	1.83	3.14	3.26	2.97	4.36	2.04	0.86
Salary	1.41	1.28	1.18	1.16	1.17	1.46	2.16	1.17	1.39	1.48	2.07	2.06	2.14	2.52	4.00	2.62	3.11	2.66	4.39	2.08	0.96
Large personal failure (e.g. fired from previous job)	1.30	1.50	1.25	1.24	1.48	1.46	1.88	1.62	1.58	1.80	2.21	2.59	2.33	2.79	2.47	3.00	3.29	3.33	4.21	2.17	0.85
Personal behavior I feel bad about (e.g. spoke sharply to a colleague)	1.17	1.56	1.36	1.56	1.70	1.62	2.00	2.00	2.05	2.27	2.28	2.35	2.73	2.68	2.77	2.79	2.89	3.13	3.79	2.25	0.68
Buddy list (who's on my list)	1.32	1.25	1.55	1.61	1.62	1.70	1.72	1.67	1.93	2.05	2.57	3.21	2.19	3.05	2.33	3.22	3.19	3.10	3.50	2.25	0.75
Non-work related websites I've looked at at work	1.24	1.67	1.57	1.56	1.80	1.83	1.92	1.93	1.79	2.20	2.64	2.76	2.60	2.70	2.60	3.08	2.74	3.17	3.71	2.29	0.66
Recent history of status (looking for trends)	1.57	1.41	1.62	1.85	2.05	2.05	1.90	2.14	2.13	2.27	2.32	2.87	2.59	2.60	2.73	2.80	2.62	2.68	3.38	2.29	0.51
History of my job performance scores	1.17	1.29	1.39	1.68	1.53	2.03	2.24	1.80	1.74	1.83	2.28	2.59	2.40	2.96	4.17	3.00	3.07	2.97	4.10	2.33	0.87
Opinions I have about other people (assume in digital form)	1.43	1.67	1.46	1.56	1.73	1.79	1.56	1.90	1.89	2.03	2.79	2.53	2.50	3.11	2.37	3.43	3.29	3.50	3.97	2.34	0.79
My application to another job/school	1.33	1.61	1.25	1.44	1.43	1.76	1.52	1.63	1.58	1.67	2.93	2.71	2.30	3.50	1.97	3.71	3.79	3.80	4.62	2.34	1.06
Access to my computer with personal assurance that they won't look at anything	1.20	1.19	1.29	1.32	1.57	1.69	1.88	1.93	2.53	2.40	2.54	2.71	3.23	2.81	3.37	3.15	3.22	3.14	3.82	2.37	0.84
Small personal failure (e.g. project missteps that led to failure)	1.30	1.50	1.29	1.48	1.73	2.00	2.08	2.07	2.47	2.43	2.59	2.76	3.03	3.07	3.33	3.21	3.36	3.47	4.03	2.48	0.82
What email groups I belong to (external to the company)	1.50	1.71	1.59	1.92	2.21	2.21	2.08	2.32	2.29	2.28	2.70	3.00	2.62	3.11	2.62	3.27	3.42	3.59	4.11	2.56	0.71
Record/summary of database/sharepoint interactions	1.29	1.29	1.76	1.91	2.73	2.60	2.59	3.00	3.17	3.31	2.59	2.87	3.85	2.90	3.96	2.90	2.95	2.91	3.77	2.76	0.76
Preferences (politics, religion, associates, etc.) (assume in digital form)	1.70	2.33	1.79	1.72	1.77	2.38	1.84	2.10	2.32	2.33	3.66	3.65	2.90	4.00	2.57	4.07	4.11	4.27	4.52	2.84	1.00
Work-related documents I've accessed	1.29	1.18	1.79	2.04	2.83	2.76	2.92	3.03	3.42	3.53	2.56	2.94	4.20	2.71	4.23	2.91	3.00	3.08	3.76	2.85	0.84
Your health status	1.50	1.78	1.96	2.12	2.17	2.24	2.36	2.30	2.50	2.57	3.41	3.47	3.23	3.57	3.10	3.93	3.93	4.03	4.55	2.88	0.88
Specific calendar entries	1.52	1.78	2.00	2.17	3.07	2.59	2.54	3.17	3.16	3.17	3.08	3.40	3.48	3.36	3.62	3.38	3.40	3.56	4.18	2.98	0.70
Pregnancy status	1.87	2.11	2.00	2.07	2.27	2.29	2.40	2.33	2.22	2.73	3.73	4.13	3.53	3.79	3.40	3.83	4.00	4.20	4.64	3.03	0.92
Work in progress	1.32	1.67	1.67	2.16	3.21	3.07	2.96	3.76	3.67	3.72	2.89	3.50	4.21	2.92	4.31	3.17	3.08	3.14	3.78	3.06	0.84
Desktop video conference number	1.29	1.83	2.50	3.17	3.83	3.20	3.50	4.33	3.33	3.83	3.00	2.75	3.71	3.20	4.29	2.00	3.33	3.17	3.83	3.16	0.81
Work-related websites I've looked at	1.41	1.72	2.00	2.52	3.20	3.03	3.16	3.60	3.26	3.70	3.39	3.53	4.13	3.33	4.23	3.62	3.37	3.48	4.00	3.19	0.77
Current location	1.63	1.94	2.11	2.25	3.07	3.07	2.76	3.73	3.26	3.37	3.41	4.06	3.77	3.75	3.70	3.64	3.79	3.83	4.31	3.23	0.76
Current status (on line, "busy") from IM	1.78	1.82	2.33	2.24	3.18	3.05	2.58	3.45	3.47	3.45	3.77	4.07	3.55	4.05	3.50	3.78	3.86	3.91	4.19	3.27	0.76
Past finished papers, products	1.55	2.61	2.43	3.24	3.63	3.59	3.64	3.93	3.79	4.13	3.25	3.47	4.43	3.26	4.60	3.31	3.48	3.48	4.00	3.46	0.71
What email groups I belong to (internal to the company)	1.45	1.81	2.43	3.32	3.69	3.52	3.76	3.97	4.11	4.33	3.19	3.38	4.63	3.52	4.63	3.58	3.64	3.78	4.08	3.52	0.84
Small personal success (e.g. project chosen to demo)	1.87	2.50	2.89	3.16	3.23	3.45	3.24	3.47	3.65	3.53	3.72	4.12	4.00	4.07	4.30	4.29	4.25	4.30	4.76	3.62	0.71
When available (on a shared calendar)	1.67	2.00	2.30	2.61	4.10	3.39	3.29	4.24	4.21	4.07	3.69	4.13	4.38	4.12	4.38	4.00	4.04	4.22	4.59	3.65	0.88
Home phone number	1.55	1.47	2.07	2.25	2.76	3.32	3.17	3.31	3.44	3.59	4.75	5.00	4.45	4.96	4.59	5.00	4.96	4.93	5.00	3.71	1.25
Large personal success (e.g. big promotion)	1.90	2.67	2.96	3.24	3.40	3.62	3.36	3.60	3.85	3.73	3.90	4.24	4.17	4.29	4.43	4.50	4.50	4.43	4.83	3.77	0.74
Age	2.57	2.89	3.00	3.20	3.30	3.24	3.60	3.47	3.95	3.90	4.76	4.65	4.00	4.82	4.07	4.71	4.68	4.63	4.83	3.91	0.75
Marital status	2.60	2.83	3.11	3.12	3.37	3.41	3.48	3.67	3.85	3.97	4.72	4.76	4.17	4.79	4.13	4.71	4.82	4.83	4.83	3.96	0.76
Cell phone number	1.78	2.00	3.00	3.22	3.77	3.84	3.86	3.92	3.50	4.15	4.44	4.80	4.48	4.79	4.41	4.83	4.75	4.81	4.92	3.96	0.93
Desk phone number	2.57	2.28	4.26	4.67	4.76	4.50	4.92	4.90	5.00	4.97	4.32	4.81	5.00	4.74	5.00	5.00	4.93	4.83	5.00	4.55	0.78
Work email address	2.37	2.56	4.21	4.56	4.87	4.62	4.96	4.87	5.00	5.00	4.66	4.65	5.00	4.79	5.00	4.79	4.81	4.97	5.00	4.56	0.77
Average	1.55	1.76	1.95	2.16	2.49	2.50	2.59	2.72	2.76	2.86	3.04	3.25	3.26	3.33	3.43	3.46	3.53	3.53	4.19	2.86	0.79
Standard Deviation	0.42	0.45	0.72	0.79	0.67	0.55	0.73	0.58	0.61	0.59	0.63	0.57	0.50	0.60	0.49	0.61	0.55	0.53	0.37	0.47	0.14

As can be seen in the previous table (Table 2), the dark area is much larger than that in the following table (Table 3**Error! Reference source not found.**), reflecting less privacy sharing than their Arab counterparts.

Table 3: The willingness of workers in the UAE to share information

	Salesperson (live or web-based)	My personal website/blog	Potential or confirmed competitor	Company newsletter	People in an upcoming meeting	People I want to impress (e.g. hire, date)	Corporate lawyer	People in a project for whom it is relevant	People who work for me	Other team members	People in extended family	Young child of mine	Trusted colleague/team member	Sibling	My manager	Adult child of mine	Parent/grandparent	Best friend outside of work	Spouse
1																			
2	Transgression that is well understood to be wrong (e.g. accessing pornographic images on a work	1.15	1.17	1.53	1.34	1.14	1.25	1.68	1.36	1.34	1.18	1.86	1.10	1.10	1.10	1.10	1.10	1.10	1.10
3	All of my email content	1.10	1.10	1.10	1.50	3.50	2.80	3.50	4.80	4.90	4.80	4.80	2.00	4.90	4.90	4.90	4.50	4.90	4.90
4	Credit card number	1.10	1.10	1.10	1.10	1.10	1.10	1.20	1.10	1.10	1.10	2.90	1.10	4.70	4.90	3.10	4.80	4.90	4.90
5	Social Security Number	1.10	1.10	1.10	1.10	1.10	1.10	1.20	1.10	1.10	1.10	2.90	1.10	4.70	4.90	3.10	4.80	4.90	4.90
6	A potential transgression -- action not universally understood as wrong, more in a grey area (e.g. using your work computer for charitable activities)	2.00	1.90	1.14	1.13	1.17	1.10	1.16	1.11	1.12	1.14	4.90	4.20	4.90	4.90	3.50	4.90	4.90	4.90
7	Outside income	2.00	1.90	1.15	1.15	1.18	1.17	1.15	1.17	1.18	1.39	4.90	4.20	4.90	4.90	1.50	4.90	4.90	4.90
8	Salary	1.10	1.10	1.10	1.10	1.10	1.10	1.20	1.10	1.10	1.10	2.90	1.10	4.70	4.90	3.10	4.80	4.90	4.90
9	Large personal failure (e.g. fired from previous job)	1.10	1.10	1.10	1.10	1.10	1.10	1.20	1.10	1.10	1.10	2.90	1.10	4.70	4.90	3.10	4.80	4.90	4.90
10	Personal behaviour I feel bad about (e.g. spoke sharply to a colleague)	2.00	1.90	1.10	1.10	1.10	1.10	1.17	1.10	1.17	1.28	4.90	4.20	4.90	4.90	1.50	4.90	4.90	4.90
11	Buddy list (who's on my list)	2.00	1.90	1.10	1.10	1.10	1.10	1.10	1.13	1.10	1.40	4.90	4.20	4.90	4.90	1.50	4.90	4.90	4.90
12	Non-work related websites I've looked at at work	1.10	1.10	1.10	1.10	1.10	1.10	1.20	1.10	1.49	1.30	2.90	1.10	4.70	4.90	3.10	4.80	4.90	4.90
13	Recent history of status (looking for trends)	1.10	1.10	1.10	1.10	1.10	1.10	1.20	1.10	1.10	1.10	2.90	1.10	4.70	4.90	3.10	4.80	4.90	4.90
14	History of my job performance scores	4.50	4.50	3.00	3.80	4.50	4.50	4.50	4.90	4.90	4.90	4.90	4.50	4.90	4.90	4.90	4.90	4.90	4.90
15	Opinions I have about other people (assume in digital form)	1.10	1.10	1.10	1.10	1.10	1.10	1.20	1.10	1.10	1.10	2.90	1.10	4.70	4.90	3.10	4.80	4.90	4.90
16	My application to another job/school	4.50	4.50	3.00	3.80	4.50	4.50	4.50	4.90	4.90	4.90	4.90	4.50	4.90	4.90	4.90	4.90	4.90	4.90
17	Access to my computer with personal assurance that they won't look at anything	1.10	1.10	1.10	1.50	3.50	2.80	3.50	4.80	4.90	4.80	4.80	2.00	4.90	4.90	4.90	4.50	4.90	4.90
18	Small personal failure (e.g. project missteps that led to failure)	2.00	1.90	1.10	1.10	1.10	1.10	1.10	1.10	1.10	1.10	4.90	4.20	4.90	4.90	3.50	4.90	4.90	4.90
19	What email groups I belong to (external to the company)	4.50	4.50	3.00	3.80	4.50	4.50	4.50	4.90	4.90	4.90	4.90	4.50	4.90	4.90	4.90	4.90	4.90	4.90
20	Record/summary of database interactions	3.00	3.80	2.50	4.60	4.30	4.20	4.20	4.00	4.00	4.00	4.90	2.00	3.50	3.90	3.85	3.40	3.00	4.00
21	Preferences (politics, religion, associates, etc.) (assume in digital form)	4.50	4.50	3.00	3.80	4.50	4.50	4.50	4.90	4.90	4.90	4.90	4.50	4.90	4.90	4.90	4.90	4.90	4.90
22	Work-related documents I've accessed	3.00	3.80	2.50	4.60	4.30	4.20	4.20	4.00	4.00	4.00	4.90	2.00	3.50	3.90	3.85	3.40	3.00	4.00
23	My health status	4.50	4.50	3.00	3.80	4.50	4.50	4.50	4.90	4.90	4.90	4.90	4.50	4.90	4.85	4.85	4.85	4.85	4.90
24	Specific calendar entries	1.10	1.10	1.10	1.50	3.50	2.80	3.50	4.80	4.90	4.80	4.80	2.00	4.90	4.85	4.85	4.50	4.85	4.90
25	Pregnancy status	2.00	1.90	1.10	1.10	1.10	1.10	1.10	1.10	1.10	1.10	4.90	4.20	4.90	4.85	4.85	4.85	4.85	4.90
26	Work in progress	4.50	4.50	3.00	3.80	4.50	4.50	4.50	4.90	4.80	4.90	4.90	4.50	4.90	4.85	4.85	4.85	4.85	4.90
27	Desktop video conference	1.10	3.50	3.50	4.50	4.50	4.00	4.00	4.80	4.60	4.50	2.50	2.90	4.50	4.50	4.90	2.00	2.00	4.60
28	Work-related websites I've looked at	4.80	3.20	4.00	4.20	4.60	4.50	4.00	4.10	4.70	4.80	4.50	3.00	4.50	4.20	4.90	4.50	4.50	4.90
29	Current location	4.80	4.50	4.90	4.60	4.80	4.80	4.90	4.50	4.50	4.80	4.90	4.20	4.90	4.90	4.90	4.90	4.90	4.90
30	Current status (on line, "busy") from IM (Instant Messenger)	4.80	4.50	4.90	4.60	4.80	4.80	4.90	4.50	4.50	4.80	4.90	4.20	4.90	4.90	4.90	4.90	4.90	4.90
31	Past finished papers, products, etc.	3.00	3.80	2.50	4.60	4.30	4.20	4.20	4.00	4.00	4.00	4.90	2.00	3.50	3.90	3.85	3.40	3.00	4.00
32	What email groups I belong to (internal to the company)	4.50	4.50	3.00	3.80	4.50	4.50	4.50	4.90	4.90	4.90	4.90	4.50	4.90	4.90	4.90	4.90	4.90	4.90
33	Small personal success (e.g. project chosen to demo)	4.80	4.50	4.90	4.60	4.80	4.80	4.90	4.50	4.50	4.80	4.90	4.20	4.90	4.90	4.90	4.90	4.90	4.90
34	When available (on a shared calendar)	4.80	4.50	4.90	4.60	4.80	4.80	4.90	4.50	4.50	4.80	4.90	4.20	4.90	4.90	4.90	4.90	4.90	4.90
35	Home phone number	4.50	4.80	4.80	4.20	4.50	4.90	4.90	4.90	4.90	4.90	4.90	4.90	4.90	4.90	4.90	4.90	4.90	4.90
36	Large personal success (e.g. big promotion)	4.80	4.50	4.90	4.60	4.80	4.80	4.90	4.50	4.50	4.80	4.90	4.20	4.90	4.90	4.90	4.95	4.90	4.32
37	Age	3.00	3.80	2.50	4.60	4.30	4.20	4.20	4.00	4.00	4.00	4.70	4.70	4.70	4.70	4.87	4.90	4.90	4.90
38	Mobile number	4.50	4.80	4.80	4.20	4.50	4.90	4.90	4.90	4.90	4.70	4.70	4.70	4.70	4.70	4.76	4.90	4.90	4.12
39	Work desk phone number	4.50	4.50	3.00	3.80	4.50	4.50	4.50	4.90	4.90	4.70	4.70	4.50	4.70	4.70	4.90	4.12	4.90	4.90
40	Work email address	4.30	4.90	3.50	3.90	4.90	4.50	4.90	4.90	4.90	4.70	4.50	4.70	4.70	4.23	4.01	4.12	3.96	4.33

4.1.1.2 Qualitative Approach

Qualitative research interviews were conducted to provide a deeper understanding of the issues of culture in information security. Questions were devised and a schedule was prepared and piloted. The questions followed recommended techniques for interviews, such as giving examples in the questions to clearly state what is needed (Bell, 2005). In accordance with best practice, it was ensured that no leading, presumptive or offensive questions were presented. The order of the questions was considered to be from the general to the specific. While the interviews were based on an unstructured format, a list of items to be discussed and probes into the particular issues to cover were prepared.

The literature search has identified key issues that require investigation in a local context. These centre on:

- Are standards and policies sufficient to guarantee privacy?
- What further measures would enhance security?
- Are employees provided with effective training on the importance of information?
- To what extent is culture a factor in information?

Interviews were conducted with two IT executives in Abu Dhabi after obtaining informed consent. The questions asked can be found in Appendix 1. The interviews were conducted in Arabic and transcribed.

The first is an interview with Lieutenant Colonel Faisal Mohammed Al-Shammari, Chief Information Security Officer of Abu Dhabi Police. Al-Shammari considers that internal policies and compliance with international standards are not enough to prevent employees from sharing sensitive information with each other or to those outside of the organisation. He maintains that awareness and sense of ownership of information from the employee are needed in order to make them feel responsible for this information. Not only does this require awareness, but also a procedural system of retribution. In addition, there should be forms of awareness assessment to categorise the level of awareness of the employee, for example beginner, intermediate or advanced. In certain ways, this can start by a pre-assessment prior to hiring and continue as a regular course over the employment period, which advances with their job promotion. Although sharing sensitive information is more acceptable in some cultures than others, he believes this can be mitigated by devising an adaptive punishment-reward system to the particular culture. He stresses that there are procedures rather than measures that may be taken along with policies and standards,

such as evaluation of employee awareness of information security, which may be part of his or her annual assessment. Al-Shammari asserts that there have been some courses at Abu Dhabi Police Department delivered by experts on information security, but there is a weakness in continuity as courses are more likely to provide discrete events rather than a culture of information security. Customs and traditions may affect sharing information especially in a collectivistic society such as in Abu Dhabi. This is more noticeable with the technological development. For example, some people broadcast over Blackberry Messenger the locations of road inspection points, knowing that the broadcasts may have originated from the police department itself. The evolution in methods of communication has revealed new vulnerabilities that would not have been obvious in the past. Public awareness is very important to reach an acceptable level of security. However, he argues that the problem is not inherent in Arab culture, rather in the lack of appreciating the value of information. He also states that deciding what constitutes sensitive information depends on the cultural and educational background and awareness. Al-Shammari considers these three factors to be significant in the arbitration of dealing with sensitive information. For example, an information security expert who deals with highly confidential information in a highly responsible way, driven by his professional background, practical experience and his awareness that disclosing such information may expose him to expulsion or even prosecution. Reinforcing these factors is the direct way of reducing information sharing.

The second interview was conducted with Mr Mohammed Husein Karmastaji, Standards and Governance Manager in Abu Dhabi Systems and Information Centre (ADSIC), the centre responsible for information security policy in Abu Dhabi Emirate.

According to Karmastaji, standards and policies are created to provide guidelines. The challenge lies in the adoption of the policies or standards. Policies are clear on the system but the implementation is what usually generates problems as it involves people. We try to adjust standards to fit culture in order to create awareness of information security bearing in mind that the availability of policies are not enough alone. Awareness is the most important factor in information security and it has to be continuous and assessed to confirm that people are familiar with it. The presence of policies is also important to ensure that people implement information security. The value of information in terms of sensitivity varies. Hence, there should be a focus on the different groups of people by various training courses educating them on information security. Karmastaji maintains

that there are courses in his organisation targeting people who handle sensitive information. He considers that the cultural background of the employee is important for their understanding of the value of information. It has been noticed that employees from non-Arab cultures are more aware of the value of information and are more discreet in sharing it. This has been witnessed in the organisation. There have been clear examples of cultural differences regarding information handling in the organisation. For example, a foreign employee would take all his documents off his desk and shut off his PC before leaving, while an Arab counterpart would leave some papers on the desk or his PC logged on and just leave the workplace. Despite providing courses on information security, along with policies and awareness, employee practice has not changed. This change cannot even be attained by coercion as it would be a later stage anyway. If the importance of information security existed from a young age, the situation would be different from that of today. Awareness in childhood would also mitigate the financial burdens of continuous yet inefficient training at a later time. A simple example is that in the UAE, house doors are left open as people are not frightened by issues of security, whereas in the West, people never leave their doors open as they are concerned about security.

4.1.1.2.1 Summary of Key Issues

- Internal policies and compliance to international standards are not enough to prevent employees from sharing sensitive information;
- Policies are clear on the system but the implementation is what usually generates problems as it involves people;
- There are procedures rather than measures that may be taken along with policies and standards, such as evaluation of employee awareness of information security;
- Courses by experts have been given to employees but little progress has been noticed;
- The technological development has revealed information sharing in a more obvious way than that of the past (e.g. message broadcasts, etc.);
- Awareness is the most important factor in information security and it has to be continuous and assessed to confirm that people are familiar with it;
- It has been noticed that employees from non-Arab cultures are more aware of the value of information and are more discreet in sharing it. This has been witnessed in the organisation;
- There have been clear examples of cultural differences regarding information

handling in the organisation;

- Awareness in childhood would also mitigate the financial burdens of continuous yet inefficient training at a later age.

4.1.2 Phase Two - Further Study

The results of a previous survey in the UAE to gauge private information-sharing (Al-Kaabi and Maple, 2012) showed that most respondents share sensitive information that people of other cultures (especially in the West) would usually withhold. The results have shown that respondents mostly share private information with family and close friends.

To further investigate to what extent that cultural behaviour can impact on information security, more countries of the GCC (Gulf Cooperation Council) area are considered in this study. We devised and administrated a questionnaire with municipality staff in 3 GCC countries, namely, Oman, Saudi Arabia (KSA) and United Arab Emirates (UAE), which represent the majority of the GCC population.

In addition, the UK, as a western culture, was selected to be compared with the GCC countries to provide a deeper understanding and comparison of cultural issues on information security.

The above investigations were designed to establish the cultural impact on information security as represented in the following hypotheses:

Hypothesis 1: Sharing sensitive information in UAE is different than in other GCC countries (KSA, Oman).

Hypothesis 2: Sharing sensitive information in GCC countries is different than in the UK.

The questionnaire was based on a five-point (from 5 strongly agree to 1 strongly disagree) Likert scale. The questionnaire contained 21 mandatory questions about sharing information (work and personal) with family and close friends typically regarded as private. 90 responses were collected in the GCC, 30 from each country studied. The first 3 questions asked about the country (i.e. Oman, KSA and UAE), age and gender. The other 18 questions concerned sensitive information-sharing.

4.1.2.1 Questionnaire Design

Based on social engineering attacks targeting user behaviour, a questionnaire was designed particularly to investigate preferences of information sharing that may lead to compromising the first security control: the authentication mechanism. The design

focused on areas such as: personal belongings, work belongings, and trust and social influences of family members and friends. These areas are illustrated in Table 5.

Table 4: Nature of information sharing and vulnerabilities to personal and work assets

Nature of sharing and vulnerabilities	Personal asset	Work asset
Sharing with family members and friends	Access to PC Credit card details Email password Current location Mobile phone password Social media password Email content Online banking details Access to a mobile phone Access to a USB memory Access to other mobile devices	Access to a PC Access to confidential information Email password Email content Work related documents Past finished work Access to a USB memory
Vulnerability	Social engineering attack	Social engineering attack
Impact	Loss of Confidentiality, Integrity and Availability /digital forensics issues	Loss of Confidentiality, Integrity and Availability /digital forensics issues
Potential risk to personal assets	Yes	Yes
Potential risk to work assets	Yes	Yes

Sharing sensitive information, such as the abovementioned, with family members and friends may lead to a breach of an information system. In this respect, Orgill et al (2004) assert that trusted people can fail to be trustworthy when it comes to protecting their aperture of access to secure computer systems due to inadequate education, negligence and various social pressures. Social engineering is a known risk to the sharing phenomenon which may be overlooked in favour of looking at major security problems that often originate from a software bug, a configuration defect or a software design flaw (Simon & Cheng, 2009).

The questionnaire design focused on sharing scenarios represented by the following activities:

Sharing sensitive information and access control: sharing private and sensitive information with family, friends and sometimes with strangers over the Internet and social media has been discussed earlier as being a real threat to information security.

Such practices contribute highly to consequences such as identity theft, blackmailing and physical stalking (Ralph & Acquisti, 2005). Sensitive information can be passwords to online accounts, online banking details, date of birth, home/work address, and access details to personal digital devices where sensitive information is stored, amongst others. Internet users may post a large amount of personal information in their online profiles without realising the risk behind it. Some criminals may be working heavily to accumulate such information in order to perform their hacking activities successfully. Information gathered by hackers can be put together to allow unauthorised access. Furthermore, sharing passwords can mean sharing identity (Ralph & Acquisti, 2005). Therefore, if a person shares their password with another person in order to access a secure service, this means that the one using this password will be presented to the system as the owner of the account. If anything goes wrong with the stored data (through activities such as modifying or deleting), standard digital forensic tools may find that it is extremely difficult to identify the person responsible, even though these activities are recorded.

Privacy and location information sharing: Posting private information on social media websites is widely practised by Internet users. It has also become an ordinary practice to update online friends with the current location and activity, and even future plans. This phenomenon has resulted in some major privacy attacks such as the structural re-identification attacks, inference attacks, information aggregation attacks and traditional attribute re-identification attacks. However, some countermeasures have been proposed to mitigate such attacks, but only a few of them have been well tested on real data (Yang et al, 2012). The risk varies according to each criminal intention (for example home theft, property harm and online stalking). The threat is increasing from one day to the next on all age groups of social media users and can even lead to kidnapping and murder (Baruah, 2012).

Personal information, the current location and daily activities available on social media user profiles can pose a real threat to online users where others, including unknown ones (i.e. with fake profiles), who appear on their list can make use of this information. Users with fake profiles have the ability to mislead people through posted information, resulting in victims of, for example, online harassment and cyberstalking (Baruah, 2012; Malagi et al., 2013).

Vulnerabilities: Information system security weaknesses vary according to the nature of

the vulnerability. For example, there are some weaknesses in technical application designs that lead to a technical vulnerability, which can be exploited technically. In certain settings, however, where a lack of information security awareness exists, hackers tend to use the weakness of the human factor to obtain information which can lead to bypassing the technical measures. Sharing private information among family members and friends makes a better basis for hackers to penetrate a system through performing social engineering attacks. According to several studies, social engineering attacks are rapidly increasing due to the difficulty of alternative technical attacks (Twitchell, 2006; Long, 2011; Krombholz et al, 2013).

Impact: The majority of breaches of information security lead to a financial loss (to individuals or organisations) or politically sensitive information disclosure (Verdasys, 2011; Molok et al., 2010). However, the spread of Internet services and social media has extended the impact of cybercrime to Cyberterrorism (Conway, 2007). Cyberterrorism has become an issue and has challenged the world due to wide applications of ICT facilities and the absence of strict border information security (Goodman et al, 2007).

Sharing sensitive information including passwords with friends has an impact on compromising the information security triad. These three elements are believed to be the core protection of information security. However, none of these three facets is attainable if there is a weak link in one of the others. It is highly believed that the weak link is associated with the human factor (Berti & Rogers, 2004). For instance, identity theft is a traditional crime of fraud that results in many issues, such as opening a new bank account, taking over an existing credit card, renting properties, amongst many others (Chawki & Wahab, 2006). Fraud has become widespread due to issues related to online presence, as it is very difficult for law enforcement officers to identify online fraudsters who can commit crimes on a broader scale than that of their real-world counterparts (Chawki & Wahab, 2006). Identity theft is also an issue for the forensic investigation centres. Forensics can help analyse a particular computer or device that has been used to commit a crime. However, although it may be relatively easy to identify the computer or device used for a crime, identifying who used that device at the time the crime was committed may be more difficult, especially if access details are shared or socially engineered (Jones & Martin, 2010).

Risk to Personal/work assets: Attacks on information security systems that lead to a breach could have further consequences. For example sharing a work email password

with colleagues could have an impact on the Facebook password account if the same password is used. Password reuse practices are common with most online users (Notoatmodjo & Thomborson, 2009). Almost all social media accounts such as Facebook, Twitter, Instagram, etc. need password verification. In the work environment, employees need to access the work network and different applications related to their work. It may be difficult for the user to use a difficult and different password for each and every account (Campbell & Bryant, 2010).

4.1.2.2 Hypothesis 1: Users' attitudes in Oman, KSA and UAE

Proposition one relates to a comparison between UAE computers' users with other GCC computers' users (Oman and KSA). Those countries were selected due to their large population compared to other GCC countries (Kuwait, Qatar and Bahrain) although all of the GCC countries stem from the same cultural background.

Results and analysis (Oman, KSA, UAE)

Analyses of ordinal data, particularly as in Likert surveys, are not as straightforward and transparent as analyses of nominal, interval and ratio data. Hence, non-parametric measures should be used for the analyses (Allen and Seaman, 2007). Ignoring the discrete nature of the responses can lead to inferential errors. Since the questionnaire uses Likert scales, non-parametric measures will be used for the analyses of the collected data. According to Allen and Seaman (2007), any parametric analyses based on the normal distribution, such as mean and standard deviation, are invalid for descriptive statistics whenever data are on ordinal scales. Therefore, nonparametric procedures, based on the rank, median or range, are more appropriate for analysing these data, as are distribution free methods such as tabulations, frequencies, contingency tables and chi-squared statistics.

The questionnaire comprises 18 questions targeting different attributes of sharing private and sensitive data among relatives, close friends or friends of friends. The respondents were all public service employees of different municipalities in 3 Gulf countries: Saudi Arabia, Oman and the United Arab Emirates. 90 respondents answered the questionnaire equally distributed over the 3 countries. The questionnaire was posted online and links to it was emailed to respondents.

The respondents were asked to choose one of 5 answers to the given questions. The information they were asked if they would share included a variety of aspects, such as

work and personal PC passwords, confidential work-related documents, work and personal email contents and passwords, current location, and other data thought to be confidential. The respondents had to select their gender and age group while their identities are kept undisclosed. All questions required answers.

4.1.2.2.1 Data Summary

The following table (Table 5: Sensitive information-sharing in 3 GCC countries) summarises the results obtained from the questionnaire:

Table 5: Sensitive information-sharing in 3 GCC countries

Are you willing to share the following information with or allow access to people (i.e. relatives, close friends or friends of friends)?					
* Please indicate your country, age and sex first					
* All questions require answers					
Location	Age Groups			Sex	
30 respondents from Saudi Arabia (33%) 30 respondents from Oman (33%) 30 respondents from United Arab Emirates (33%)	0 (0%) below 19 41 (45.6%) between 19 and 30 43 (47.8%) between 31 and 42 6 (6.7%) between 43 and 54 0 (0.0%) above 54			71 (78.9%) male 19 (21.1%) female	
	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
1. Access to personal PC	35 (38.89%)	44 (48.89%)	8 (8.89%)	3 (3.33%)	0 (0%)
2. Work email content	30 (33.33%)	48 (53.33%)	8 (8.89%)	4 (4.44%)	0 (0%)
3. Credit card details	22 (24.44%)	37 (41.11%)	18 (20%)	8 (8.89%)	5 (5.56%)
4. Work email password	27 (30%)	49 (54.44%)	8 (8.89%)	5 (5.56%)	1 (1.11%)
5. Personal email password	31 (34.44%)	46 (51.11%)	7 (7.78%)	3 (3.33%)	3 (3.33%)
6. Confidential work information	27 (30%)	47 (52.22%)	12 (13.33%)	3 (3.33%)	1 (1.11%)
7. Current location	38 (42.22%)	40 (44.44%)	6 (6.67%)	6 (6.67%)	0 (0%)
8. Work-related documents	27 (30%)	48 (53.33%)	13 (14.44%)	1 (1.11%)	1 (1.11%)
9. Personal mobile phone's password	32 (35.56%)	38 (42.22%)	16 (17.78%)	4 (4.44%)	0 (0%)
10. Access to work PC	26 (28.89%)	55 (61.11%)	8 (8.89%)	1 (1.11%)	0 (0%)

11. Past finished work-related papers/products	25 (27.78%)	48 (53.33%)	15 (16.67%)	2 (2.22%)	0 (0%)
12. Social media password (Facebook, Twitter)	20 (22.22%)	47 (52.22%)	15 (16.67%)	8 (8.89%)	0 (0%)
13. Personal email content	28 (31.11%)	48 (53.33%)	11 (12.22%)	3 (3.33%)	0 (0%)
14. Online banking details	23 (25.56%)	43 (47.78%)	11 (12.22%)	10 (11.11%)	3 (3.33%)
15. Access to personal mobile phone	29 (32.22%)	42 (46.67%)	13 (14.44%)	4 (4.44%)	2 (2.22%)
16. Access to personal USB memory drive	34 (37.78%)	40 (44.44%)	11 (12.22%)	4 (4.44%)	1 (1.11%)
17. Access to a work USB memory drive	29 (32.22%)	50 (55.56%)	5 (5.56%)	6 (6.67%)	0 (0%)
18. Access to other personal mobile devices (laptop, tablet, PDA, etc.)	32 (35.56%)	44 (48.89%)	9 (10%)	3 (3.33%)	2 (2.22%)

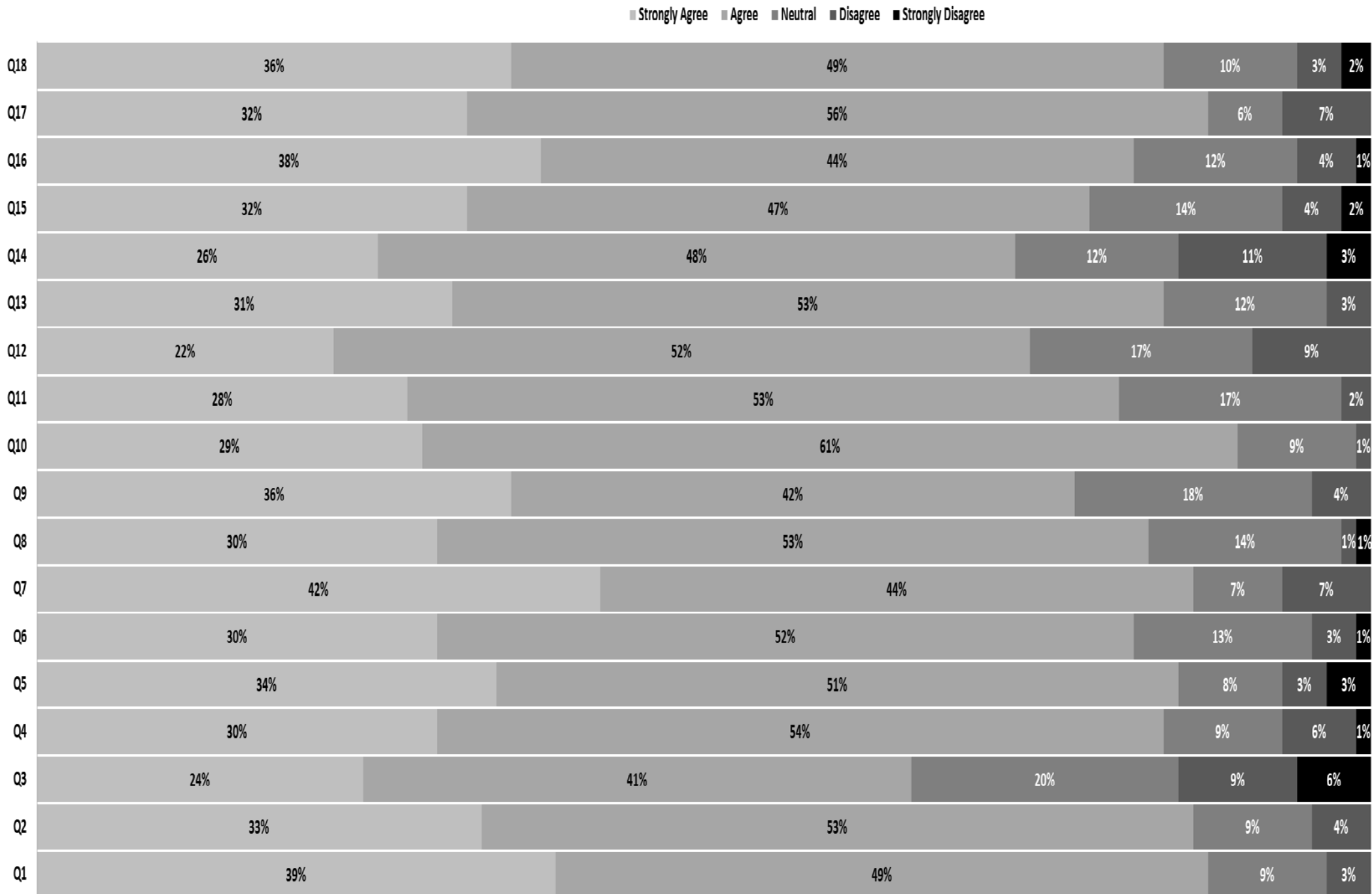


Figure 4: Sharing information which may lead to information security breach GCC

4.1.2.2.2 Descriptive Analysis (Aggregation)

As noted above, using Likert scales for descriptive analysis is highly beneficial. However, central tendency of the scales are best described by mode and median. Calculating the mean and standard deviation is not the best or most informative method for analysing Likert scales. Therefore, colour coding is more expressive in showing the amount of sharing sensitive information for every country. This is shown in the following tables and diagrams:

Oman

Table 6: Sensitive information sharing in Oman

Oman	Strongly Agree	Agree	Neither	Disagree	Strongly Disagree
Q1	15 (50%)	13 (43.33%)	1 (3.33%)	1 (3.33%)	0 (0%)
Q2	7 (23.33%)	21 (70%)	1 (3.33%)	1 (3.33%)	0 (0%)
Q3	2 (6.67%)	17 (56.67%)	4 (13.33%)	7 (23.33%)	0 (0%)
Q4	6 (20%)	20 (66.67%)	2 (6.67%)	2 (6.67%)	0 (0%)
Q5	8 (26.67%)	20 (66.67%)	1 (3.33%)	1 (3.33%)	0 (0%)
Q6	6 (20%)	19 (63.33%)	4 (13.33%)	0 (0%)	1 (3.33%)
Q7	13 (43.33%)	12 (40%)	1 (3.33%)	4 (13.33%)	0 (0%)
Q8	9 (30%)	19 (63.33%)	2 (6.67%)	0 (0%)	0 (0%)
Q9	10 (33.33%)	15 (50%)	4 (13.33%)	1 (3.33%)	0 (0%)
Q10	9 (30%)	18 (60%)	3 (10%)	0 (0%)	0 (0%)
Q11	9 (30%)	18 (60%)	2 (6.67%)	1 (3.33%)	0 (0%)
Q12	6 (20%)	19 (63.33%)	3 (10%)	2 (6.67%)	0 (0%)
Q13	7 (23.33%)	17 (56.67%)	5 (16.67%)	1 (3.33%)	0 (0%)
Q14	1 (3.33%)	17 (56.67%)	4 (13.33%)	8 (26.67%)	0 (0%)
Q15	5 (16.67%)	16 (53.33%)	7 (23.33%)	1 (3.33%)	1 (3.33%)
Q16	11 (36.67%)	16 (53.33%)	3 (10%)	0 (0%)	0 (0%)
Q17	8 (26.67%)	18 (60%)	1 (3.33%)	3 (10%)	0 (0%)
Q18	12 (40%)	16 (53.33%)	1 (3.33%)	1 (3.33%)	0 (0%)

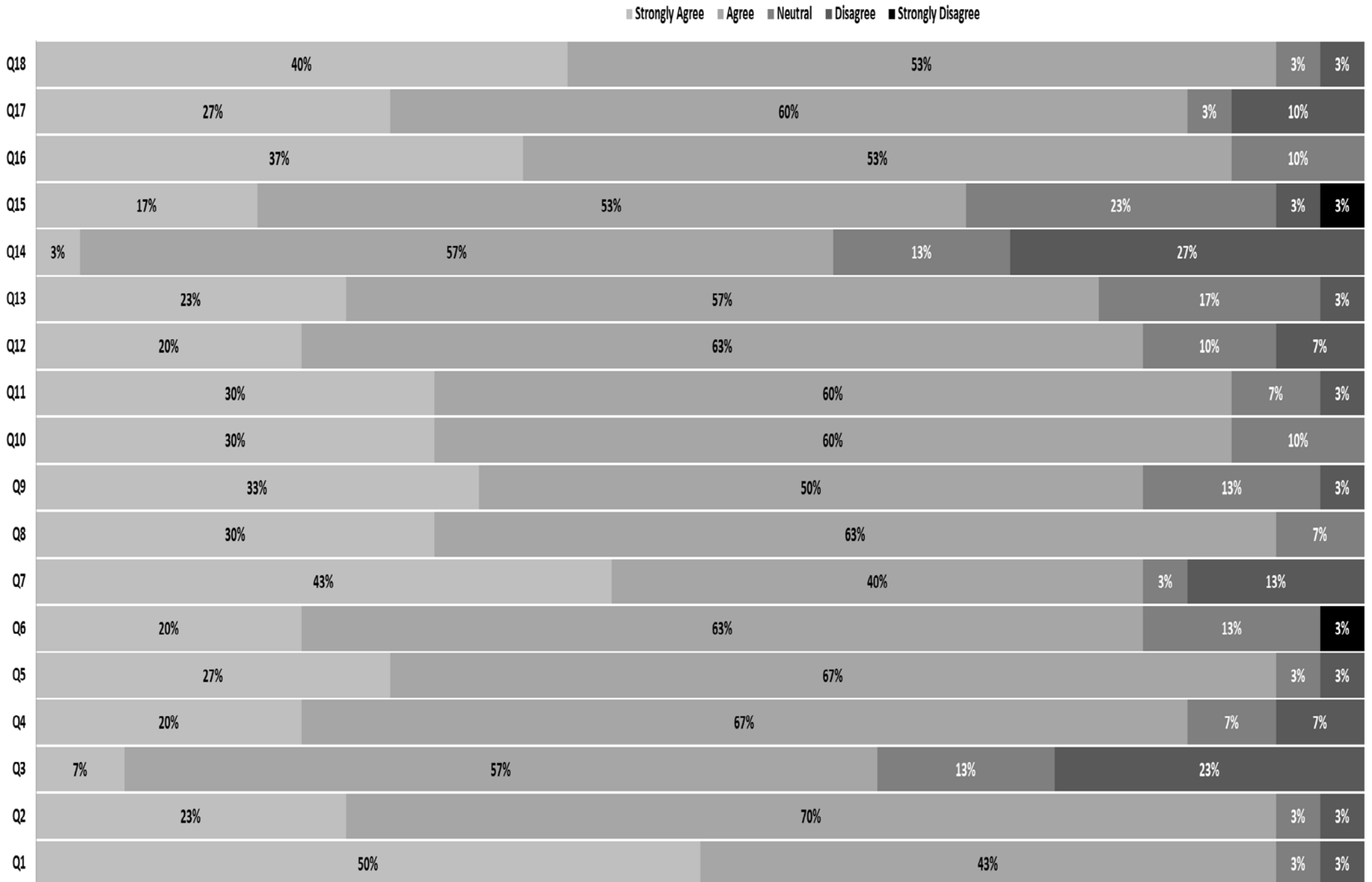


Figure 5: Sharing information which may lead to information security breach (Oman)

KSA

Table 7: Sensitive information sharing in the KSA

KSA	Strongly Agree	Agree	Neither	Disagree	Strongly Disagree
Q1	14 (46.67%)	13 (43.33%)	2 (6.67%)	1 (3.33%)	0 (0%)
Q2	17 (56.67%)	8 (26.67%)	3 (10%)	2 (6.67%)	0 (0%)
Q3	15 (50%)	8 (26.67%)	5 (16.67%)	1 (3.33%)	1 (3.33%)
Q4	15 (50%)	10 (33.33%)	2 (6.67%)	2 (6.67%)	1 (3.33%)
Q5	16 (53.33%)	10 (33.33%)	2 (6.67%)	2 (6.67%)	0 (0%)
Q6	15 (50%)	10 (33.33%)	3 (10%)	2 (6.67%)	0 (0%)
Q7	14 (46.67%)	14 (46.67%)	1 (3.33%)	1 (3.33%)	0 (0%)
Q8	11 (36.67%)	13 (43.33%)	4 (13.33%)	1 (3.33%)	1 (3.33%)
Q9	13 (43.33%)	13 (43.33%)	2 (6.67%)	2 (6.67%)	0 (0%)
Q10	10 (33.33%)	17 (56.67%)	2 (6.67%)	1 (3.33%)	0 (0%)
Q11	11 (36.67%)	12 (40%)	6 (20%)	1 (3.33%)	0 (0%)
Q12	8 (26.67%)	15 (50%)	3 (10%)	4 (13.33%)	0 (0%)
Q13	15 (50%)	12 (40%)	2 (6.67%)	1 (3.33%)	0 (0%)
Q14	15 (50%)	12 (40%)	1 (3.33%)	1 (3.33%)	1 (3.33%)
Q15	17 (56.67%)	10 (33.33%)	1 (3.33%)	1 (3.33%)	1 (3.33%)
Q16	14 (46.67%)	10 (33.33%)	3 (10%)	2 (6.67%)	1 (3.33%)
Q17	13 (43.33%)	12 (40%)	2 (6.67%)	3 (10%)	0 (0%)
Q18	13 (43.33%)	12 (40%)	3 (10%)	0 (0%)	2 (6.67%)

Strongly Agree Agree Neutral Disagree Strongly Disagree

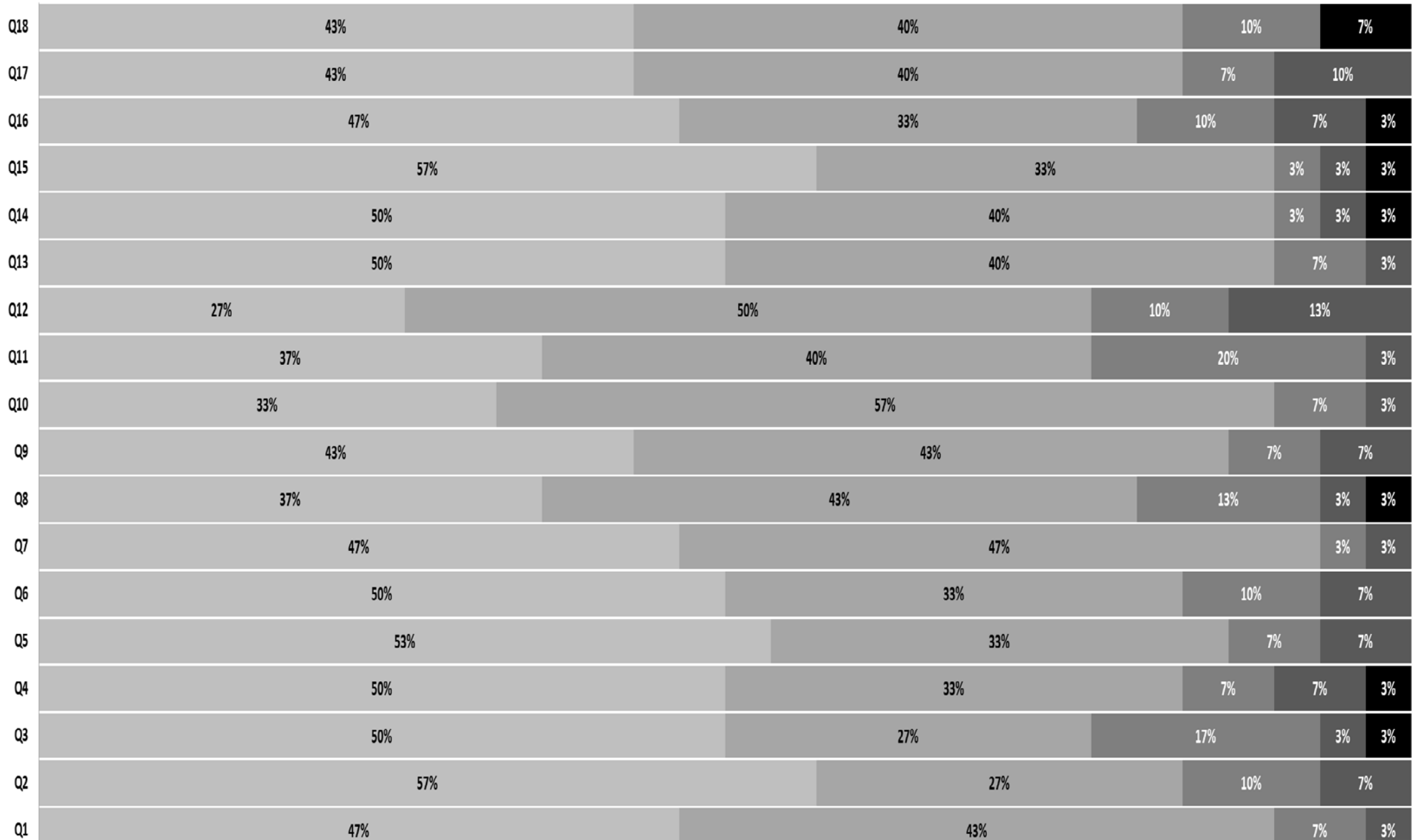


Figure 6: Sharing information which may lead to information security breach (KSA)

UAE

Table 8: Sensitive information sharing in UAE

UAE	Strongly Agree	Agree	Neither	Disagree	Strongly Disagree
Q1	6 (20%)	18 (60%)	5 (16.67%)	1 (3.33%)	0 (0%)
Q2	6 (20%)	19 (63.33%)	4 (13.33%)	1 (3.33%)	0 (0%)
Q3	5 (16.67%)	12 (40%)	9 (30%)	0 (0%)	4 (13.33%)
Q4	6 (20%)	19 (63.33%)	4 (13.33%)	1 (3.33%)	0 (0%)
Q5	7 (23.33%)	16 (53.33%)	4 (13.33%)	0 (0%)	3 (10%)
Q6	6 (20%)	18 (60%)	5 (16.67%)	1 (3.33%)	0 (0%)
Q7	11 (36.67%)	14 (46.67%)	4 (13.33%)	1 (3.33%)	0 (0%)
Q8	7 (23.33%)	16 (53.33%)	7 (23.33%)	0 (0%)	0 (0%)
Q9	9 (30%)	10 (33.33%)	10 (33.33%)	1 (3.33%)	0 (0%)
Q10	7 (23.33%)	20 (66.67%)	3 (10%)	0 (0%)	0 (0%)
Q11	5 (16.67%)	18 (60%)	7 (23.33%)	0 (0%)	0 (0%)
Q12	6 (20%)	13 (43.33%)	9 (30%)	2 (6.67%)	0 (0%)
Q13	6 (20%)	19 (63.33%)	4 (13.33%)	1 (3.33%)	0 (0%)
Q14	7 (23.33%)	14 (46.67%)	6 (20%)	1 (3.33%)	2 (6.67%)
Q15	7 (23.33%)	16 (53.33%)	5 (16.67%)	2 (6.67%)	0 (0%)
Q16	9 (30%)	14 (46.67%)	5 (16.67%)	2 (6.67%)	0 (0%)
Q17	8 (26.67%)	20 (66.67%)	2 (6.67%)	0 (0%)	0 (0%)
Q18	7 (23.33%)	16 (53.33%)	5 (16.67%)	2 (6.67%)	0 (0%)

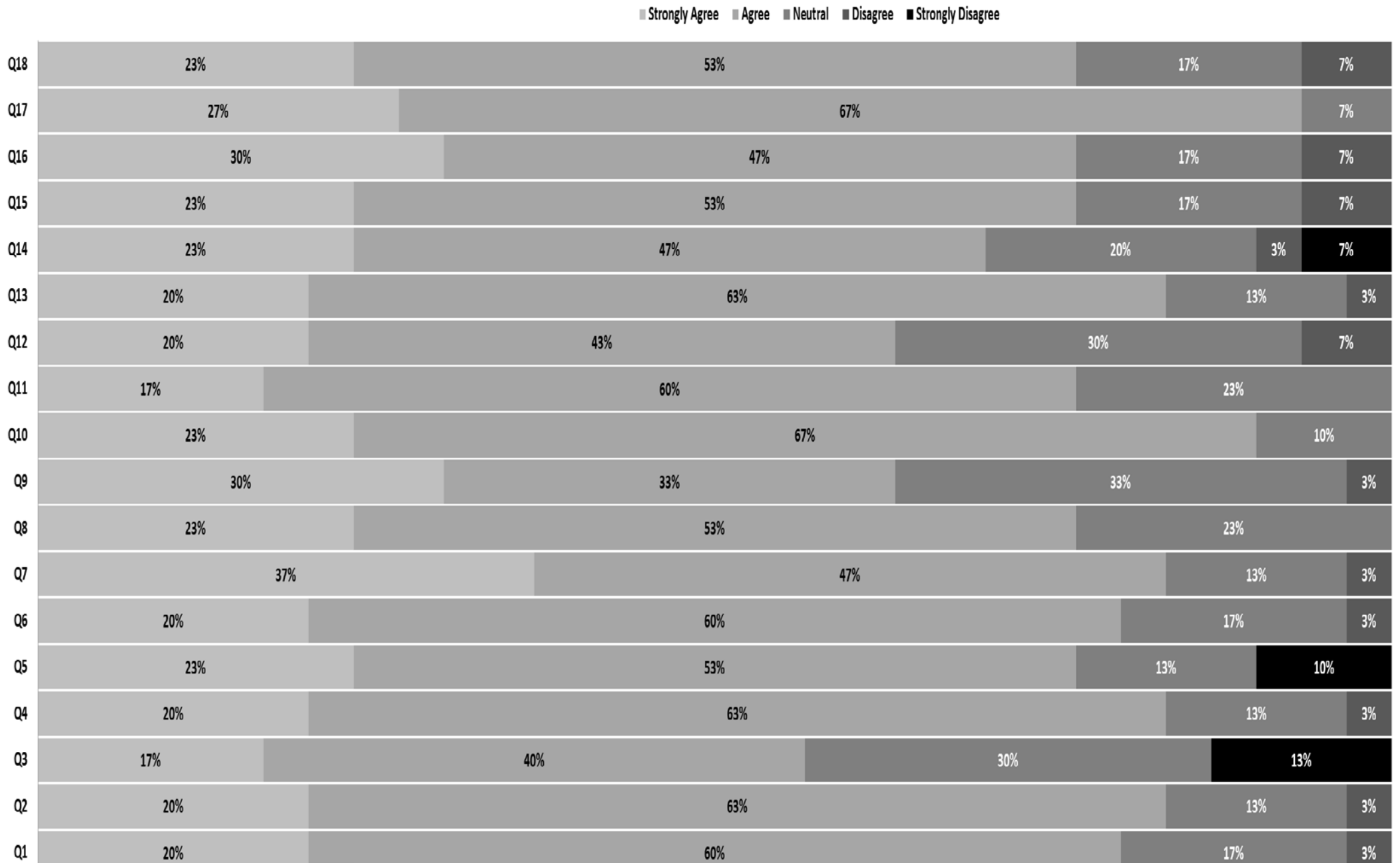


Figure 6: Sharing information which may lead to information security breach (UAE)

4.1.1.1.1 *Inferential Analysis*

Inferential Analysis on the differences among the three groups (Saudi Arabia, Oman and United Arab Emirates)

The table below shows the results of Kruskal-Wallis One-Way ANOVA. As can be seen, the 3 samples collected show a similar behaviour in almost all questions towards information-sharing.

Kruskal–Wallis One-Way ANOVA Test

This method is used for non-parametric data as the same data was obtained from the three countries (Saudi Arabia, Oman and the United Arab Emirates). This method is the most suitable one for measuring the significant difference between more than three groups (McCrum-Gardner, 2008)

Table 9: The Kruskal-Wallis One-Way ANOVA test results

Hypothesis Test Summary				
	Null Hypothesis	Test	Sig.	Decision
1	The distribution of Q1 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.026	Reject the null hypothesis.
2	The distribution of Q2 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.058	Retain the null hypothesis.
3	The distribution of Q3 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.006	Reject the null hypothesis.
4	The distribution of Q4 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.135	Retain the null hypothesis.
5	The distribution of Q5 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.056	Retain the null hypothesis.
6	The distribution of Q6 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.100	Retain the null hypothesis.
7	The distribution of Q7 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.591	Retain the null hypothesis.
8	The distribution of Q8 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.438	Retain the null hypothesis.
9	The distribution of Q9 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.235	Retain the null hypothesis.
10	The distribution of Q10 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.791	Retain the null hypothesis.
11	The distribution of Q11 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.315	Retain the null hypothesis.

Hypothesis Test Summary				
	Null Hypothesis	Test	Sig.	Decision
12	The distribution of Q12 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.543	Retain the null hypothesis.
13	The distribution of Q13 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.043	Reject the null hypothesis.
14	The distribution of Q14 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.000	Reject the null hypothesis.
15	The distribution of Q15 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.004	Reject the null hypothesis.
16	The distribution of Q16 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.482	Retain the null hypothesis.
17	The distribution of Q17 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.639	Retain the null hypothesis.
18	The distribution of Q18 is the same across categories of Country.	Independent-Samples Kruskal-Wallis Test	.163	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

The Kruskal-Wallis One-Way ANOVA test reveals similarities among the 3 countries in most questions, showing similar behaviour towards information-sharing in the 3 GCC countries.

4.1.1.2 Discussion

Developing advanced hacking methods is the ultimate aim of cyber criminals, which can be used to steal money and information. Social engineering is changing the face of hacking activities as there is no technology that can prevent a social engineering attack. However, user education that leads to the outcome of less social trust will slow the pace of social engineering (Warren and Leitch, 2006).

The attitude of sharing sensitive information shown by the above study is believed to have a strong relation to the cultural attitude. Although Arab culture has been visibly

influenced by globalisation and, in particular, the West, Islam is still the most prevalent religion in the Arab countries and that affects almost every aspect of their behaviour. Certain characteristics of Arab culture are strengthened by Islam such as honesty, loyalty, flexibility, and trust (Obeidat et al, 2012).

The issue of sharing sensitive information can only be solved by looking at the root of the problem which is human behaviour in this case. Furthermore, the culture of trust needs to be examined in depth. Understanding cultural issues is essential in IT management as there might be some internal resistance by employees or users. Using foreign companies' services and experts to develop policies and procedures about information security raises the risk that these policies may not consider the current organisational culture (Khalfan, 2004). Encouraging ICT users not to share their confidential information with their friends or relatives because it is the wrong attitude (only because this practice cannot be seen in developed countries) will not lead to a significant contribution from other perspectives. Looking at the root causes of the problem and developing a solution according to those causes will significantly reduce the likelihood of risk.

There are two main drivers of the information-sharing problems: the first one is the cultural factor and the second one is the lack of information security awareness. The cultural factor resulting from the trust phenomena makes the user share his or her private information with friends and relatives. It is clearly recognised that privacy and security are difficult to manage from the technical perspective since they are entangled in larger collective rhetoric and practices of risk, danger, secrecy, trust, morality, identity. Consequently, dealing with these issues individually produces an incoherent and weak outcome (Dourish & Anderson, 2006). Concerning the lack of security awareness, the high Internet penetration growth rate in the Arab countries and the limited security awareness among users renders online resources attractive for cyber criminals (Aloul, 2012). In this connection, Aloul (2012) asserts that education on user privacy is imperative for Arab Internet users due to the lack of knowledge of social engineering attack techniques. Furthermore, the continuous increase of Internet usage increases the likelihood that attackers can gain unauthorised access to information by exploiting a user's trust and tendency to help (Aloul, 2012). Security awareness courses and training approaches are prominently suggested as a remedial attempt to reduce IT security threats. Information security awareness programmes should focus more on the social and cultural differences and the different terms and concepts related to them (Kruger et al, 2011).

It is clear that sharing sensitive information is a social vulnerability which can be easily exploited using social engineering attack. As a result, the damage can have an impact on both individuals and organisations. However, dealing with the above factors separately can lead to unexpected human reaction. Instead, looking for an effective solution that takes into consideration every contributing factor (causes and impacts) of the sharing phenomena and then combining these factors to design the solution (cost, ease, and efficiency) can bring about the required results.

4.1.1.3 Hypothesis 2: Users' attitudes in GCC Countries and the UK

Proposition 2 relates to a comparative investigation between two different cultural backgrounds. Despite the fact that the United Kingdom is known as an individualist culture, where its characteristics are different than GCC countries, the aim of this study was to identify any similarities or differences between the two cultures in relation to the sharing preferences with friends and family members.

4.1.1.3.1 Results and analysis (GCC and UK)

Data Summary

The following table summarises the results obtained from the questionnaire that targeted 90 private individuals (white English) who work in Council departments in the UK:

Table 11: Sensitive information sharing in the UK

Are you willing to share the following information with or allow access to people (i.e. relatives, close friends or friends of friends)?					
* Please indicate your country, age and sex first					
* All questions require answers					
Location	Age Groups			Sex	
90 respondents (White English)	34 (37.8 %) between 23 and 34 29 (32.2%) between 35 and 44 27 (30%) over 44			42 (46.7%) male 48 (53.3%) female	
	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
1. Access to personal PC	25 (27.78%)	34 (37.78%)	7 (7.78%)	10 (11.11%)	14 (15.56%)
2. Work email content	5 (5.56%)	12 (13.33%)	7 (7.78%)	19 (21.11%)	47 (52.22%)
3. Credit card details	4 (4.44%)	5 (5.56%)	3 (3.33%)	25 (27.78%)	53 (58.89%)
4. Work email password	3 (3.33%)	4 (4.44%)	1 (1.11%)	25 (27.78%)	57 (63.33%)
5. Personal email password	6 (6.67%)	9 (10%)	8 (8.89%)	23 (25.56%)	44 (48.89%)
6. Confidential work information	0 (0%)	4 (4.44%)	4 (4.44%)	24 (26.67%)	58 (64.44%)
7. Current location	16 (17.78%)	33 (36.67%)	14 (15.56%)	16 (17.78%)	11 (12.22%)
8. Work-related documents	1 (1.11%)	4 (4.44%)	6 (6.67%)	28 (31.11%)	51 (56.67%)
9. Personal mobile phone's	3 (3.33%)	10 (11.11%)	14 (15.56%)	16 (17.78%)	47 (52.22%)

password					
10. Access to work PC	3 (3.33%)	8 (8.89%)	4 (4.44%)	18 (20%)	57 (63.33%)
11. Past finished work-related papers/products	2 (2.22%)	9 (10%)	10 (11.11%)	21 (23.33%)	48 (53.33%)
12. Social media password (Facebook, Twitter)	4 (4.44%)	5 (5.56%)	10 (11.11%)	25 (27.78%)	46 (51.11%)
13. Personal email content	5 (5.56%)	13 (14.44%)	13 (14.44%)	23 (25.56%)	36 (40%)
14. Online banking details	2 (2.22%)	5 (5.56%)	3 (3.33%)	20 (22.22%)	60 (66.67%)
15. Access to personal mobile phone	8 (8.89%)	19 (21.11%)	18 (20%)	15 (16.67%)	30 (33.33%)
16. Access to personal USB memory drive	6 (6.67%)	15 (16.67%)	18 (20%)	19 (21.11%)	32 (35.56%)
17. Access to a work USB memory drive	2 (2.22%)	5 (5.56%)	6 (6.67%)	20 (22.22%)	57 (63.33%)
18. Access to other personal mobile devices (laptop, tablet, PDA, etc.)	9 (10%)	20 (22.22%)	13 (14.44%)	17 (18.89%)	31 (34.44%)

As opposed to the table obtained from the three GCC countries surveyed, it can be seen that respondents in the UK are less inclined to share information that is regarded sensitive from an information security perspective. The results can be better seen in Figure 6.

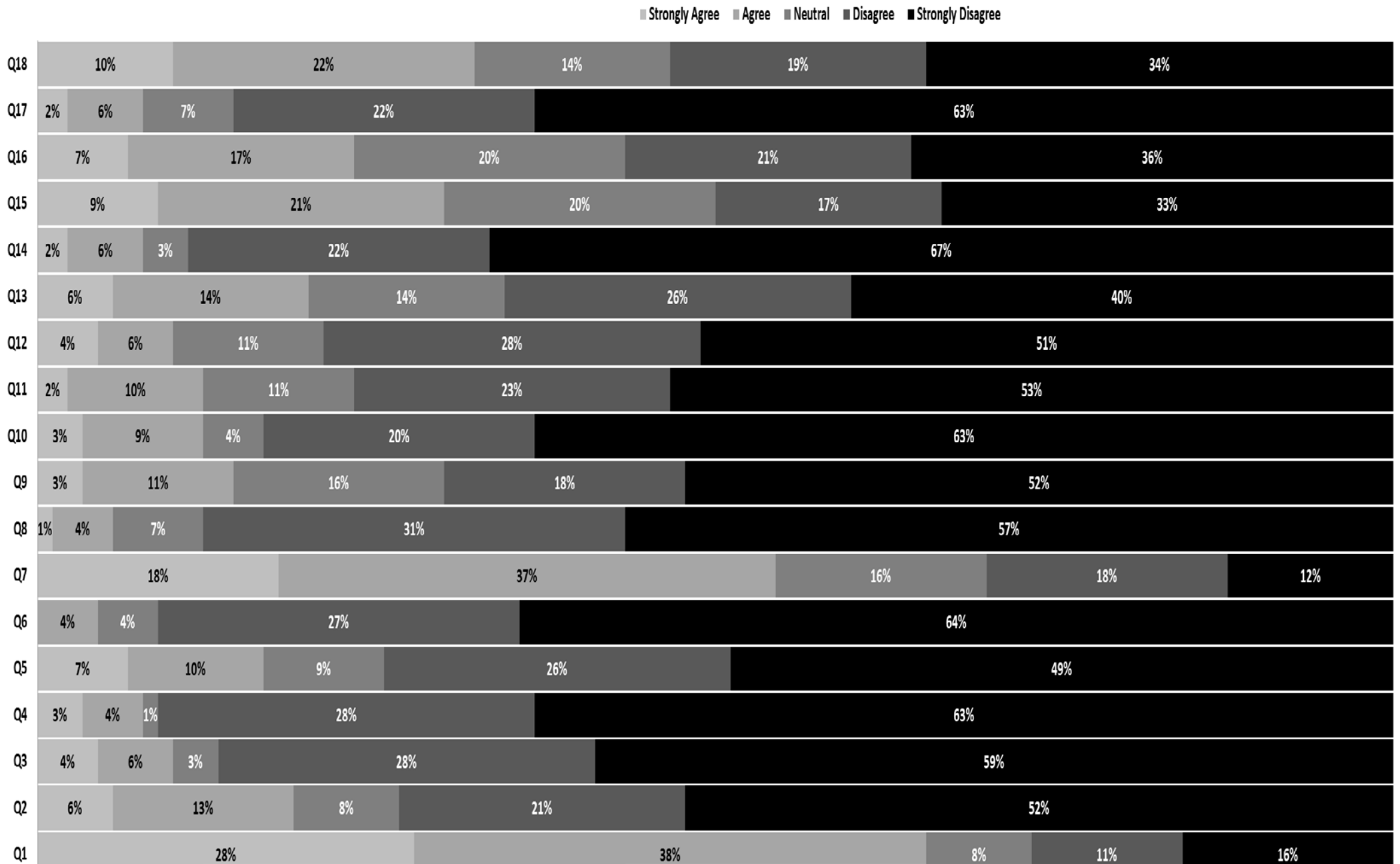
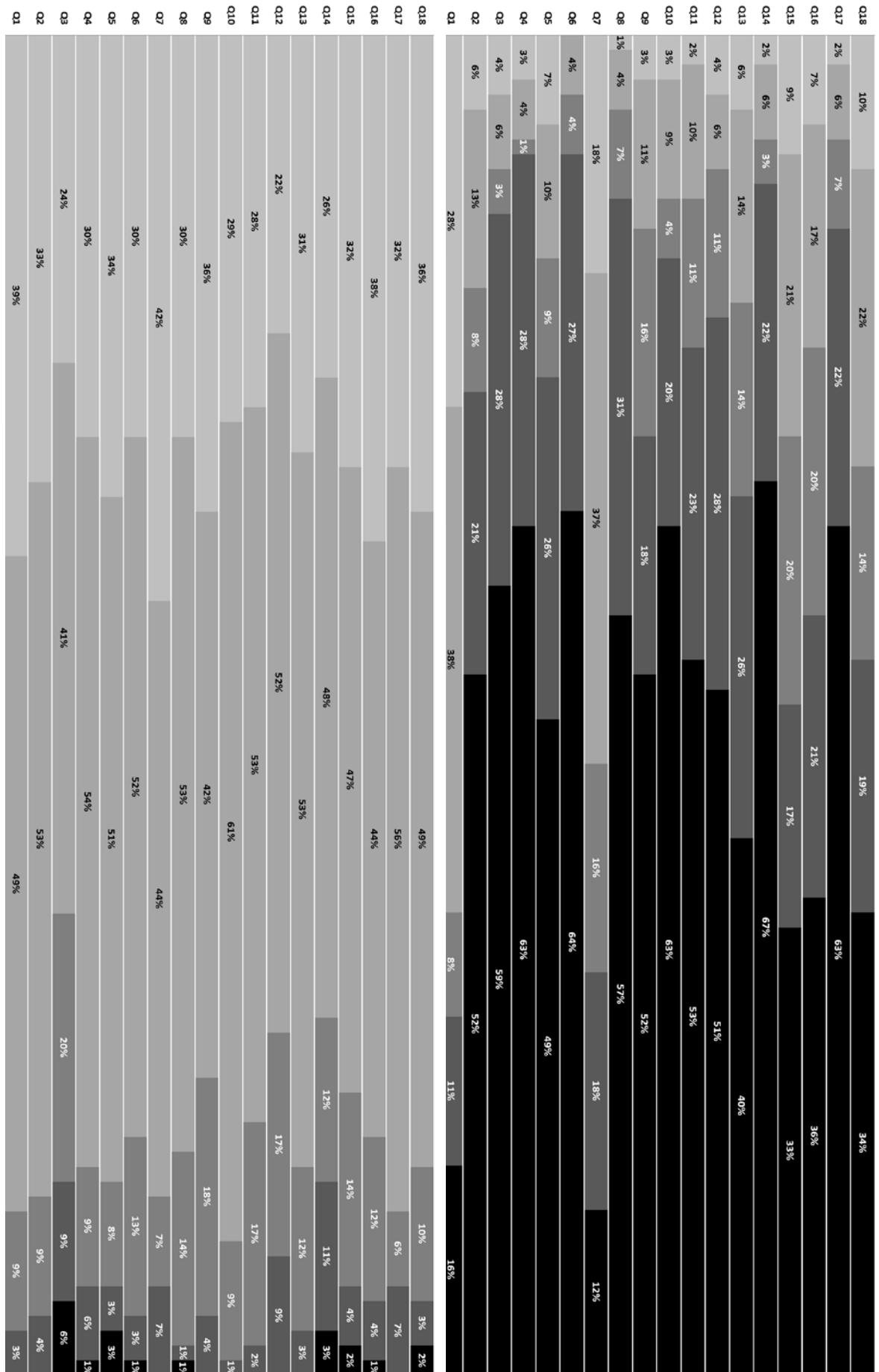


Figure 7: Sharing information which may lead to information security breach (UK)

The difference between the two groups may be better observed if the figures are placed next to each other as shown in Figure 4.



GCC

UK

Figure 8: Inferential analysis of the differences between the two regions (GCC and the UK)

To maintain that the difference in the results between the two groups, the three GCC countries and the UK, was not due to chance, statistical testing was used on the results. The non-parametric Mann-Whitney U test was used to compare the two groups. The Mann-Whitney U test was conducted to evaluate whether there exists a statistically significant difference in information security preferences between the two groups. The null hypothesis is stated below:

H₀: There is no significant difference between the two groups

The Mann-Whitney U test supports the conclusion that the difference indicated in the above tables and figures are actually significant. The table below shows the results of Mann-Whitney U One-Way ANOVA. As can be seen, the two groups show a different behaviour in all questions towards information sharing.

Table 10 - Results of Mann-Whitney U One-Way ANOVA

Null Hypothesis	Test	Sig.	Decision
The distribution of Q1 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q2 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q3 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q4 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q5 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q6 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q7 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q8 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis

Null Hypothesis	Test	Sig.	Decision
of Group	Samples Mann-Whitney U Test		reject the null hypothesis
The distribution of Q9 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q10 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q11 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q12 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q13 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q14 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q15 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q16 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q17 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q18 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis

Asymptotic significances are displayed. The significance level is .05.

4.1.1.4 Discussion

As indicated above, there is a significant difference between the GCC and UK respondents in terms of sensitive information sharing in all of the answers collected. The

results show that there are culture-related differences regarding perspectives to information security and privacy. However, there is a further result to note in this respect. Despite the fact that people of the GCC countries share sensitive information among their family members and friends more commonly than their UK counterparts, UK people show risky behaviour in some scenarios, which may result in threats to the authentication mechanism and consequently to digital accounts that require a credential pass. Several studies conducted in the UK addressing the extent of social engineering attacks and its impact on information security show that many users fall victim to social engineering attacks (Robila & Ragucci, 2006; Aburrous et al, 2010; Dimensional Research, 2011). It is believed that such attacks are possible only because of posting of personal information on social networking websites, as well as lack of awareness of fraud and phishing attacks. Governments worldwide try to reduce the impact of computer crimes by raising user education and information security awareness. For example, the UK cybersecurity strategy of 2011 alludes to the risk of social engineering attacks and the need to enhance the individual's skills through security education. Moreover, the UK strategy aims to improve cybersecurity education at all levels using different approaches of user awareness in the public and private sector. It aims to provide Internet users with a complete understanding of cybersecurity risks associated with using Internet social media.

Although it happens on a smaller scale in comparison to the GCC countries, the results of this study imply that the UK cybersecurity strategy may also need to consider the sharing preference of private information publically when designing information security education courses. Due to the potentially significant results of sharing sensitive information, it is important for the UK cybersecurity to put more effort into this aspect. For example, the UK cyber strategy recommends some websites designed to educate online users such as www.getsafeonline.org and make them aware of the actual risks of information security. These online resources may need to include sharing sensitive information and the impact of this activity on online users as indicated this study.

The prevalence of social media websites makes it easier for attackers to accumulate, compare and analyse people's personal information and then start implementing an attack. For example, a telephone number sent to a Facebook user with a fake profile can be verified using a real caller application (another social media source) in order to retrieve some information about the user. Internet users must therefore be educated about

real breaches as this will make them aware of the threat that is inherent in online activities. The same topic is further discussed in a study conducted in the healthcare domain. The study asserts that awareness and training of end users should focus on their behaviour, in particular password sharing, which may lead to a breach (Ferreira et al, 2010).

In respect of the GCC countries, it is extremely important that they carefully consider the problem of sensitive information sharing. The problem is rooted in the culture of trust and sharing sensitive information among friends and family members. Therefore, any information security strategy in these countries must consider trust and social influences of Arab culture when designing security courses.

4.2. Conclusion

The weakest link is the preferable place for hackers to penetrate any authentication controls. It is believed that humans are this link as rather than system security. In this Chapter the challenges to the information security triad have been linked to human behaviour based on cultural attributes. A culture of trust allows sharing sensitive information which may lead to compromised digital authentication and consequently potential harm to both individuals and organisations.

A questionnaire consisting of 18 questions was administered to test information-sharing attitudes of a sample of 180 employees in UAE, Oman, KSA and the U.K. The questions were related to direct and indirect aspects which lead to compromising digital authentication. Based on social engineering threats and user behaviour on the Internet, a questionnaire was designed particularly to investigate the sharing preferences to the first security control: the authentication mechanism. The data collected were focused on areas in a cultural context such as: personal belongings, work belongings and trust and social influences towards family members and friends.

The results indicate that there are similarities among the 3 countries in most questions, showing similar attitudes towards sharing sensitive information in the 3 GCC countries and this is believed to have a strong relation with the cultural and social background.

This chapter also presented a comparison between the UK and the GCC (Gulf Cooperation Council) countries in terms of attitude and behaviour towards information sharing. The data analysis showed that there is a significant difference between GCC and the UK cultures in terms of information sharing. This chapter also discussed the actual

and potential threats associated with the phenomenon of sharing sensitive information with family and friends.

Certain social and cultural backgrounds of employees may represent a threat to the organisation when those backgrounds inherently conflict with information security awareness, which may consequently breach the criteria used for information security compliance. This aspect of conflict may be, and usually is, exploited by social engineering, which manipulates users to bypass the security controls instead of using technical skills. Social engineering attacks have proven effective resulting in serious damage to both individuals and organisations. The damage that could potentially occur due to the sharing of sensitive information among individuals because of cultural traits is extended to the law enforcement community. Law enforcement bodies find it extremely difficult to deal with identity theft if it occurs as a result of information sharing. Social engineers use different approaches to gather a victim's personal information which can be a key element for the next hacking stages. The threat of social engineering is strong as shown in the scenarios provided by this study. The behaviour of employees should be in line with the information security policy of the organisation in order not to become a victim of such social engineering.

The results show the need for information security awareness and education in the GCC region. It is observed that in order to reduce the impact of these threats, it is strongly recommended to consider the root causes of the problem which stem from cultural factors and the lack of information security awareness. Looking for a different solution to each factor of the cause will not lead to the desired results of information security. This may be referred to as a culture-integrated information security solution.

It was shown that, despite the fact that people of the GCC countries share sensitive information among their family members and friends more significantly than those of the UK, UK people show risky behaviour in some scenarios, which may comprise potential threats to the authentication mechanism and consequently to other digital accounts that require a credential pass.

Account access is meant to be the account owner's sole right and the owner should be aware of the consequences that may result from sharing this right with others.

CHAPTER 5: SOCIAL ENGINEERING ATTACK MITIGATION

In the previous chapter it was indicated that there is a cultural difference towards sharing of sensitive information between the GCC countries and the UK. People of the GCC countries share sensitive information among their family members and friends more commonly than those in the UK. This social attribute forms a threat such as a privacy attack or a social engineering attack. Similarly, sharing of sensitive information was also identified in health care institutions (Medlin et al, 2008; Ferreira et al, 2010) which can also be used to execute using social engineering attacks.

Although the results obtained call for a mitigation of information security awareness and education in the GCC region, there are some other mitigation measures which could help to reduce the threat of social engineering attacks. According to several studies (for example Baker et al, 2005; Ferreira et al, 2010) combating social engineering attacks can be performed through the following measures:

- Legislation
- Technology
- Education and Awareness

Based on the outcomes of the previous chapter, the lack of information security awareness and the cultural impact are behind the sharing phenomena among family members and friends. This chapter provides several mitigation measures as candidates for further implementation plans that cover both the cultural influence and the lack of information security awareness.

5.1. Legislation Measures

According to the Science and Technology Committee (2007), a law requiring organisations to notify their clients whenever there is a breach of data security should be the first step towards promoting personal security and privacy on the Internet. In the U.S., such laws are commonplace, with at least 45 states having adopted data breach disclosure laws by the end of 2009. Ideally, data breach disclosure laws are meant to help people mitigate the consequences of their personally identifiable information (PII) being

disclosed to third parties. According to Romanosky et al. (2010) such laws are motivated by the concept that if corporate organisations and government bodies are required by law to disclose any information security breaches, they will realise that such disclosures will have negative publicity for them. Consequently, they will improve their security measures and rid themselves of substandard security practices. The Ponemon Institute (2005) supports the previous argument by indicating that a significant number of consumers have been found to lose confidence in firms that suffer information security breaches.

Although no country has fully tapped into the legal approach of creating consequences for perpetrators of social engineering attacks, Lewis (2014) notes that attribution of such attacks is not too complicated nowadays. In other words, it is not easy to pinpoint who the perpetrator is in a social engineering attack. Lewis (2014) notes that the absence of criminal or civil consequences for perpetrators means that they can escape responsibility for the attack. Admittedly, pursuing a perpetrator who may reside in a different geographical area may be expensive and difficult. However, governments can use legislation to ensure people found engaging in social engineering attacks will pay for their crimes.

The challenge with identity theft can be extended to law enforcement too. The investigator must provide rigorous evidence to prove, beyond reasonable doubt, that the suspect was the person who was in control of the device when the actions took place. This can be difficult especially when the case is related to passwords and tokens, as they could have been obtained and used by someone else (Jones & Martin, 2010).

Lewis (2014) further argues that legislation needed to establish how much is too much when companies or governments retaliate (e.g. by hacking back). The author argues that placing false information on one's network is one way which companies can mislead hackers. However, companies, individuals and/or governments should avoid going out of their own network. If a company goes into another company's network, with the intention of retaliating against alleged social engineering attacks, Lewis (2014) argues that then becomes a matter that needs to be handled by the law. Unfortunately, not enough legislative measures are in place to provide the necessary deterrent measures to such retaliatory attacks.

From the literature, it would appear that most efforts to address social engineering are

based in the US. For example, the US enacted the Identity Theft and Assumption Deterrence Act in 1998, which made it a felony to:

Knowingly transfer, possess or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local laws (Scheb & Scheb , 2011).

Other countries are yet to catch up, despite their populations being equally susceptible to social engineering attacks. In an effort to curb identity theft, the US established the Identity Theft Task Force (ITTF), whose mandate was to examine the use of legislative measures in investigating, prosecuting and recovering proceeds obtained by criminals who carry out identity theft (Ryder, 2011). Another mandate of the ITTF is to suggest policies and safety mechanisms which can enhance people's security and privacy of information. ITTF recommend that: People's social security numbers should be used by federal agencies (or corporate organisations) only when necessary, national standards requiring corporate organisations to safeguard PII, and give notice to consumers whenever there is a breach need to be established; federal agencies need to create awareness among consumers, the public and private sectors on defending themselves against detecting and deterring perpetrators of social engineering; and that a law enforcement centre, with a specific responsibility to coordinate information and efforts on curbing social engineering, should be established (Ryder, 2011). Despite the apparent support from US legislature, some authors such as Lafferty (2007), indicate that there is still no law enforcement on the ground. Consequently, Lafferty (2007) suggests that most of the war against social engineering will have to be fought by individual organisations and professionals.

At the European level, the Data Protection Directive 95/46/EC is cited as a leading legislative instrument in combating social engineering attempts. The directive indicates that anyone who violates its legal requirements, which make it unlawful for people to unlawfully acquire and use personal data, can be prosecuted (Robinson et al, 2011). Another policy that has been suggested by Robinson et al (2011) is a requirement for biometrics to be produced by users of PII. Such a requirement, it has been argued, would make it impossible for hackers to fraudulently benefit from the PII obtained about people. For example, without being able to match victims' biometrics, their names, addresses, date of birth, financial and insurance details, a perpetrator, who wanted to use them for

financial gain, would not benefit (Robinson et al, 2011). However, this proposal remains only a proposal to date. Even if it were made into a legislative instrument, it is argued that corporate organisations that stand the risk of losing their trade and competitive information to hackers would not benefit much from the proposal. Notably however, such a policy measure would safeguard the interests of millions of private citizens whose vulnerability to social engineering attacks costs them a great deal of money annually and subjects them to distress.

Alder (2006) cites that many of the recent statutes, regulations and court cases demonstrate regulatory requirements for security that closely resemble established information security standards. Abu Dhabi Police Department has recently faced a case of fraud, theft and seizure by a police sergeant who was made redundant in 1999 after being diagnosed unfit for service due to ill-health. The prosecutors accused the former policeman of breaking into the electronic system of the Ministry of Interior as an official and promoting himself to Captain and to Major eight months after. Having no evidence of breaking into the system, the judge could not reach a verdict on the policeman being guilty on the grounds of UAE criminal law.

Edward Snowden, the former US NSA contractor, obtained several login access details from employees working at NSA (Reuters). Snowden successfully used a social engineering attack to trick between 20 and 25 fellow workers at the NSA regional operations centre into giving their passwords to allow access to classified information, which he later leaked to the media. Most interestingly, NSA was not clear what regulations the employees had broken by giving Snowden their password login details which allowed him to access classified data.

Overall, it would appear from the analysis above that, legislative measures for curbing social engineering attacks are still an area that needs to be developed. As Robinson et al (2011) note, effective legislation would require governments to work together to provide punitive and deterrence measures that are not only applicable in one geographical jurisdiction, but also across borders. This is informed by the fact that social engineering attacks are not limited by geographical locations. A perpetrator in China can, for example, wage attacks on British citizens or on UAE citizens.

5.2. Technological Measures

Although there are several techniques that offer solutions to the problem of privacy attack

and social engineering attack, such as cryptography, digital certificates, biometrics, etc, these solutions involve a danger that implementations will ignore the realities of how users and administrators behave. Implementations of technology should have reasonable expectations about what the user can and will do (Cox et al, 2001). The same point is addressed by (Inthiran & Seddon, 2007) who claim that although technological measures may add to the strength of policies and technological devices may increase the immunity of the organisation, organisations have to realise that having policies does not guarantee protection of its resources and reputation without the entire cycle of conceptualisation and employee involvement.

Bjork (2005) noted that “it doesn’t matter what technology you have – there is no technology that can protect you against human beings” (p. 186). While the truth of this statement is arguable, the statement holds some sense in that social engineering attacks do not target the technological aspect of an organisation. Rather, it targets the individuals within it, with the aim of obtaining information that will enable perpetrators to gain access to the system. However, the foregoing does not mean that technology measures are completely irrelevant. Technical controls such as routers, encryption, antivirus software, firewalls, smart cards, alarms and alerts, biometrics, and dial-up call-back systems, amongst others, can be used to protect information in a manner that ensures that confidentiality and integrity of data is maintained.

5.1.3 Restricting Data Access

To succeed in restricting access to data, Davis (2014) observes that technology experts need to build technological features into an operating system. The features restrict access to information based on the user’s knowledge of a common secret or based on their identity. When used correctly, restricting access to data is an efficient manner of curbing social engineering efforts; however, and as Davis (2014) indicates, it has its limitations. For example, it may not prevent different users in the same network from accessing information stored in different computers. The implication of this is that if one computer is compromised, the effects can be felt in an entire network.

5.1.4 Encrypting data

Data encryption is another technical measure that organisations can adopt to curb social engineering. The primary goal of data encryption is to make data undecipherable to anyone who has access to it, but does not have a decryption key. Cryptography can protect data from being accessed by unauthorised parties, prevent data from being altered,

and prevent non-repudiation where the receiver would deny receiving information or the sender would deny ever sending it (Klingman, 2005). Using an encryption key, the person encrypting data converts readable text into non-readable ciphertext, and only a person with an encryption key can re-convert it into readable text. The challenge for organisations that use data encryption as a method of curbing social engineering is to ensure that the decryption key is well hidden and that no unauthorised persons can access or control the same (Davis, 2014). It has been argued that encrypting data merely transforms problems associated with data protection into problems “of protecting cryptographic keys” (Davis, 2014,).

5.1.5 Data Hiding

Also known as security through obscurity, data hiding strives to store sensitive information in a place where people cannot easily find it. Some of the places where information is hidden include the application source code, Windows registry and configuration files (Davis, 2014). It is however suggested that social engineers can easily detect when data is hidden, particularly with utilities such as diskmon, filemon, and regmon (Davis, 2014). Data hiding can be done by embedding secret messages on images, in video sequences, audio sequences, and even in IPv4 headers (Kayarkar & Sanyal, 2012). The latter is especially useful when transmitting data over networks, and involves fragmenting data into different sizes and appending each fragment with a message authentication code (MAC). For the recipient to decipher the information, he or she needs to have the message authentication code. In other words, the sender and the recipient need to have pre-shared the MAC in the same sequences that the messages were sent (Davis, 2014).

5.1.6 Controlling System Access

Controlling access to information by layering the clearance levels is also cited as a measure through which social engineering can be reduced. For example, an organisation may require people to use passwords, a personal identification number (PIN), or biometric identifiers before accessing specific information. Of these, biometric identifiers are the most efficient, yet the most expensive to run (Siddiqui & Muntjir, 2013). In biometrics, the system captures a person’s unique biometric identifiers, processes them, and stores them. During verification, the specific biometric identifier is captured, processed, compared with what is in the system and either accepted or denied depending on whether a match was found. Some of the biometric measures available include face

recognition, voice analysis, signature biometrics, vein geometry, iris scan, retina scan and geometry of the hand (Siddiqui & Muntjir, 2013). One of the advantages of using biometrics is that they cannot be easily mimicked or stolen. The downside of biometrics, however, is that for it to work it has to first gather and store someone's intrinsic information. To people of different cultures and religious persuasions, obtaining and using such intrinsic information is contrary to their privacy expectations (Smart Card Alliance, 2003).

5.1.7 Updating Software

It is said that social engineers often seek to ascertain whether an organisation is running out-of-date or unpatched software, because such information gives them a window to exploit the system (Granger, 2002). The challenge for the technical experts in charge of running a system is in ensuring that the software is up-to-date, because as Tornikoski (2014) indicates, "your software is like the front door to your PC". If the software is out-of-date, the system is prone to all kinds of attacks. For instance, even banner ads which run on a website could pose a danger to the system because most are built to take advantage of different plug-ins (e.g. flash and Java) in order to access data.

Overall, although technological measures provide the basic infrastructure from which information protection is carried out, there is overwhelming evidence in the literature (Nohlberg, 2008; Granger, 2002; Mitneck & Simon, 2002) that human beings are always the greatest source of risk for information exposure. As such, one can conclude that technological measures alone cannot succeed in curbing social engineering; rather, for relative success to be achieved, organisations would need to combine both technological and human aspects. Specifically, and as discussed below, organisations would need to educate and create awareness among employees regarding the value of the information they have access to, how to protect it, and how to react in cases in which the information is inadvertently exposed.

5.3. Education and Awareness

The literature on social engineering seems to agree about the absence of an overall solution to the problem. Education and awareness is recommended as the most desirable way through which social engineering attack vulnerabilities can be reduced (Mitneck & Simon, 2002; Granger, 2002). It has been argued that an educated and informed population would be knowledgeable about the kinds of attacks that could occur, ways of

detecting such attacks and how to react when an attack is suspected to have occurred (Mitneck & Simon, 2002). One of the biggest lessons in education and awareness is related to letting employees know that no one (not even a fellow employee, but mostly not a remote caller) can be trusted with sensitive information such as passwords.

The weakest link in an organisation (and the most likely target for social engineering attacks) are those employees, managers, or business owners who are unaware of the value of the information contained in the system; people who have special privileges (e.g. system administrators); specific departments who hold potentially valuable information (e.g. human resource, accounting etc); and manufacturers or vendors who supply an organisation with software and hardware (Mitneck & Simon, 2002). It has been found that in most organisations, people have a certain degree of security awareness. However, their knowledge on security matters is often inadequate, and even where it is adequate, it is overshadowed by paranoia, caution, gullibility, and a level of suspicion.

Education and awareness should address a number of issues. According to Nohlberg (2008), corporate policies are the first step about which employees need to be educated. By understanding such policies, employees would be better positioned to understand what is considered right or wrong in an organisation. Next are security issues, which include personal safety and collective organisational safety. Again, understanding security issues would enable employees to understand when they are secure, and when their security is compromised. Employees also need to be educated about their role. According to Nohlberg (2008), understanding one's role enables the employee to know what to do or how to react when something that is out of the ordinary is suspected. Finally, the employees need to be educated about reporting and responding. In general terms, this means that employees need to be empowered with knowledge that would enable them to know how to report a suspected breach in security. Nohlberg (2008) argues that every organisation needs to ask itself if its employees would become suspicious and report, in the appropriate manner and to the right person, an unknown person who enters the office, sits on a computer and starts working on it. If the answer is in the negative, the organisation needs to educate its employees further, because they would easily fall prey to social engineering attacks. In relation to awareness creation, employees need to know: the information that has value (and therefore needs to be protected); that their friends are not necessarily the organisation's friends (hence the need to keep trade secrets secret and sensitive organisational information confidential); that passwords are personal and should

not be shared even with their colleagues at work; and that knowing each other and identifying strangers who have not been introduced to them as co-workers is vital for their own security and for security of the organisation (Nohlberg, 2008).

Granger (2002) further notes that social engineering attacks are conducted either in the physical aspect (e.g. an imposter calls, visits an organisation, or dumps a malware-laden flash drive in a strategic place near the organisation where he or she is almost certain an employee will pick it up and use it in the office); or in the psychological aspect (i.e. friendliness, conformity, ingratiation, impersonation, and persuasion). If employees are to help in the fight against social engineering, it is important for them to understand the form of social attacks that can target them. Additionally, employees need to understand that they should protect themselves even outside the organisational environment. For example, carrying flash drives that have sensitive company information is risky in that the flash drive can be stolen or lost. Additionally, particularly for those who take work home, employees need to be educated that they cannot share their laptops or PCs with their friends. Picked up flash drives (especially those that are unusually marked (e.g. with a mark indicating some strange content inside) should be avoided even in home computers.

As not every employee will abide by everything they are told, organisations also need to put in place security policies which every employee will have to adhere to. According to Granger (2002), organisations need to develop policies that are neither too general nor too specific. This is informed by the idea that policy enforcers (employees) would need some flexibility, but would also need some limits in their daily practices to avoid being too complacent. Overall, it would appear that education and awareness play a critical role in averting or reducing social engineering exposure. It has been argued that the human link is easier to use when seeking to access information as opposed to penetrating a system through hacking. As such, it is important that employees are made to understand the value of the information they hold, the possible attacks that might come their way, the form that such attacks may take, and how and who to report suspected social engineering attacks to. Overall, it can be argued that education empowers people by making them more aware, not only of the physical social engineering attacks, but also about the psychological attacks, which may not seem or even feel like attacks when being executed. The psychological social engineering attacks are manipulative, friendly, and meant to source information from unsuspecting employees without raising eyebrows.

5.4. Cultural Change

As illustrated in the previous Chapter, there exists an information security problem whose solution may lie in a particular cultural environment.

Certain cultural attributes must be changed in order to prevent information sharing and eventually achieve information security. However, the ability to do so involves a long process.

According to Haviland et al. (2010), cultures have always changed over time. Changes take place in response to certain events, such as population growth and technological innovation. Hence, it is possible to change culture after a significant event. Among the triggering events, according to Haviland et al. is technological innovation, such as the growth in use and capability of ICT. They further assert that people growing up in modern industrial and post-industrial societies generally value personal freedom, individuality, and privacy as essential in their pursuit of happiness. Hence, they maintain that valuing privacy is an aspect of post-industrial societies, which is still not common for Arabs at the current stage of their development.

Naylor (1996) argues that changing a culture requires changing the people, their beliefs or behaviours. Determining whether you need to do this is the first step. Legislative accountability is not a particularly useful strategy for changing ideas. Legislating change has been shown to be of limited value in any culture change (Naylor, 1996). Coercion through the promise of punishment will fare no better; experience has shown this generally results in only superficial change. Kotter and Schlesinger (2008) argue that using coercion is a risky process because inevitably people strongly resent forced change.

Although integrating change can be a long and demanding process, it is still possible. Furthermore, the required change is clear and identified, namely, sensitive information sharing. Naylor (1996) maintains that education is perhaps the best defence against resistance to cultural change.

The need for effective user privacy education has been discussed in several respects. For example, Aloul (2012) conducted research on information security in the UAE and came to the conclusion that users should be educated against the risk of information sharing, which can be exploited by social engineering attacks. He also asserts that schools should offer security awareness courses as part of their computer course curriculum.

5.5. Conclusion

Ultimately, a mixture of legislative measures, technological measures, and education and awareness will be needed to reduce the prevalence of social engineering attacks. At present, it would appear that legislative measures are underdeveloped, technological measures are insufficient, and education and awareness is still something that many organisations have not fully ensured their employees are equipped with.

As seen in Chapter 4, lack of awareness and the cultural impact are the main issues for sharing sensitive information among family members and friends.

CHAPTER 6: NATIONAL CYBERSECURITY STRATEGIES: RESPONSE TO PASSWORD SHARING

This chapter describes the background and development of an effective education and awareness approach. Approaches from other countries are analysed to develop a programme which can be adopted in the UAE in order to minimise the risk of sharing sensitive information.

Although many national cybersecurity strategies are developed as a result of earlier national threats and risk assessments, and despite cultural, legal, and political differences among countries, there are some elements within these strategies that can be beneficial for other nations (Luijckx et al, 2013) which do not have their own cybersecurity strategy.

This chapter considers the Gulf Cooperation Council (GCC) countries' initiatives towards cybersecurity and the response to the threat of password sharing. In addition, a critical analysis is conducted on three national cybersecurity strategies of the USA, the UK and Australia in relation to security awareness and education in password sharing. The analysis is centred on the initiatives that target online user security education. The analysis also considers the awareness tools developed in these countries and the possibilities of adopting them to reduce the identified risks found in the UAE.

6.1 Research Strategy

As discussed previously, the cultural nature of the problem dictates that a proposed solution would have to consider the cultural basis. Such a solution would inherently result in resistance to change. However, studies show that education is the best defence against resistance to cultural change (Naylor, 1996) and which can produce effective outcomes (Aloul, 2012).

Furthermore, where the risk of sharing sensitive information in the UAE is identified (e.g. Alkaabi & Maple, 2013; Alkaabi & Maple, 2012; Alarifi et al, 2012) a successful approach to producing effective information security results should consider the causes of risk (Blakley et al, 2001). Identifying the causes of risk can contribute to the design of effective information security strategies (Everett, 2011). National cybersecurity strategies

commonly identify and comprise elements of reducing cybersecurity threats. For example, the national cybersecurity strategy for the UK provides actions to reduce the risks that affect an individual’s personal information resulting in fraud and identity theft on the information security awareness website (www.getsafeonline.org).

Accordingly, this work critically analyses three national cybersecurity strategies of the United Kingdom (UK), the United States (U.S.) and Australia (AUS) in order to identify any information security awareness education designed to educate online users about the risk of sharing sensitive information, including passwords. The GCC countries do not have national cybersecurity strategies but they refer to such practice as computer emergency response team (CERT). The computer emergency responses of the GCC countries are analysed in place of a strategy. The analysis particularly covers elements of the availability of information security programmes recommended by cybersecurity documents.

Due to the password sharing threat found in the UAE, an investigation into password security awareness was conducted to critically analyse and compare the aspects designed by those countries to educate online users about the risk and impact of password sharing and its applicability to the UAE.

Figure 9 shows the hierarchy of the investigation and the applicability to the UAE cybersecurity threats:

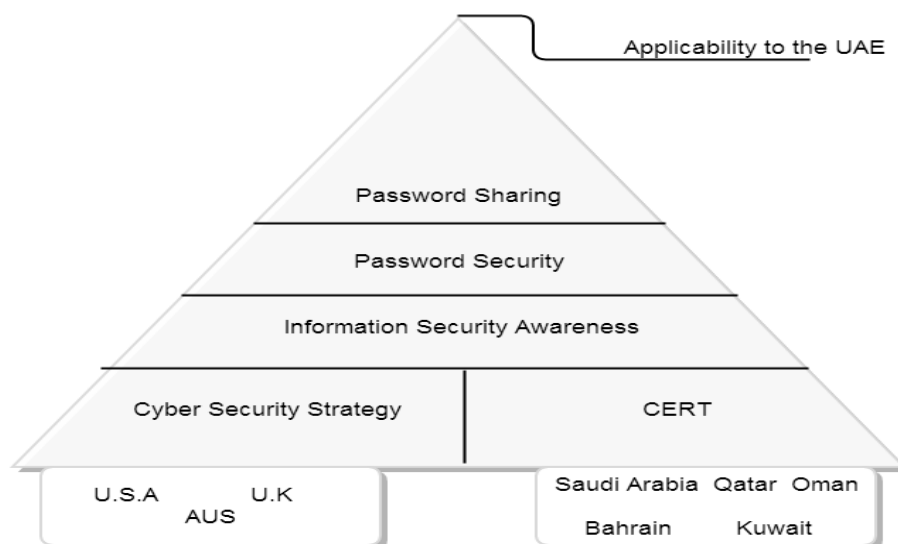


Figure 9: Hierarchy of the investigation and the applicability to the UAE cybersecurity threats

6.2 Information Security Strategy in the GCC

The GCC countries share the same culture of trust that stems from loyalty and religious attributes, which contributes to information security threats (Alkaabi & Maple, 2013). According to a study by Alkaabi & Maple (2013), access login sharing with co-workers and family members is one of the information security awareness issues that need to be dealt with effectively. However, strategic orientation of raising information security awareness is not found in the GCC. The European Union Agency for Network and Information Security (ENISA) has listed all of the National cybersecurity Strategies in the world based on publicly available material. There is no national cybersecurity for any of the GCC countries in the list (National cybersecurity Strategies in the World — ENISA). Furthermore, there is also no national cybersecurity strategy beyond the Computer Emergency Response Team (CERT) for some of the GCC countries according to the United Nation International Security Trends and Realities report (UNIDIR, 2013). Despite the fact that CERT is designed by a country to provide both technical and managerial support for cyber incidents for both organisations and online users, security awareness is often responsibility of the CERT team. It provides limited advice on some security threats for online users rather than the awareness tools recommended by the governmental cybersecurity strategy (for example, the UK and AUS cybersecurity strategies).

Although there is no cybersecurity strategy for the GCC countries, governmental awareness initiatives for each country that aims to raise public information security knowledge and cover the risk found in the inherited culture were considered. Below are the findings for each GCC country:

6.2.1 Saudi Arabia (KSA)

Saudi Arabia has a National Information Security Strategy drafted in 2011. However, information security awareness and education is still a target in the KSA. Furthermore, the Saudi strategy does not include any information security awareness tools similar to those in the UK, AUS and the U.S., which provide citizens with comprehensive knowledge of information security risks (NISS, 2011).

The Saudi CERT (CERT-SA) was established to play a pivotal role in increasing and spreading awareness, knowledge, management, detection, prevention, coordination and to provide responses to information security incidents at the national level.

However, CERT-SA also provides a limited information security awareness programme as it covers a limited scale of security advice. The awareness programme lists some ways for protecting the privacy of the individual in the digital world through sharing sensitive information such as passwords is not mentioned. Similarly, the information awareness programme focuses on the password management structure such as the length, complexity, different passwords for different accounts etc. whilst ignoring the issues password sharing.

6.2.2 Oman

Oman does not have a national cybersecurity strategy but does have some initiatives are related to cybersecurity incident recovery and public security awareness. Due to the necessity of addressing risks and security threats in Oman cyberspace, the government of Oman officially launched Oman CERT (OCERT) in April 2010 (OCERT, 2014). OCERT was developed to build trust between the Omani government and citizens with regards to e-government services. In addition, OCERT provides awareness and training services upon request. This initiative was introduced due to the considerable number of Omani citizens who are unaware of their exposure to security risks. However, there is currently no information security awareness advice on their website or booklet.

6.2.3 Bahrain

There is no cybersecurity strategy for Bahrain and no CERT to provide security awareness to online users. Bahrain is advised to set up a national security strategy to combat cyber threats according news in March 2014 (Middle East Association).

6.2.4 Qatar

Qatar CERT (Q-CERT) was established in December 2005 in cooperation with Carnegie Mellon's Software Engineering Institute. Its mission is centred on providing the nation's information security needs and safeguarding local society (Q-CERT).

National information security centres provide awareness programmes to the audience upon request. However, they do not have a national cybersecurity strategy based on a national risk assessment that aims to raise user awareness in relation to the vulnerability of the human factor. cybersecurity awareness designed by Q-CERT does not provide any security awareness advice.

6.2.5 Kuwait

Kuwait does not have a national cybersecurity strategy or CERT that may provide an

awareness mechanism.

6.2.6 United Arab Emirates (UAE)

The UAE does not have a national cybersecurity strategy. However, the UAE CERT has provided several initiatives to raise public security awareness. In the security awareness domain provided by the CERT website, different environments have been considered such as home and work (aeCERT).

The UAE CERT website also offers several types of material on security awareness such as posters, reminder cards, frequently asked questions and others. Password security is one of the security issues that the UAE is concerned about and is covered in the material. With regard to password sharing, the website provides advice asking citizens not to share passwords with others, while no discussion of the impact of password sharing is provided.

Table 11 below summarises the GCC countries governmental initiatives to cybersecurity:

Table 11: GCC countries governmental initiatives to cybersecurity

Country/ initiatives	Cybersecurity Strategy	CERT		
		Security Awareness Programme	Password Security	Password Sharing
Saudi Arabia	✗	✓	✓	✗
United Arab Emirates	✗	✓	✓	✓
Bahrain	✗	✗	✗	✗
Kuwait	✗	✗	✗	✗
Qatar	✗	✓	✗	✗
Oman	✗	✓	✗	✗

6.3 National cybersecurity Strategies for the U.S., the UK and Australia

6.2.7 United States (U.S.)

Password creation and sharing in the U.S. was considered by Stanton & Stam (2005) in a study of people behaviour and attitude. The study targeted 1,167 end-users in the U.S. investigating their behaviour towards information security. The study revealed that sharing account access with a friend was the most noticeable end-user behaviour. The study also showed that 23% of the respondents sometimes shared their passwords with their work-assigned group, 7% revealed their passwords to colleagues in the company who did not belong to their work group, and 4.1% shared their passwords with people

who did not work for the same company. Stanton et al (2005) assert that considering end user behaviour is one of the success factors for information security compliance. The authors also stated that although password creation and sharing is generally poor across different organisation sectors such as military organisations, telecommunications, and others, improvements to this phenomenon are associated with training, awareness and education.

Another study was conducted by Medlin et al. (2008) in the healthcare field in the U.S. to analyse the vulnerability of hospitals to social engineering attacks. The findings of the study maintained that employees reveal their passwords with co-workers and co-workers' friends. Out of 118 respondents surveyed, 73% of the respondents shared their passwords. Such behaviour is vulnerable to social engineering whereby the trust environment among healthcare staff could be misused to obtain unauthorised access to patient profiles. The threat of social engineering to the medical system has a higher impact than that to, for instance, financial institutions as medical records could be tampered with resulting in life threatening outcomes. The study raised serious concerns about the state of employee security awareness and the necessity of organising initiatives to make employees aware of the risks of information sharing.

The U.S. Health Insurance Portability and Accountability Act (HIPAA) has specific standards related to security and privacy of information to ensure the protection of health care information. HIPAA refers to the security and privacy measures in relationship to Security Management Process, Security Awareness and Training and Access Control. However, the behaviour practiced by healthcare employees in the U.S. clearly violates HIPAA's regulations, which are definitive in terms of patient information privacy (Medlin et al, 2008).

Another study in critical infrastructure sectors in the U.S. by (Moore et al, 2008) targeted the insider threat and the impact of employee practices on IT sabotage. The study revealed several cases of IT misconduct including the sharing of passwords among co-workers. The authors proposed that such behaviour could be reduced through continuous security awareness training and suggested that information security policies should include password management that prohibits password sharing.

President Obama has publically stated that cybersecurity is one of the most serious economic and national security challenges for the U.S. One of the initiatives that the U.S.

aims to achieve is to expand cybersecurity awareness and education from the boardrooms of the U.S. government sector to the classrooms (The White House). According to the International Strategy for Cyberspace (2011) developed by the U.S. government, making the end user aware of cybersecurity threats remains one of the priorities in cyberspace defence (The White House, 2011). The strategy covers different security threats that compromise end user privacy due to the country's acknowledgment that the growth of social networks brings new challenges. As the citizens increasingly engage in Internet resources in their public and private lives, they should be aware of Internet security risks that could lead them to a compromise of their personal data resulting in identity theft and fraud, amongst others. In addition, the strategy recommends building a culture of cybersecurity as this increases knowledge of the cybersecurity risks among citizens.

The cybersecurity strategy for the U.S. does not provide much information about the tools used to increase public information security awareness. However, the National cybersecurity Alliance (NCSA) is responsible for creating and implementing broad-reaching education and awareness efforts to provide users at home, work and in school environments with the best prevention awareness that they need to keep themselves, their organisations, their systems, and their sensitive information safe and secure online and to encourage a culture of cybersecurity. NCSA has developed a website that helps increase public knowledge of cybersecurity. The website, staysafeonline.org, is an education source that aims to provide citizens with knowledge of common threats and the possible ways to protect themselves while they are online. The website covers different protection domains in the information security awareness field, such as personal information, work environment, home and mobile devices, amongst others.

In addition, "Stop. Think. Connect." is a national public security awareness campaign developed by the Department of Homeland Security in cooperation with the National cybersecurity Alliance (Stop.Think.Connect). This campaign provides all the tools to host a classroom discussion or community meeting on online safety including advice and suggestions to stay safe online.

Password sharing with friends and employees is covered on these websites which clearly states "*never share your password with any one*", and this applies to work and home, adults and young people. The awareness websites advise citizens to keep their social security numbers, account numbers, passwords, and other personal details private and never share them with others. The advice on passwords includes making them complex

and changing them regularly (Stop.Think.Connect). However, according to major cases which have recently affected U.S. national security (discussed below), U.S. citizens are still willing to share their access login details with friends and co-workers.

According to the 2011 U.S. Verizon Data Breach Report, The spread of insider threats taking place as a result of password sharing has led to security breaches. Trusted insiders, including those who have access to sensitive information, usually steal larger quantities of information. The Data Breach Report also indicated that the actual number of incidents that occurred as a result of an insider threat almost doubled in 2010 (SANS, 2012).

Similarly, the information available on the WikiLeaks websites comes from sensitive information sharing amongst insiders. The WikiLeaks cables were initiated from the misuse of system privileges by employees within governments, and companies from where the data are stolen (Verdasys, 2011). Edward Snowden, the former U.S. NSA contractor, obtained several login access details from employees working at NSA (Reuters). Snowden successfully used a social engineering attack to trick between 20 and 25 fellow workers at the NSA regional operations centre into giving their passwords to allow access to classified information, which he later leaked to the media. Most interestingly, NSA was not clear what regulations the employees had broken by giving Snowden their password login details which allowed him to access classified data.

6.2.8 United Kingdom (UK)

According to the UK's largest NHS trust, password sharing has been discovered in 70,000 cases of "unauthorised access" to IT systems, including medical records (Computer Weekly). This forms a risk to the security of patient data. For example, in 2008, password sharing discovered in an X-ray system at a hospital in Devon, made it difficult to identify which doctor wrongly authorised a treatment for a patient who died after a mistake (Ritter, 2008).

However, NHS doctors say that sharing login access is a normal practice which provides staff with flexibility to perform their job more easily.

The NHS trust criticises this phenomenon and aims to introduce a new security policy that ensures proper control over login access to NHS trust systems and data (Computer Weekly).

The UK cybersecurity strategy 2011 considers information security awareness of citizens as one of its main goals to meet the 2015 vision of the UK cybersecurity space.

Prevention of identity theft and fraud attacks has been introduced within the information security awareness tool provided in the website Get Safe Online www.getsafeonline.org. The strategy also aims to improve cybersecurity education at all levels in order that UK citizens are well-equipped to use cyberspace safely.

6.2.9 Australia (AUS)

According to a study conducted in Australia by Singh et al (2007) investigating online banking and security rules, password sharing among family members does not meet the Australian government cybersecurity goals. The study showed that password sharing occurs due to the high trust within family relationships. The study also found that people with disabilities, who may need the help of others to carry out online banking, share their online private access. Singh et al (2007) recommended that social and cultural practices should be taken into account while performing information security design. They suggested that ignoring these two elements may lead to more violations of the information security policy.

It is easier for a hacker to obtain user access credentials if the hacker knows the security environment and the user behaviour in an Australian community. Hackers prefer simple sensitive information that may be available, especially in a high trust environment, in order to perform their social engineering attacks and obtain such information (Singh et al, 2006). Identity theft is a well-known social engineering attack; this kind of attack works on user behaviour to steal access credentials. Australia's Internet banking system has been targeted by such attacks since early 2003 (McCombie & Pieprzyk, 2010). These attacks have resulted in the stealing of victims' personal identity data and financial account credentials.

Although the Australian cybersecurity Strategy 2009 stresses the information security fundamentals CIA (Availability, Integrity, Confidentiality) while communicating across the country, social engineering attacks and other privacy attacks have been a serious concern in Australia's cybersecurity strategy. The strategy also maintains in its design that all Australians should be aware of the cybersecurity risks and impact, and should protect their personal information from being compromised by identity theft attacks.

Information security awareness is a strategic priority for the Australian government. This approach focuses on providing confidence and practical tools for citizens to protect themselves while operating in a cyber-environment. The strategic approach involves

educating online users on the safe ways to use cyber services and introduce the Australian people to the associated risks of falling victim to fraud or other attacks. The strategy also states that awareness is an ongoing programme, organised in partnership with businesses, consumer groups and community organisations, to educate online users on updated security risks and threat mitigations.

The Australian cybersecurity Strategy 2009 recommends changing cybersecurity behaviour. This has been discussed extensively in terms of cultural change to create a safe environment for all Australian ICT users. Maintaining such a culture can be achieved through education and awareness. In addition, the Australian Government Ministry of Defence maintains that human behaviour plays a significant role in information security and when looking at this factor consideration needs to be given to the organisational culture, individual differences and personality traits (Parsons et al, 2010).

To reach the target of promoting a culture of cybersecurity, the government has developed a single authoritative website for cybersecurity information for Australian home users and small businesses (<http://www.staysmartonline.gov.au>).

Although the Australian cybersecurity Strategy 2009 states “Never share your password with anyone”, a study of Australian attitudes toward password use and management shows that nearly 42% of Australians have shared their passwords with a friend, family member or work colleague (CIS, 2011). This sharing phenomenon has caused significant breaches to information security in Australia. According to SANS password sharing report (2012), in January 2011, Vodafone fired employees in Australia for misusing a privileged password or providing it to criminals, causing a breach to the database where sensitive customer information was stored.

In conclusion, Australian online users are still willing to share their online access details with family members and friends despite the strategic initiatives to reduce online identity theft and raising user privacy awareness. Changing culture is another cybersecurity strategy that the Australian government is targeting. However, promoting a culture of cybersecurity among Australians is different from analysing online user behaviour and attitudes. This could potentially be related to the Australian culture of, and the social attitudes towards, information security. It is evident that information security culture differs from the impact of culture on information security (Glaser, 2009).

6.4 Analysis and Discussion

The cybersecurity strategies detailed above consider end user awareness and education in their security design. Accordingly, the countries have developed some awareness tools (websites). These websites contain different awareness domains such as home, work environment and others. The aim of these awareness websites is to expand security best practice and make users aware of the security threats in cyberspace. Although the UAE does not have a national cybersecurity strategy, CERT.ae provides similar security awareness tools including password sharing awareness (Figure 10). However, the problem still exists despite the dissemination of information security awareness regarding password sharing.

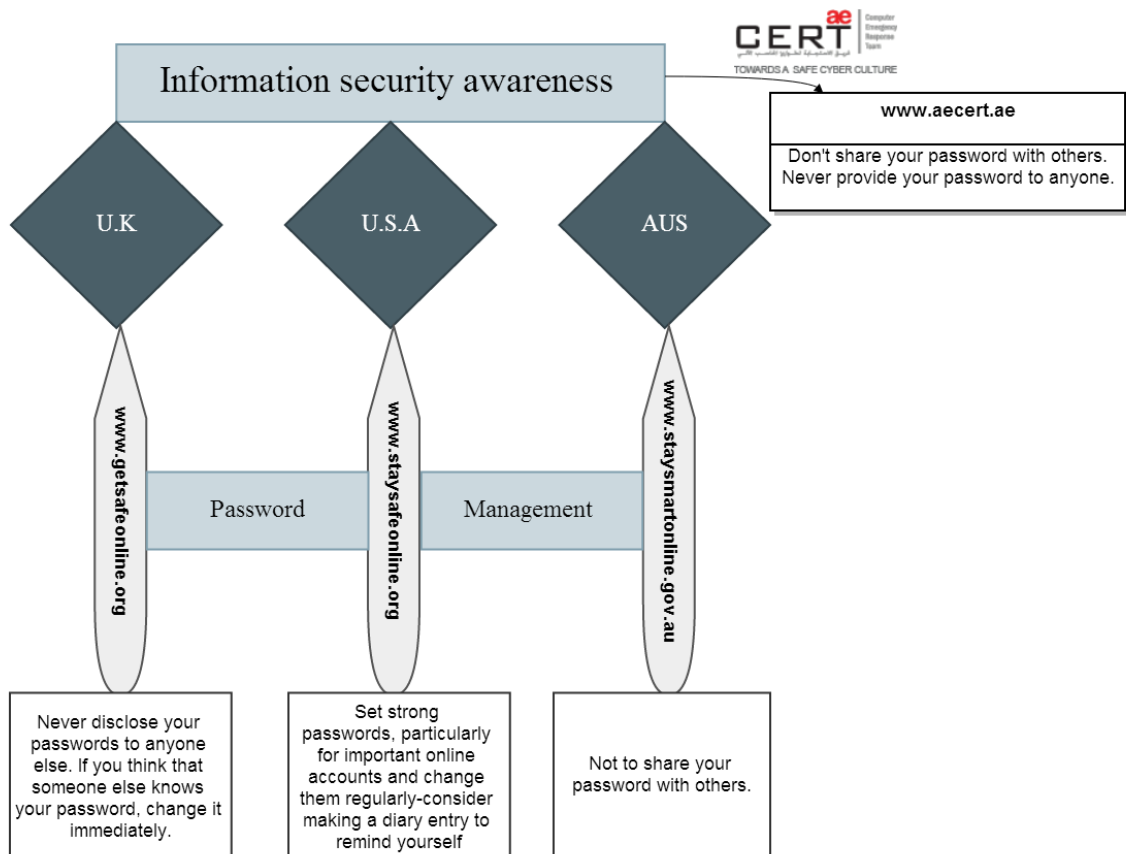


Figure 10: The strategic responses of the UK, the U.S. and Australia to sharing sensitive information compared to the UAE's CERT

The awareness websites provided by the U.S., the UK and Australia contain some education initiatives for several security threats in the password security domain. For example, the strategies maintain the importance of the selection of the password and the risk of choosing a weak password. However, sharing passwords with others is stated only as advice (as shown in Figure 6) without going into the details of the risk associated with

sharing passwords and the impact on both individuals and organisations.

The possibility of adopting awareness advice without educating users will not make any significant difference to cybersecurity threats in the UAE, as CERT.ae provides similar advice without educating online users on the risk and the impact of this activity. Moreover, it is advisable that the U.S., the UK and Australia should enhance their awareness tools by providing education on sharing sensitive information including passwords.

While information security awareness, training and education play a significant role in raising the knowledge of information security, there is a clear difference between awareness, training and education (Layton, 2006). Awareness is developed to be delivered to all users and tends to focus on global security principles whereas training targets a specific group to deliver knowledge of a specific topic with an expected outcome. Education plays a great role in theory and research by answering the question “why” and provides concepts in order to develop new skills and alter outcomes in some way (Layton, 2006).

Generally speaking, information security awareness alone is insufficient as an element to reduce the impact of user behaviour on information security. Education on the other hand plays a significant role in creating knowledge by educating users on specific information security issues (McCoy et al, 2004). Education helps in changing people’s behaviour and will keep users aware of any new issues related to the taught subjects (Thomson et al, 1998). Simply making end users listen to advice on not practicing behaviour against the information security policy will prove ineffective. Rather, organisations must further approach information security awareness programmes by strengthening education in security behaviour modification (Rhee, 2009).

The awareness tools provided by the above countries should consider the education of password sharing. Therefore, education should be designed to show the risk and impact of sharing passwords on both organisations and individuals.

6.5 Conclusion

Countries have different priorities regarding raising awareness to sensitive information sharing. However, wider and significant security education about sharing passwords is required.

In the U.S., advising the end user not to share their access control with anyone is not

enough. Instead, educating the end user about the risks and impacts of sharing sensitive information in all environments (home, work, school, etc.) is necessary for national security.

Although sensitive information sharing happens in the UK it is on a smaller scale than the GCC countries. The UK cybersecurity strategy 2011 may also need to consider the sharing preferences of citizens.

The Australian cybersecurity strategy 2009 should focus on the design of security awareness tools and consider the sharing of sensitive information among family members and friends in both home and work environments. Strategy makers should also investigate the sharing phenomenon and how it is related to the cultural norms, behaviour, attitudes and trust.

As education contributes greatly to the change of end user behaviour, national security strategies should consider education as a strategy for reducing the impact of human behaviour on information security with regard to sensitive information sharing.

Finally, the information security risks found in the UAE should be dealt with strategically in order to provide an information security education that reduces the cultural impact of password sharing.

CHAPTER 7: STRATEGIC INFORMATION SHARING SECURITY FRAMEWORK

This chapter introduces an education strategy programme that models the needs of UAE's organisational requirements in securing their information security. This strategy is to be implemented in the long-term by targeting the younger generation and starting with school students.

As discussed in the previous chapter, awareness in itself may not achieve the required result of reducing the amount of password sharing among family members and friends. Rather, computer users should be educated about the risks in order to change their behaviours and attitude. This chapter provides a case study implemented in Abu Dhabi schools to test the efficacy of the education programme and the study will contribute to the design of a framework for information security education.

The need for effective user privacy education has been discussed by several authors. For example, Aloul (2012) conducted research on information security practices in the UAE and came to the conclusion that users should be educated about the risks of information sharing through social engineering attacks. Aloul (2012) also asserts that schools should offer security awareness courses as part of their computer course curriculum.

The intervention study proposes a strategy designed to provide information security education for the younger generation and the possibility to mitigate the risk of sharing sensitive information.

7.1 The Intervention Study: Information Security Awareness Education

Information security is based on risk management. A successful approach to information security should thus consider the causes of risk (Blakley et al, 2001). While risk management is a core element for any security strategy, it is very important to educate users on the associated threats and the inherited risks of their actions (Everett, 2011).

Several studies (for example Alarifi et al, 2012 and Alkaabi & Maple, 2013) have been conducted in Arab countries regarding online users' perceptions to awareness of information security. These studies have shown some social vulnerability in information

security systems with causes deeply rooted in Arab culture. Sharing security control credentials such as passwords or other sensitive information among family members and friends is something that is not unusual in Arab culture.

The most obvious potential threat that takes advantage of information security controls is social engineering. Social engineering techniques obtain information by exploiting human behaviours, rather than technical vulnerabilities. Many studies in the literature have recorded the spread of social engineering and the huge destruction that results from this form of attack (Ferreira et al, 2010).

The current study argues that school education can patch this social vulnerability as long as it is targeted appropriately, and acknowledges nuances of culture, in this case Arab culture. The study proposes a strategy designed to provide information security education for the younger generation with the aim of reducing the likelihood of sharing sensitive information. The solution proposed is based on the root causes of sensitive information sharing: the cultural impact and the lack of information security awareness (Alkaabi & Maple, 2013).

The figure below (Figure 7) depicts the proposed strategy that is based on the social risk of sharing sensitive information with family members and friends:

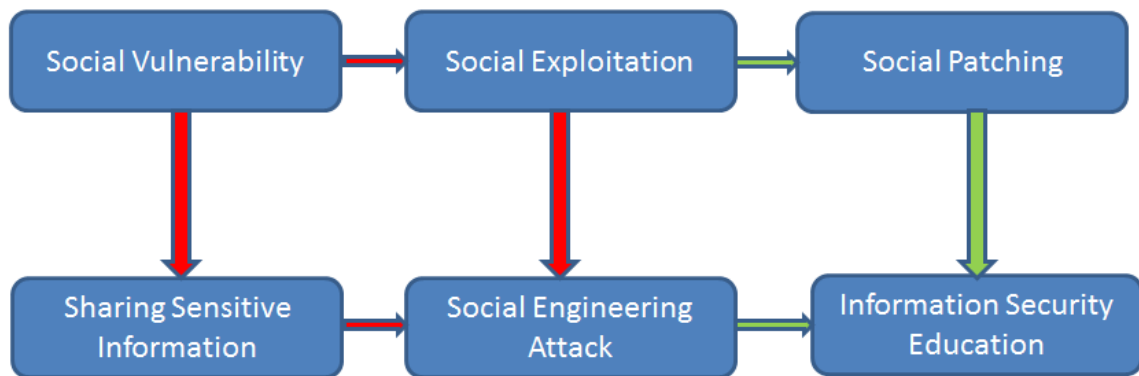


Figure 11: The proposed strategy

Figure 11 shows that sharing sensitive information among others is a social vulnerability. This social vulnerability could potentially be exploited using the social engineering attack. The proposed strategy (with the green arrow) is aimed at patching this social vulnerability through the information security education programme.

A strategy should be developed, for private information sharing in Arab culture, which aims to reduce overall information security risks. Two aspects had been taken into

consideration while designing the intervention study:

- The education programme
- The structured approach

7.1.1 The Education Programme

The education programme (Appendix 5) should be designed to cover the following aspects:

- *Differentiation between private and other information:* This focuses on distinguishing between the different natures of information. The individual should be aware of this before exposing sensitive information to others. It also covers other information that is allowed to be shared in order to communicate with others over the Internet.
- *The potential risk posed by sensitive information sharing:* This element focuses on the risk that might occur from sharing sensitive information. Such risks might be, for example, an outcome of matters such as accessing others' accounts, knowing account passwords and accessing unauthorised accounts by using the same shared passwords of other authorised accounts. Unauthorised access may cause severe consequences to confidentiality, integrity and availability.
- *The impact of the risk as a result of the sharing phenomenon:* This shows the consequences that might occur from sharing sensitive information with others such as identity theft, unauthorised access, and personal information disclosure.

The above aspects were discussed with computer teachers in schools (under the mandate of Abu Dhabi Educational Council ADEC) in Abu Dhabi before running the course. The discussions set the basis for the educational material that covered common aspects that may lead to compromising digital authentication as a result of the information sharing phenomena.

Therefore, the course material (Appendix 5) was designed to help students identify the risks of sharing sensitive information while using Internet services. Furthermore, the course material covered the differentiation between sensitive information that is commonly prohibited to be disclosed and information that is commonly permitted to be shared.

7.1.2 The Structured Approach

In order to design and implement an effective information security strategy we must

acknowledge the reaction of school children to the information security education programme and how much this can contribute to building the required strategy for Abu Dhabi Emirate.

Implementing an information security awareness programme does not automatically guarantee that all employees understand their role in ensuring the security and safeguarding of information and information assets. In order for security awareness programmes to add value to an organisation, and at the same time make a contribution to the field of information security, it is necessary to follow a structured approach to study and measure its effect (Kruger et al, 2011).

The study followed two approaches (quantitative and qualitative) to measure the awareness of social engineering attacks and the potential information sharing that leads to compromise of the digital authentication. Accordingly, two types of surveys were designed to gauge the students' sharing preferences before and after the training programme took place.

The first survey proposed for implementation used Likert scales as pre and post assessments of security awareness of the student groups under research. The use of Likert scales to assess school student has proven useful in different occasions. Benson et al. (2011) used Likert scale questions to assess the effectiveness of courses given to school on the basis of a post-course survey. Pornari & Wood (2010) used Likert scale questionnaire to investigate the relationship between cognitive mechanisms, applied by people to rationalise and justify harmful acts and engagement in traditional peer and cyber aggression among school children. Kubiatico & Haláková (2009) researched the differences between gender and age according to computer attitudes. They used a Likert scale questionnaire with 518 of all grade (first, second, third and fourth) students from 9 high schools in Slovakia. Their research concluded that younger students had more positive attitudes towards ICT.

The conducted questionnaire was based on a series of test-like questions before and after a teaching course was given. The teaching material used lessons and interactive software on privacy as an aspect of information security. A sample of 1200 students divided into age groups (11-17) and sex groups were considered in the target schools. The respondents were equally divided between genders and with the following age groups:

- Less than 11 (20%) from each gender

- Between 11 and 13 (20%) from each gender
- Between 13 and 15 (20%) from each gender
- Between 15 and 17 (20%) from each gender
- Over 17 (20%) from each gender

The questionnaire used Likert-scale measures and 1071 responses were collected in December 2012. Shortly after the responses were collected, taught material was given to the students (1200) with the aim of raising the students' awareness of information security risks.

In February 2013, the second stage of the assessment targeted the experiment group (given the taught material) of 500 students of both genders of the initial 1200 respondents, based on the same percentages as above for every age group. The approach used Yes/No questions with the reason of the choice, and for the aim of assessing their security awareness. There were 450 responses collected.

In April 2013, the questionnaire was distributed to a group (control group) of respondents who had not been given the taught material. This step was been done to analyse the impact of teaching on students by the comparing the result obtained from the taught group and that from the non-taught group. There were 460 responses collected.

In May 2013 the initial group of 1200 students were assessed using the Likert-scale measure in order to critically analyse the difference between the two assessments. There were 1053 responses collected.

The methods also included using a questionnaire based on yes/no type answers in order to evaluate the gained knowledge after teaching. The answers required the students to explain why they chose either answer to each question. "Yes" and "no" options were given to each question with space for writing the reason(s) for the choice. This type of questionnaire is popular in the literature with young age respondents due to its simplicity as well as its ability to extract qualitative data from the provided explanations. Examples of its use with school students are numerous in the literature. For example, Imura & Kimizuka (2011) undertook research to measure communication awareness and understanding in English of Japanese international students and used yes/no type questionnaires. Tuna et al. (2011) used yes/no questionnaires in some schools in Istanbul to measure students' knowledge about climate change. In a similar manner, the Adolescent Depression Awareness Program (ADAP) in used yes/no type questions to

measure awareness of depression in U.S. schools. Wu et al (2010) used yes/no questionnaires to measure awareness of college students about copyright laws. Maftoon & Soroush S. (2010) utilised the analysis of social practices to raise critical language awareness in EFL writing courses. They also used yes/no questionnaires to measure the awareness levels after conducting the course.

The yes/no survey used two groups of 500 students each. The first group (experiment group) was given taught material on information security threats and precautions measures. The other group (control group) was not given the material.

7.2 Quantitative Study

7.2.1 Method: Likert Scale Questions

The method used a collection of taught material and interactive software to educate students on information security. There was a series of surveys conducted with a sample of students divided into age (11-17 years old) and sex groups. The sample considered 1200 respondents to a questionnaire in target schools.

The students were provided with a set of questions examining different aspects of security awareness. The students were evenly distributed over age groups and gender. The answers were based on five-point Likert scales from 1 “Strongly Agree” to 5 “Strongly Disagree”. There were five age groups examined covering different levels and classes. These are depicted in the following tables:

Table 12: Likert Scales

Code	Answer
1	Strongly Agree
2	Agree
3	Neutral
4	Disagree
5	Strongly Disagree

Table 13: Age Groups

Code	Age Group
1	Less than 11
2	Between 11 and 13
3	Between 13 and 15
4	Between 15 and 17
5	Over 17

The survey used pre and post teaching assessments. The students were initially assessed prior to being introduced to any teaching material. The questions (Appendix 3) covered different areas of information security awareness that include: sharing sensitive information including passwords to personal and school accounts, giving access to personal electronic devices such as a personal computer and mobile phone, revealing some sensitive information that would threaten the confidentiality of information to friends and family members, and so on. A list of the evaluated aspects is provided in Table 14. The first two statements are questions about the age group and gender.

Table 14: Information security areas covered by the questions and their codes

Code	Description
1	Age Group
2	Gender
Q3	Access to a personal computer
Q4	Personal Email Password
Q5	Confidential school information, such as registration details, former school records, etc.
Q6	Current location, such as updates on social media websites
Q7	School-related documents, such as transcripts, marks, performance, etc.
Q8	Personal mobile password
Q9	Access to your school computer
Q10	Past school-related information, such as previous school marks, performance, etc.
Q11	Social media password (Facebook, Twitter)
Q12	Personal email content
Q13	Access to personal mobile phone
Q14	Access to personal USB Flash memory drive
Q15	Access to other personal mobile devices (laptop, tablet, PDA, etc.)

As seen in the above table, the information security awareness statements aim to assess how much the respondents may share or provide information about their personal and school matters, which is believed to be sensitive and may lead to security threats.

7.2.2 Initial Assessment

In the initial assessment, the material had not yet been given to the students. In December 2012, 1200 students were asked to complete an online questionnaire available exclusively

for them. The students answered a set of questions evaluating security awareness as detailed above. 1071 respondents participated in the survey out of the sample of 1200 students (out of 859.224 school students in the UAE according to the UAE Statistics Centre (Report Details, 2013)), distributed among genders and age groups. The results of the initial assessment organised in an age/gender matrix are shown in Table 15:

Table 15: Results of the initial assessment organised in age and gender

	Age Groups				
	1	2	3	4	5
Male	114 (50.89%) (21.35%)	103 (49.05%) (19.29%)	104 (49.29%) (19.48%)	112 (50.91%) (20.97%)	101 (49.03%) (18.91%)
Female	110 (49.11%) (20.48%)	107 (50.95%) (19.93%)	107 (50.71%) (19.93%)	108 (49.09%) (20.11%)	105 (50.97%) (19.55%)
Total per age group	224 (20.92%)	210 (19.61%)	211 (19.70%)	220 (20.54%)	206 (19.23%)
Total	1071				

The results of the answers to individual questions are colour-coded in Figure 12 below.

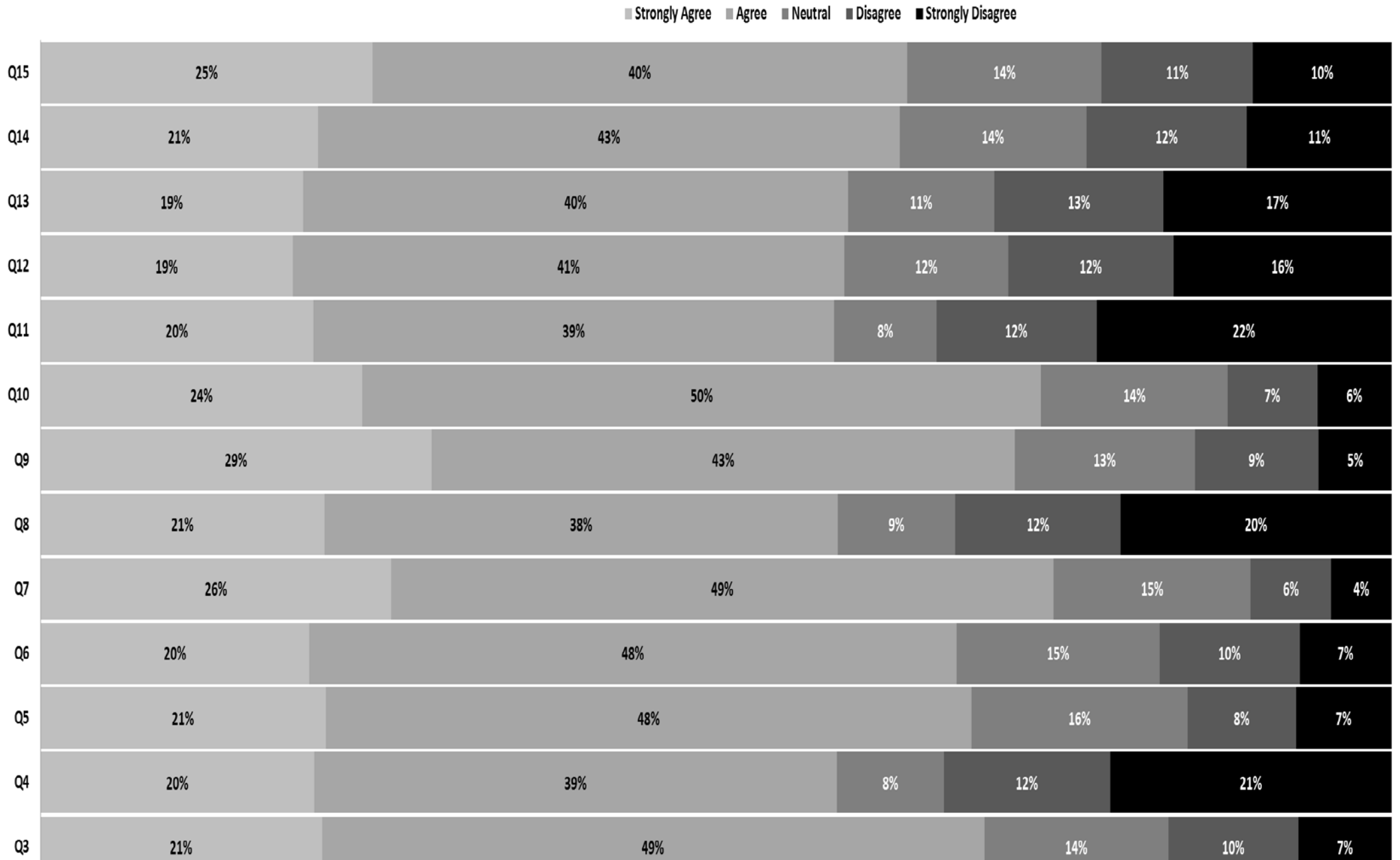


Figure 12: Results of the initial test in a colour-coded diagram

As the legend to the right of the diagram shows, the light colours represent agreement with the statements. Each horizontal bar reflects the answers to each statement (from 3 to 15. 1 and 2 are the gender and age group). It can be seen at a glance that the light colours occupy most of the area of the diagram, reflecting more willingness to share sensitive information under the given circumstances.

The details of the results are shown in the table below:

Table 16: Results of the initial test

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q15	263 (24.56%)	424 (39.59%)	154 (14.38%)	120 (11.2%)	110 (10.27%)
Q14	220 (20.54%)	461 (43.04%)	148 (13.82%)	127 (11.86%)	115 (10.74%)
Q13	208 (19.42%)	432 (40.34%)	116 (10.83%)	134 (12.51%)	181 (16.9%)
Q12	200 (18.67%)	437 (40.8%)	130 (12.14%)	131 (12.23%)	173 (16.15%)
Q11	216 (20.17%)	413 (38.56%)	81 (7.56%)	127 (11.86%)	234 (21.85%)
Q10	255 (23.81%)	538 (50.23%)	148 (13.82%)	71 (6.63%)	59 (5.51%)
Q9	310 (28.94%)	462 (43.14%)	143 (13.35%)	98 (9.15%)	58 (5.42%)
Q8	225 (21.01%)	407 (38%)	93 (8.68%)	131 (12.23%)	215 (20.07%)
Q7	278 (25.96%)	525 (49.02%)	156 (14.57%)	64 (5.98%)	48 (4.48%)
Q6	213 (19.89%)	513 (47.9%)	161 (15.03%)	111 (10.36%)	73 (6.82%)
Q5	226 (21.1%)	512 (47.81%)	171 (15.97%)	86 (8.03%)	76 (7.1%)
Q4	217 (20.26%)	414 (38.66%)	85 (7.94%)	132 (12.32%)	223 (20.82%)
Q3	223 (20.82%)	525 (49.02%)	146 (13.63%)	103 (9.62%)	74 (6.91%)

7.2.3 Post-teaching Assessment

According to the intervention criteria, it is necessary to acknowledge the school children's behaviour towards a course aimed at raising information security awareness in Abu Dhabi Emirate. Knowing that such information, if shared, may lead to security breaches, which may threaten the individual, the solution suggested was to educate the students about the outcomes of the actions of sharing sensitive information. The teaching material was discussed with the teaching team in Abu Dhabi, aimed at covering the above aspects. Accordingly, material was designed aimed at helping the student to identify the risk of sharing sensitive information while using digital devices. In addition, the course material covered the differentiation between the sensitive information that is prohibited from being shared and other information that is permitted to be shared.

Shortly after the responses were collected, the taught material was introduced to the students (1200). The students were taught over the period from December 2012 to June 2013. In May 2013 (still the teaching programme was running) the initial group of 1200

students were reassessed using the same questionnaire. 1053 responses were collected. The answers organised in an age/gender matrix are shown in Table 17:

Table 17: Results of the second assessment organised in age and gender

	Age Groups				
	1	2	3	4	5
Male	101 (48.10%) (19.24%)	96 (45.71%) (18.29%)	116 (53.70%) (22.10%)	100 (49.26%) (19.05%)	112 (52.34%) (21.33%)
Female	109 (51.90%) (20.64%)	114 (54.29%) (21.59%)	100 (46.30%) (18.94%)	103 (50.74%) (19.51%)	102 (47.66%) (19.32%)
Total per age group	210 (19.94%)	210 (19.94%)	216 (20.51%)	203 (19.28%)	214 (20.32%)
Total	1053				

The results obtained are depicted in the following colour code diagram (Figure 13):

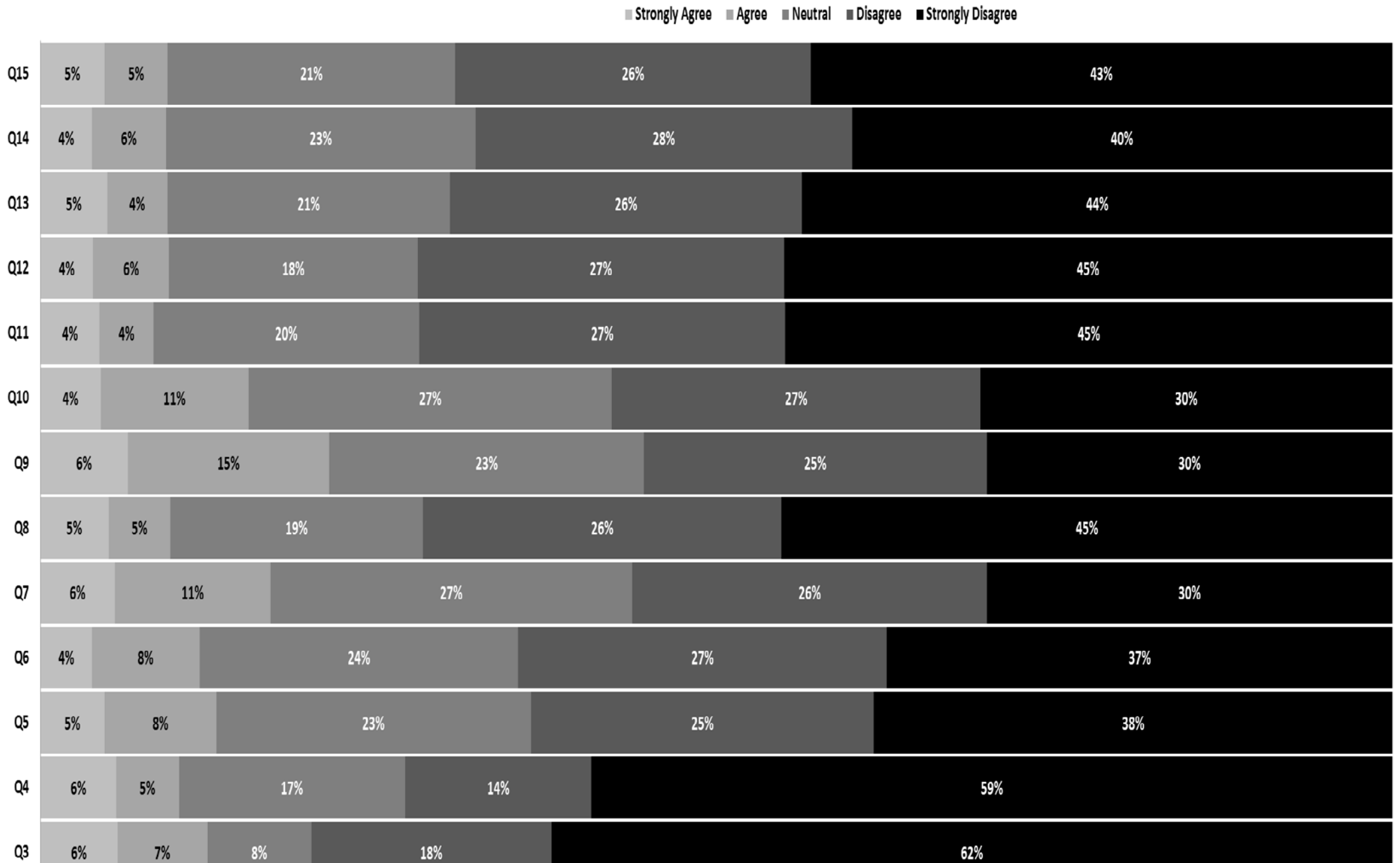


Figure 13: Results of the second test in a colour-coded diagram

The above diagram shows, as a percentage, the ranks of the answers to each question. The dark-colour shaded areas show disagreement with the given statements. The light-colour shaded areas represent agreement with the statements. At a glance, it can be seen that the dark shaded areas occupy more space in the diagram than the light shaded areas. This represents a higher general disagreement with the given statements in comparison to the results of the survey conducted prior to teaching, and hence more information security awareness learnt by the students.

The details of the results are shown in the table below:

Table 18: Results of the second test

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q15	50 (4.75%)	49 (4.65%)	224 (21.27%)	277 (26.31%)	453 (43.02%)
Q14	40 (3.8%)	58 (5.51%)	241 (22.89%)	293 (27.83%)	421 (39.98%)
Q13	52 (4.94%)	47 (4.46%)	220 (20.89%)	274 (26.02%)	460 (43.68%)
Q12	41 (3.89%)	59 (5.6%)	194 (18.42%)	285 (27.07%)	474 (45.01%)
Q11	46 (4.37%)	42 (3.99%)	207 (19.66%)	285 (27.07%)	473 (44.92%)
Q10	47 (4.46%)	115 (10.92%)	283 (26.88%)	287 (27.26%)	321 (30.48%)
Q9	68 (6.46%)	157 (14.91%)	245 (23.27%)	267 (25.36%)	316 (30.01%)
Q8	53 (5.03%)	48 (4.56%)	197 (18.71%)	279 (26.5%)	476 (45.2%)
Q7	58 (5.51%)	121 (11.49%)	282 (26.78%)	276 (26.21%)	316 (30.01%)
Q6	40 (3.8%)	84 (7.98%)	248 (23.55%)	287 (27.26%)	394 (37.42%)
Q5	50 (4.75%)	87 (8.26%)	245 (23.27%)	267 (25.36%)	404 (38.37%)
Q4	59 (5.6%)	49 (4.65%)	176 (16.71%)	145 (13.77%)	624 (59.26%)
Q3	60 (5.7%)	70 (6.65%)	81 (7.69%)	187 (17.76%)	655 (62.2%)

7.2.4 Results and analysis

The two diagrams are shown next to one another in Figure 14.

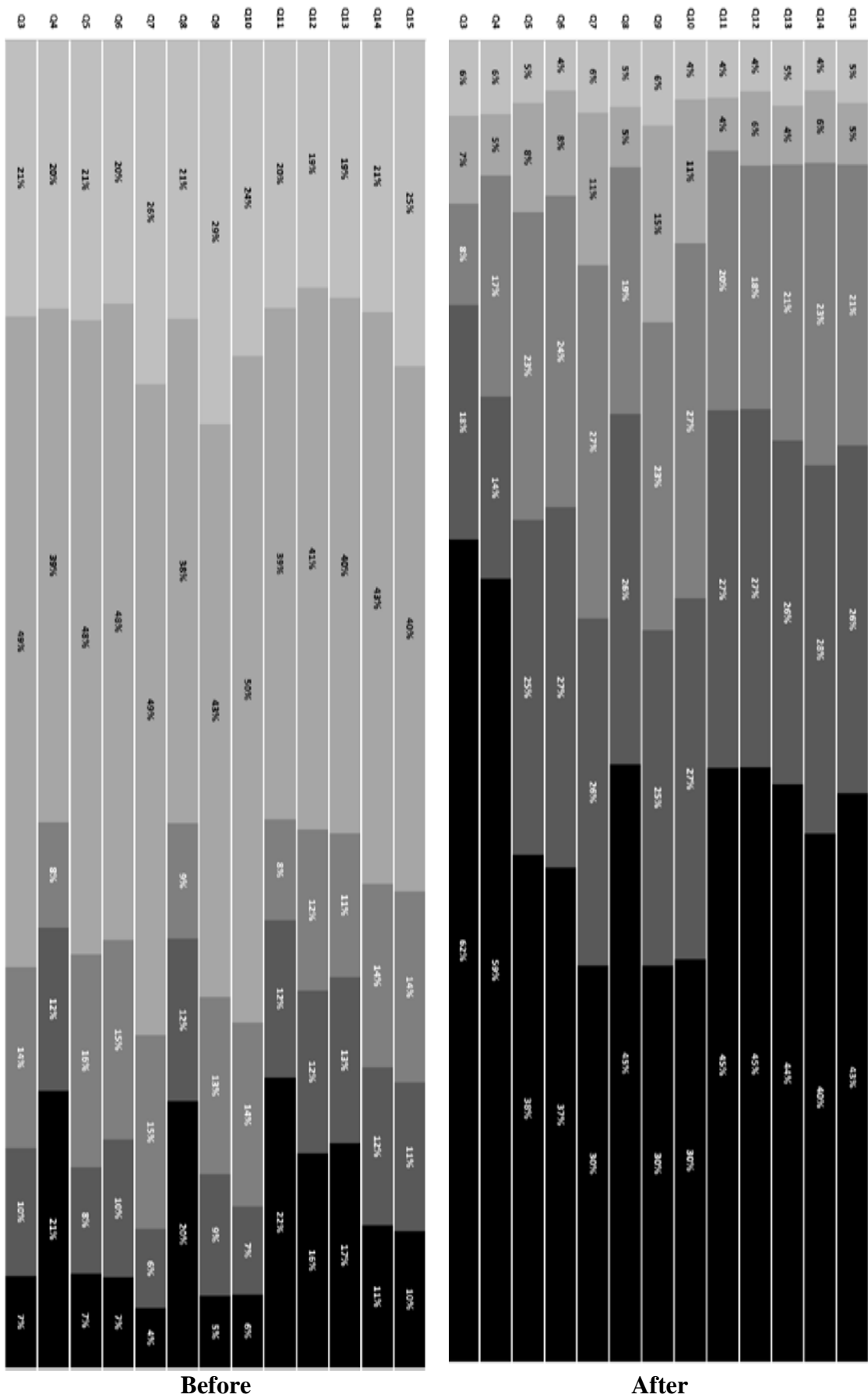


Figure 14: Results and analysis

As can be seen in Figure 14 above, the dark shaded areas occupy more space in the post assessment, implying that students became more aware of the risks of sharing certain information which are typically believed to yield security threats.

To verify that the results were not due to chance, statistical testing was used on the results. Due to the sensitivity of the information collected and the anonymity of the survey, comparison of individual students in the pre- and post- tests was avoided. Therefore, there was no way to pair individual students of the pre-test to themselves in the post-test. Therefore, the results of the pre-test and post-test were considered as two independent samples, although they are not. Although this method may result in the loss of some information (for example individual awareness improvement), it is common for it to be used in similar situations (Fallan, 1999; Reymond et al, 2005; Wonnacott & Wonnacott, 1990).As earlier the non-parametric Mann-Whitney U test was used to compare students’ rankings of information sharing.

Essentially, the Mann-Whitney U test was conducted to evaluate whether the learning offered to students elicits a statistically significant change in the understanding of information security among taught students. The hypothesis is stated below:

H₀: There is no significant difference in the group before and after learning

The questions in the pre-teaching assessment were compared to those of the post-teaching assessment.

The Mann-Whitney U test supports the same conclusion. The test results indicate an improvement in security awareness by students, as more students chose to share less information on the aspects exhibited by the questions.

The result of the test for each question is shown in Table 19:

Table 19: The Mann-Whitney U Test

Null Hypothesis	Test	Sig.	Decision
The distribution of Q3 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q4 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q5 is the same across categories	Independent-	.000	Reject the

Null Hypothesis	Test	Sig.	Decision
of Group	Samples Mann-Whitney U Test		null hypothesis
The distribution of Q6 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q7 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q8 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q9 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q10 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q11 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q12 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q13 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q14 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis
The distribution of Q15 is the same across categories of Group	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis

Asymptotic significances are displayed. The significance level is .05 ((Hair et al, 2010)

As shown in Table 19, the Mann-Whitney U statistics resulted in a significant difference in the group before and after the taught material was introduced in every question. The

test indicated a significant difference ($p < 0.05$) for each question between students' willingness to share sensitive information before and after the learning programme took place (or taken as two independent sample groups). The results strongly suggest that the education programme offered to students over the indicated period had contributed to creating more awareness of information sharing with others, especially relatives and friends, which are common in Arab culture (Al-Kaabi & Maple, 2012).

7.3 Qualitative Study

7.3.1 Questionnaire Design

The questionnaire's design is similar to that of the quantitative questionnaire with the difference that, in some of the scenarios given to the students, the students were required to provide the reasons for their preferences of sharing (see Appendix 4). There were 20 questions representing 20 scenarios designed to cover four classes, namely, Password Sharing, Device/Account Access Sharing, Personal/Confidential Information Sharing and Others. The questions (scenarios) are as follows:

7.3.1.1 Password Sharing

Question no	Scenario
4	Would you share your email password with a friend?
11	If there is an urgent matter, would you give your password to a trusted person to access your computer?
14	Would you give your email password to a person you trust?
15	In case you shared your account password with someone, will you change it later on?
18	Do you have your password(s) written somewhere?
19	Have you ever given your password of any account to someone?
22	Do you share any instant messenger's passwords with others?

7.3.1.2 Device/Account Access Sharing

Question no	Scenario
7	Would you allow access to your personal computer that contains sensitive information to a friend or relative if requested?
8	Would you allow access to your phone to a friend or relative if requested?
13	Would you give access to your Facebook to a person you trust?
17	Would you lend your USB flash memory to a friend if requested without checking whether it has sensitive information stored?

7.3.1.3 Personal/Confidential Information Sharing

Question no	Scenario
3	May all information be shared with friends and relatives?
5	Would you share your email content with a friend if requested?
6	Would you share your sensitive information with a friend that you met in social media website (i.e. Facebook, twitter, chatting website)?
9	Can there be serious consequences of sharing sensitive information with others?
10	Generally, is it safe to share your email content with people you trust?
12	Would you regularly tell where you are in your social media accounts?
21	Do you have any shared email or other Internet accounts?

7.3.1.4 Others

Question no	Scenario
16	Do you have different passwords for different accounts?
20	Are you careful when you open email attachments?

This assessment is necessary in order to show how much the students learn from the taught material and how much they are aware of the risk and impact of sharing sensitive information.

7.3.2 Method: Questionnaires Based On Yes/No Questions

A qualitative research study was conducted on two groups of 500 students each. The first group (the experiment group) was given taught material on information security threats and precautionary measures. The other group (control group) was not given the material. There was no pre-test conducted on either group. The main reason for omitting the pre-test was to allow better randomisation and reduce the possible effects of pre-testing, such as gained awareness of the topic (Research Method Knowledge Base, 2013). Several authors have relied on this method in similar research studies such as Conn et al (2009) and Mok & Pang Woo (2004), amongst others. Therefore, as no pre-test was used, there can be no interaction effect on the groups. The questionnaire was completed with high return rates of 460/500 (92%) for the control group and 450/500 (90%) for the experiment group. The results of the groups are tabulated in the following tables:

Table 20: Experiment group

	Age Groups				
	1	2	3	4	5
Male	41 (45.56%) (19.07%)	47 (51.09%) (21.86%)	38 (44.71%) (17.67%)	41 (46.07%) (19.07%)	48 (51.06%) (22.33%)
Female	49 (54.44%) (20.85%)	45 (48.91%) (19.15%)	47 (55.29%) (20.00%)	48 (53.93%) (20.43%)	46 (48.94%) (16.60%)
Total per age group	90 (20.00%)	92 (20.44%)	85 (18.89%)	89 (19.78%)	87 (19.33%)
Total	450				

Table 21: Control group

	Age Groups				
	1	2	3	4	5
Male	47 (48.96%) (20.43%)	49 (55.68%) (21.30%)	39 (42.86%) (16.96%)	47 (49.47%) (20.43%)	48 (53.33%) (20.87%)
Female	49 (51.04%) (21.30%)	40 (45.45%) (17.39%)	49 (53.85%) (21.30%)	48 (50.53%) (20.87%)	44 (48.89%) (19.13%)
Total per age group	96 (20.87%)	89 (19.35%)	88 (19.13%)	95 (20.65%)	92 (20.00%)
Total	460				

Grounded theory was used in the research for several reasons as discussed below where it is compared to other qualitative analysis approaches.

7.3.3 Grounded Theory

Grounded theory was first introduced in 1967 by Glaser and Strauss. Essentially, it is a method designed to help develop ideas that provide a deeper explanation of a particular phenomenon investigated using a qualitative research approach. It was initially used in nursing research and later was adapted for use in several fields such as management, business, sociology and information systems (Mansourian, 2006). Goulding (2002) discusses how the grounded theory approach is largely undertaken to build theory from collected data. As such, grounded theory should be used to build theory rather than to test hypotheses. Goulding (2002) maintains that grounded theory is more helpful to researchers who are targeting peoples' behaviours. Razavi and Iverson (2006) argue that the grounded theory method is one of the most appropriate methods for situations where the researcher is attempting to reveal user experience or design a theoretical structure

based on reality.

There are three different types of analysis used in grounded theory, as suggested by Strauss and Corbin (1998):

- Open coding: This type of grounded theory is used to produce codes that emerge from the data itself,
- Axial coding: This type is used to combine the designed codes with sub- codes,
- Selective coding: This type is used to generate categories that are more suitable to the core research from the overall categories that developed from the acquired data.

Grounded theory has been widely used in areas related to information systems due to its success in contributing to the theoretical core of information systems (Matavire & Brown, 2008). Baskerville and Pries-Heje (1999) argue that the wider use of the grounded theory in different disciplines provides a comprehensive and deeper explanation and effectiveness of developing context-based research.

Qualitative methods such as positivist and interpretive case studies and grounded theory have proven effectiveness regarding information security risks in terms of actual motivations and computer users' behaviours (Crossler et al, 2012). Due to the theoretical basis that can be established through the use of grounded theory, it has become increasingly used in information security. Essentially, the grounded theory approach helps reveal human behaviour in information handling practices and has particular pertinence particularly in matters relating to information security and privacy (Chen & Xu, 2013).

Template analysis is another method that is used is as an analysis tool in qualitative research. However, this method is not suitable for this study due to the nature of the situation being analysed. In template analysis the researcher has an initial coding template, which is then modified or verified through data collection, while grounded theory starts from unstructured data in order to build a theory based on emerging answers to develop categories (Cassell et al., 2004).

Grounded theory is inductive in its approach in that it starts with the data to find a pattern in the data rather than imposing a framework upon it. This is in contrast to the template analysis approach which starts deductively as the analytical frameworks are predetermined (Cassell et al., 2004).

Interpretative phenomenological analysis is another method used to analyse qualitative data based on lived experience. As interpretative phenomenological analysis is developed to offer a theoretical foundation and a detailed procedural guide for a particular case, it has been widely implemented in the field of health psychology (Brocki et al., 2006).

The goal of a phenomenological study is to describe the lived experience of the participants and the meaning of that experience from the participants' perspective, unlike the grounded theory in which the goal is targeting the user's behaviour to build a theory from their experience.

Charmaz et al (2011) assert that both interpretative phenomenological analysis and grounded theory start with concrete instances of human experience and their behaviour, however, phenomenological analysis remains descriptive and does not assemble a theoretical model that yields hypotheses.

Generally speaking, the purpose of an information security education programme is to develop skills and provide wider knowledge of information security of the Internet (Armstrong & Jayaratna, 2002). Hence, this study adopted grounded theory for the initiated information security education programme. Essentially, two groups of school students were assessed. One group, the experiment group, was taught about information security risks and the other group, the control group, was assessed without prior teaching. Grounded theory was used to compare the two different groups and estimate how much knowledge of information security they had gained by examining the groups using open-ended questionnaires.

The aim of the study was to make the school students reveal their knowledge about information security and to produce theory from the data collected to by conduction a comparison between the taught and untaught groups.

7.3.4 Results and Analysis

Some of the students answered in English and others in Arabic. The data analysis was performed by considering the students' responses and creating sentences that describe the responses. Each sentence is then coded by a category. Based on the answers obtained from the two groups, the following categories were established:

Table 22: categories established from answers obtained from the two groups

Category	Description
1	Differentiation between private and other information
2	Differentiation between different accounts
3	Necessity of keeping good relationships with friends and relatives
4	Necessity of helping others
5	Depending on the situation and at the discretion of the respondent
6	Awareness of risks and outcomes of cybercrimes
7	Importance for relatives and friends to check on the respondent
8	Belief that friends and relatives will not harm the respondent
9	Passwords are protected (i.e. passwords not shared, different passwords for different accounts)
10	Carefulness with online activities

The analysis is conducted for each question showing the differences between the taught and untaught groups based on the categories developed from grounded theory divided into the following classes:

7.3.4.1 Password Sharing

Questions Q4, Q11, Q14, Q15, Q18, Q19 and Q22 fall in the “Password Sharing” class. The results obtained are summarised in the following table in percentage based on each category. T and U refer to the Taught and Untaught groups, respectively. For example, answers of the untaught group to Q4 fall by 12% in Category 1, 13 in Category 2 and so on.

Table 23: Password Sharing

Password Sharing	Q4		Q11		Q14		Q15		Q18		Q19		Q22	
	U	T	U	T	U	T	U	T	U	T	U	T	U	T
Category 1	7	12	3	13	7	12	12	17	10	9	9	11	9	18
Category 2	10	13	8	18	5	11	9	15	3	12	8	13	7	10
Category 3	23	9	15	8	12	6	17	4	9	2	16	3	15	8
Category 4	12	2	19	4	14	7	12	3	15	3	12	7	11	1
Category 5	14	16	8	12	12	12	3	12	6	17	4	15	10	11
Category 6	4	15	10	14	6	13	9	12	5	16	10	14	5	15
Category 7	4	2	10	2	13	8	12	6	18	6	17	10	14	8
Category 8	8	6	12	2	16	6	14	6	25	6	11	3	15	7
Category 9	10	12	8	12	7	12	8	12	4	13	6	11	8	11
Category 10	8	13	7	15	8	13	4	13	5	16	7	13	6	11

The following is an interpretation of the results for each question in the class.

Q4. Would you share your email password with a friend?

The taught group showed higher awareness of protecting email passwords from being shared with friends and family. These are significantly apparent in the lower response of the taught group in Category 3 (Necessity of keeping good relationships with friends and relatives) by 14% and Category 4 (Necessity of helping others) by 10% than the untaught group to cultural traits of culture.

Q11. If there is an urgent matter, would you give your password to a trusted person to access your computer?

For the above question, the taught group revealed a significant level of awareness towards sharing passwords with people they trust over the untaught group, particularly in Category 1, 2, 3, 4, 7, 8 and 10.

Q14. Would you give your email password to a person you trust?

The answers by the taught group reveal that the respondents were highly convinced of not sharing their passwords with anyone. This is particularly obvious in the significant difference between the two groups Category 8 as the untaught group reflected some extent of the belief that friends and relatives will not harm the respondent, whereas the taught group was more aware of the harms of sharing passwords even with people they trust.

Q15. In case you shared your account password with someone, will you change it later on?

The taught group showed improved recognition over the untaught group of the importance of changing passwords if divulged to someone including the trusted ones.

Q18. Do you have your password(s) written somewhere?

The reason why people write their passwords down is mainly because they think they may forget it or because they cannot memorise it. They also do not anticipate that by writing their passwords down they become under higher risk of exposing their accounts to others. Others may write their passwords also to allow others whom they trust to access

their accounts. The taught group showed stricter posture towards writing their passwords reflected in improved answers in almost all categories.

Q19. Have you ever given your password of any account to someone?

Ideally, the answer to this question from a security awareness viewpoint is no. However, the untaught group considered urgent matters, trust and convenience as aspects of possible sharing of their passwords. Although the taught group reflected that they had shared their passwords in urgent matters but they affirmed that they changed their password at the earliest opportunity after.

Q22. Do you share any instant messenger’s passwords with others?

The taught group showed better ability of differentiating between accounts that that of the untaught group and preserving their passwords even from trusted people.

7.3.4.2 Device/Account Access Sharing

Questions Q7, Q8, Q13 and Q17 fall in the “Device/Account Access Sharing” class. The results obtained are summarised in the following table in percentage based on each category.

Table 24: Device/Account Access Sharing

Device/Account Access Sharing	Q7		Q8		Q13		Q17	
	U	T	U	T	U	T	U	T
Category 1	6	10	5	12	12	12	9	13
Category 2	5	11	12	15	5	13	10	11
Category 3	13	7	15	9	13	4	15	8
Category 4	15	2	14	3	14	9	12	9
Category 5	7	14	8	14	5	13	9	15
Category 6	5	14	6	14	7	11	4	13
Category 7	23	7	15	1	14	7	9	6
Category 8	17	9	14	6	16	8	17	2
Category 9	4	12	5	12	5	12	8	11
Category 10	5	14	6	14	9	11	7	12

The following is an interpretation of the results for each question in the “Device/Account Access Sharing” class.

Q7. Would you allow access to your personal computer that contains sensitive information to a friend or relative if requested?

For this question, it is clear that the taught group expressed ability of differentiation of

information and refrained from allowing access to a computer containing sensitive information. The significant difference was in Categories 7 and 10, reflecting awareness of account access sharing risks even with relatives and friends and carefulness with possible online activities in case the computer is used by someone else.

Q8. Would you allow access to your phone to a friend or relative if requested?

Realising the importance of keeping the password secret even from friends and relatives, the taught group revealed higher awareness than that of the untaught groups particularly in Category 4 and 7.

Q13. Would you give access to your Facebook to a person you trust?

The two groups showed coherence towards the giving different accounts different importance as shown in Category 1. However, the taught group revealed better understanding that sharing one account may lead to further risks beyond the mere account access they might have given.

Q17. Would you lend your USB flash memory to a friend if requested without checking whether it has sensitive information stored?

There answers to this question showed a general improvement to awareness of sharing risks. In particular, the untaught group reflected the influence of the belief that friends and relatives will not cause them any harm. The taught group however realised that awareness is needed regardless with whom information is shared.

7.3.4.3 Personal/Confidential Information Sharing

Questions Q3, Q5, Q6, Q9, Q10, Q12 and Q21 fall in the “Personal/Confidential Information Sharing” class. The results obtained are summarised in the following table in percentage based on each category:

Table 25: Personal/Confidential Information Sharing

Personal/Confidential Information Sharing	Q3		Q5		Q6		Q9		Q10		Q12		Q21	
	U	T	U	T	U	T	U	T	U	T	U	T	U	T
Category 1	7	15	8	14	4	11	8	12	5	11	9	15	7	11
Category 2	4	12	6	15	6	23	9	11	8	11	6	14	11	13
Category 3	16	4	15	4	16	2	12	3	16	8	16	4	17	1
Category 4	14	6	20	3	14	2	19	8	9	8	12	4	13	7
Category 5	5	12	10	12	10	12	2	17	9	12	4	13	2	15
Category 6	8	11	9	11	8	11	9	14	10	14	9	15	4	14
Category 7	17	7	9	5	11	8	15	7	20	7	19	1	16	9
Category 8	14	7	12	7	12	10	17	5	11	8	12	5	15	6
Category 9	9	14	6	12	9	10	4	11	6	10	5	15	7	13
Category 10	6	12	5	17	10	11	5	12	6	11	8	14	8	11

Q3. May all information be shared with friends and relatives?

The taught group was able to provide further recognition of sensitive information as reflected in the higher percentage of Category 1 than that of the untaught group. The taught group also showed improved perception of information concepts in all other categories.

Q5. Would you share your email content with a friend if requested?

The taught group also showed better awareness of sharing presumably private information that the untaught group respondents said they would share mainly to help others (Category 4). The taught group hence refrained from sharing such information and considered the necessity to help others is not a relevant aspect of sharing information.

Q6. Would you share your sensitive information with a friend that you met in social media website (i.e. Facebook, twitter, chatting website)?

Differences between the two groups are particularly evident in Category 2 and 3, which maintain that the keeping good relations and helping others are not a solid reason for sharing sensitive information as regarded by the taught group, especially with social media acquaintances. The untaught group revealed that they might share such information for the sake of helping others or keeping relationships.

Q9. Can there be serious consequences of sharing sensitive information with others?

The answers to this question showed acquired knowledge by the taught group of the

consequences of sharing sensitive information. The untaught group however considered situational aspects and trust in friends and relatives (Category 5 and 8) as potential reasons for sharing sensitive information.

Q10. Generally, is it safe to share your email content with people you trust?

The untaught group generally claimed that sharing the email content with trusted people was a way to convey their trust in others, which is evident in the percentage of the answers falling in Category 7. The taught group however were indifferent to sharing with trusted people in favour of preserving private information.

Q12. Would you regularly tell where you are in your social media accounts?

It was evident that the untaught group paid significant attention to keeping their relatives and friends in touch through social media, ignoring potential security risks that might arise based on such behaviour. The taught group however was strictly clear about protecting their locations in social media, which is again reflected in the percentage of the answers falling in Category 7.

Q21. Do you have any shared email or other Internet accounts?

The untaught group showed inclination to having some shared online accounts, stressing the overwhelming cultural influence of sharing among close relative and friends. This factor is evidently less significant in the answers of the taught group, particularly in Category 3, 7 and 8.

7.3.4.4 Others

Questions Q16 and Q20 covering some further attention to cybersecurity are put in an individual class, called others. The results obtained are summarised in the following table in percentage based on each category.

Table 26: Others

Others	Q16		Q20	
	U	T	U	T
Category 1	5	12	12	14
Category 2	6	14	7	15
Category 3	12	9	11	4
Category 4	16	5	14	6
Category 5	7	16	6	14
Category 6	6	11	7	11
Category 7	25	5	10	1
Category 8	13	2	16	5
Category 9	6	12	8	14
Category 10	4	14	9	16

Q16. Do you have different passwords for different accounts?

The results obtained show that the untaught group consider the cultural factor of keeping good relations by sharing private information with close relative and friends. The untaught group however did not consider this as an important factor. This is reflected in the differences between the two groups' answers particularly those falling in Category 4, 7 and 8.

Q20. Are you careful when you open email attachments?

The taught group showed better attention to email attachments particularly with regard to the emails sent by close relative and friends. Whereas the untaught group held the believe that close relative and friends will cause them no harm, the taught group showed attention to the risks of email attachments regardless of the sender, and some reflected on the possibility that the sender might not be the one claiming to be.

7.3.5 Summary of the results

The taught group showed greater knowledge in the answers to questions in categories 3, 4, 7 and 8. Those categories represent the respondents' chosen preferences of sharing sensitive data with their relatives and friends. Those categories also represent the trust factor the respondents believe they have to have with relatives and friends. In the taught group, the respondents reflected a higher sense of recognition for privacy as their answers were directed towards keeping more information private. These respondents also developed more knowledge of private information, the importance of keeping certain

information private and not to share even with relatives or close friends. The tables above demonstrate more awareness of information security in the taught group. The taught students showed a better ability than the untaught students to differentiate between private and non-private information. Their answers also reflected a higher ability to distinguish between different accounts in terms of the sensitivity of the information that may be lost or stolen in the case of carelessness. The untaught group demonstrated more of an inclination towards showing more attachments to the family as the family may need to check on them through their accounts. The taught group, however, realised to a higher extent that although family and friends can be trusted, sharing information with them is still risky and perhaps more importantly, unnecessary. The taught group considered that certain situations may require sharing some information; they stated however that they will have to change the password at the next available opportunity if they had to give it to someone for any reason. The untaught group members did not reflect on changing the password in such cases. The taught students mostly understood that keeping information is their right and they did not have to share it. They maintained that they can keep friends and help them despite not telling them everything they may ask for. That was not the case of the untaught group as they mostly preferred to keep their relationships with relatives and friends than to keep some information private if they had to. The answers of the taught group showed more knowledge of what would happen if some information was shared and consequently accounts were compromised. They mentioned theft, physical and reputational harm, and other potential results of cyber-attacks. There was little evidence of knowledge of these aspects with the untaught group. The answers of the taught group showed more care about their online activities and what they access online than the untaught group. Some of the taught respondents also stated that they have different passwords for different accounts according to the sensitivity of the data the account contains. Categories of individual questions are found in Appendix 6.

7.4 Discussion

The aim of the study was to address the issue of sharing sensitive information in the settings of Arab culture, which has escalated with the increasing use of information technology. With the growth use of the Internet, it is more common now to have sensitive and private information available in digital format and in different places. Therefore, the vulnerability and accessibility of such information becomes higher. Furthermore, Arab culture is of a special nature in which private information is something that Arabs share.

This has been discussed in several studies conducted in the Arab region (Chadwick, 2002 and Koocher, 2009). In particular, Al-Kaabi and Maple (2012) showed, in a survey study conducted in the UAE concerning the cultural impact on information security, that UAE citizens are more likely to share their personal information (such as email content, credit card number) with their family and close friends. Due to increasing Internet usage by children in the UAE, an important meeting was conducted by Dubai Police, Ministry of Interior Community Development Authority and other authorities to discuss possible ways to reduce the risks resulting from Internet usage by children. The meeting maintained that children should be monitored by their parents when using the Internet. Furthermore, they must be educated about the potential risks of sharing private information in order to follow self-discipline while they are left unattended by their parents. This will help the children to have knowledge about social engineering attacks and to reduce the likelihood of them falling victim to having people hack their computers and obtain personal and financial information (Aboul Hosn, 2012).

The study aimed, therefore, to provide a strategy for UAE that helps mitigate the information sharing phenomenon in Arab culture by creating awareness of the consequences of sharing certain information. The study demonstrated that such a strategy, given the embedded cultural aspect, requires educating children in school about the dangers of information sharing and the different types of information that can and cannot be shared. The obtained results from both surveys showed improvements in student awareness of information sharing risks and the differences in information types to be shared or not in. The taught students revealed significant improvement in their perception of sharing information with their friends and relatives. The quantitative figures depicted overall improvement in all questions and were supported by statistical tests. The other survey comparing two taught and untaught groups also showed significant results of overall improvement. The qualitative analysis conducted revealed that the taught students answered the questions with more confidence about what information can be shared and what information should not.

The results provide a basis, given the large number of participants in both surveys, for the proposed information security strategy in UAE. The strategy should embed education at young ages as a crucial factor for attaining information security awareness in the Arab culture setting. The proposed strategy also supports Abu Dhabi Information Security Standard (2013) requirements and goals. Their defined information security standard

clearly states that sharing private and sensitive information with others, such as passwords and tokens used for the system identification, is prohibited due to the risks that result from this phenomenon (Abu Dhabi Government, 2013).

7.5 Sensitive Information Sharing Security Framework

Due to the results obtained from this study with school children, the overall intervention study provided a basis for the information security education framework. As a result, the framework below (Figure 15) was designed accordingly. The framework is aimed at providing education to reduce the impact of sharing sensitive information among family members, friends, employees etc.

The framework covers three main aspects in its design: Sharing environments, Information Security design structure followed by the information security education model. Each aspect is discussed in detail below:

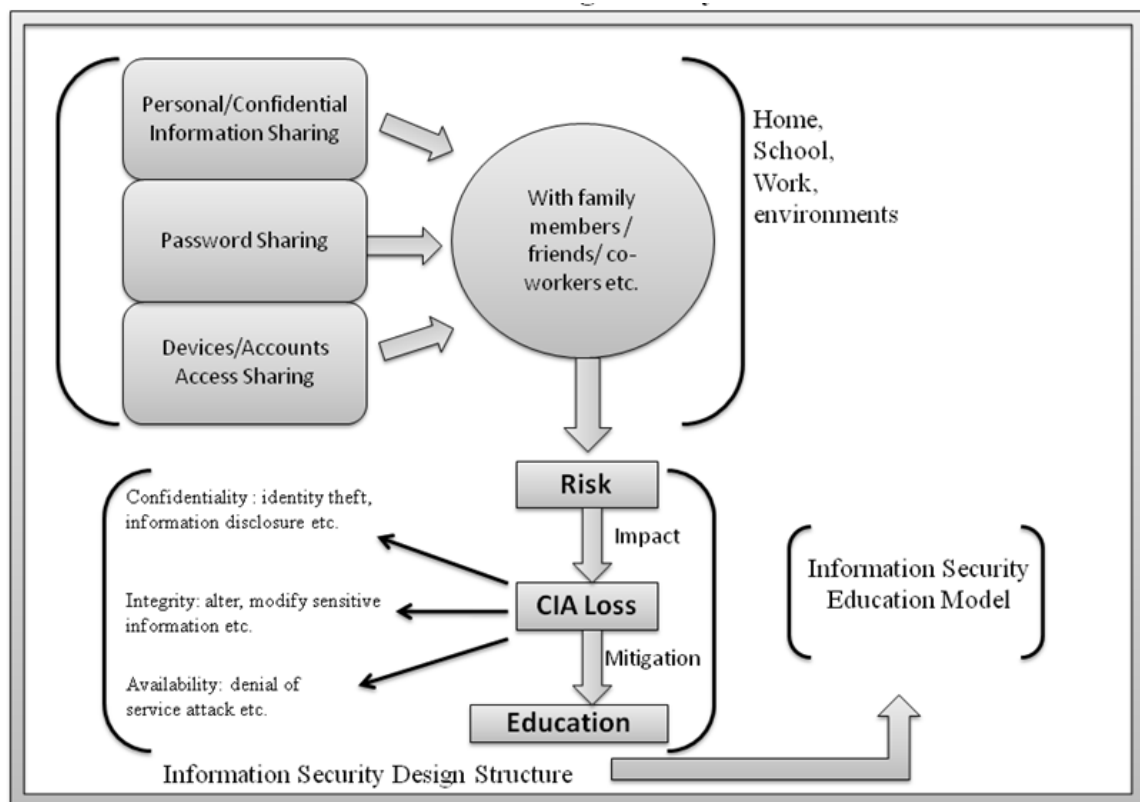


Figure 15: Sensitive Information Sharing Security Framework

7.5.1 Sharing Environments

The sharing environment can be at home, work or school and with family members, friends, colleagues, for example. No matter where it is occurring, the sharing of sensitive information in a particular environment can form a risk to any other environment. For

example, sharing a work email password will form a risk to your Facebook account if the same password is used.

The sharing activities are divided into three parts as per the conducted study in the UAE schools. These activities are shared with family members, friends and employees.

- *Personal/ Confidential Information Sharing:* This can be in the form of sharing confidential information about work, confidential information about school, etc. The aggregation of this information could lead to a privacy attack which is discussed in the questionnaire design in Chapter 4.
- *Password Sharing:* This is a direct threat to the authentication mechanism and can potentially easily compromise the system. The risk towards this activity is discussed in the Questionnaire design in Chapter 4.
- *Devices/ Account Access Sharing:* This is considered to be a risk to personal/work data. This can be in the form of personal computer access/work, USB flash memory, personal mobile and so forth. This kind of access sharing reveals some privacy issues which can potentially compromise your sensitive data through a number of privacy attacks.

7.5.2 Information Security Design Structure

After consideration of the taught material, data acquired and the statistical analysis of the study conducted with school children, the information security design structure has been developed to cover the main parts of security education. Those three parts are discussed below:

- *Risk:* The risk component concerns highlighting the risk activities that can have an impact on both individual and organisations. It is shown in the above figure that all of these activities could lead to a risk.
- *Loss of confidentiality, Integrity and Availability:* The impact of the risky activities could lead to a loss of Confidentiality, Integrity and Availability. The CIA is the fundamental aspect of ensuring the protection of information. This component should show which threat or attack can occur as a result of a particular risky behaviour. For example: sharing your twitter password means sharing a part of your identity and certainly a significant amount of personal information. Therefore, it is possible that modification/deletion/disclosure of your sensitive data could occur.

- *Education:* This is principally designed as an initiative to mitigate the risky activities. For every risky activity, there is an impact that could potentially lead to a loss. The mitigation design, therefore, should consider both the risk and impact of that activity in order to make the user more aware of the digital threats. For example, sharing current location with your Facebook friends list, could lead to a physical theft from your home. The way of mitigating the sharing activity may be done by being aware who should be in your contact list (fake profiles for example) and considering threat that might occur.

7.5.3 Information Security Education Model

All of the above information contributed to the design of a model that sought to provide information security education programme, a syllabus and set of guidelines to reduce the sharing of sensitive information. The framework is largely designed to reduce the impact of culture on information security, especially in a culture where sharing sensitive information among family members and friends is commonplace.

Due to the increased usage of Internet services by children and the necessity of introducing information security education in UAE schools (Emarat Alyoum, 2013) (Aboul Hosn, 2012), the framework also provides a basic foundation for designing information security education for children since it covers basic education knowledge about risky behaviour that is happening around the world.

Due to the problem of password sharing that occurs in some advanced countries (see Chapter 6), the framework is also beneficial for organisations that seek to reduce the impact of sharing sensitive information among employees and can align with the information security policy that is adopted in their organisation.

7.5.4 Information Security Education guidelines

The guidelines below summarise information security education according to the above framework:

7.5.4.1 Password Sharing

Risk/ Online activities	Impact	Education
Sharing your personal/school email password with your friend	Accessing your sensitive data Deletion/Modifying/Misusing Accessing other accounts that have the same password hints to your password selection.	Never share your email password with your friends In cases where you have shared, you should change it immediately with a different password

Risk/ Online activities	Impact	Education
In urgent matters, giving your password to someone you trust	Compromising your content, Deletion/Modifying/Misusing Accessing other accounts that have the same password hints to your password selection.	Try not to share it even if it is urgent, However, if you have shared it, make sure you - - Change your password as soon as you can You should also change other accounts' passwords and password formation
Writing your password for your friend and keeping it somewhere	Accessing your account, Deletion/Modifying/Misusing Accessing other accounts that have the same password hints to your password selection.	Never write down your password and keep it somewhere and if you already have, try to change your accounts' passwords and password formation
Sharing any instant messenger passwords with others	Accessing your sensitive data Deletion/Modifying/Misusing Accessing other accounts that have the same password hints to your password selection.	Never share your instant messenger passwords with others In cases where you have shared it, you should change it immediately with a different password formation. Try to change all your accounts' passwords and password formation.

7.5.4.2 Devices/Accounts Access Sharing:

Risk/ Online activities	Impact	Education
Allowing access to your personal computer if requested	Privacy attacks such as <ul style="list-style-type: none"> ▪ structural re-identification attacks, ▪ inference attacks, ▪ information aggregation attacks 	Remove/secure your sensitive information before you share your personal computer even if you trust the person. Make sure you often check your sensitive information especially if you have shared access (e.g. profile settings)
Allowing a friend to access your phone if requested	Privacy attacks such as <ul style="list-style-type: none"> ▪ structural re-identification attacks, ▪ inference attacks, ▪ information aggregation attacks 	Try to restore your sensitive information before you share your phone even if you trust. Make sure you have a regular check on your sensitive data in the case

Risk/ Online activities	Impact	Education
		where you have shared (ex. profile setting). Before allowing, make sure you sign out from your applications that need password verifications (not in an automatic sign in mode).
Sharing access to your Facebook account with someone you trust	Deletion/ modification your posted information Privacy attacks such as <ul style="list-style-type: none"> ▪ structural re-identification attacks, ▪ inference attacks, ▪ information aggregation attacks 	Try not to share your access with your friend even if you trust Make sure you have a regular check on your sensitive data in the case where you have shared (eg. profile setting).
Lending your USB flash memory to a friend if requested	Privacy attacks such as <ul style="list-style-type: none"> ▪ structural re-identification attacks, ▪ inference attacks, ▪ information aggregation attacks 	Remove/secure your sensitive information before you lend your USB flash memory.

7.5.4.3 Personal/Confidential Information Sharing:

Risk/ Online activities	Impact	Education
Sharing/Posting sensitive information about yourself on an online service such as current location/ future plans/ personal activities/ any other sensitive information (Password, Personal Information)	Cyber stalking Cyber bullying Harassment Physical theft Compromising your online account Privacy attacks such as <ul style="list-style-type: none"> ▪ structural re-identification attacks, ▪ inference attacks, ▪ information aggregation attacks 	When you post any sensitive information about yourself you should first consider the possible impact of it. Knowing who appears on your list and assuring yourself that there is no-one you do not know. Bear in mind, that there are people with fake profiles and their intentions are to mislead people through the posted information.
Sharing your email content with your friends or relatives, (confidential information, school-related documents etc.)	Privacy attacks such as <ul style="list-style-type: none"> ▪ structural re-identification attacks, ▪ inference attacks, ▪ information aggregation attacks 	You should know who you are sharing this information with. You should realise the possible impact of sharing before you share such

Risk/ Online activities	Impact	Education
		privacy information.
Having any shared email or other shared Internet accounts	Privacy attacks such as <ul style="list-style-type: none"> ▪ structural re-identification attacks, ▪ inference attacks, ▪ information aggregation attacks 	Try not to have such accounts but maintain your privacy if you have one (by not sharing sensitive information)

7.5.4.4 Others (can have an impact on sharing):

Risk/ Online activities	Impact	Education
Having one password for all your accounts that need password verification	Compromising (putting at risk) other account if one account has been hacked	Having different passwords for different accounts. Password formation should be hard to guess (should not be something that identifies you)
Care when opening attachment	Compromising your account, Putting your device at risk (viruses, malware etc.) Stealing your sensitive data	Never share sensitive information (personal information) through attachments until you make sure who the sender is and why he or she is asking for such information

7.6 Conclusion

Investment in information system security tools to protect an organisation's assets can be inadequate as a strategy for reducing overall information security risks. Risk assessment is an important consideration to ensure the success of such a strategy. Where the risk is apparently as a result of a cultural and behavioural set of attitudes, causing damage to the information security fundamentals (Confidentiality, Integrity and Availability), then the solution should be designed according to that cultural and behavioural background. Changing the culture of trust in order to be in line with best practice in information security can best be attained through education concerning information security. Privacy and security measures should be taught to school students to combat the phenomenon of sharing private details with family and friends. This study has demonstrated a significant change of attitude of sharing private information with others. Moreover, children recognised the risk and its impact in different scenarios that were provided in the second

assessment. Ultimately, the outcomes of the study are to be used to pave the way for decision makers and competent authorities to take appropriate measures for child protection over the Internet. This could further help in designing appropriate protection plans and measures based on children's attitudes reflected in this study. Since the study covers several patterns that could potentially lead to identifying victims of social engineering attacks, it would be beneficial for Abu Dhabi Educational Council (ADEC) to design their strategic plans in order to have an efficient and effective information security awareness strategy.

A framework was designed to be used as a tool for reducing the impact of culture on information security. The framework is also accompanied by sensitive information sharing education guidelines to show how the security education programme could be designed.

CHAPTER 8: CONCLUSION AND FUTURE WORK

8.1 Conclusion

This thesis has provided a comprehensive explanation of information security threats, which are represented in two main fields, the human factor and the cultural background, from the literature. It has been shown how different security initiatives reduce the information security risk; however, those initiatives that consider cultural background usually find it difficult due to the different cultural characteristics worldwide which ultimately form a hurdle to information security compliance.

In order to provide the most effective solution security issues, from previous studies worldwide, relating to the misuse of sensitive information such as passwords have been considered. Similarly, the research study has analysed in depth the impact of these behaviours and attitudes on the information security triad with respect to both individuals and organisations.

Due to the need for an understanding in respect of the cultural impact of sharing sensitive information amongst family members and friends, several countries have been considered in this research. The cultural and social investigation considered neighbourhood countries such as Oman and KSA; the research also considered the UK, as a western culture.

Due to the cultural and social nature of the problem, the research strategy proposed a solution that considered the cultural basis of these security issues. Such solutions often result in resistance to change. However, according to the literature, education is the best defence against resistance to cultural change (Naylor, 1996), and can produce effective outcomes (Aloul, 2012).

To derive the solution governmental initiatives towards sharing sensitive information such as password sharing education were analysed. The governmental initiatives of the United States, the United Kingdom, Australia and GCC countries were critically analysed in order to find an educational programme to reduce the impact of sharing sensitive information.

The cybersecurity strategies of the United States, the United Kingdom and Australia give limited reference, if any, to education regarding password sharing, whilst the GCC

countries do not have a cyber-security strategy.

An educational strategy was designed to reduce this phenomenon through an intervention study implemented in school children to patch the social vulnerability.

Following the positive results obtained from the intervention study in school children, the study provided a basis for an information security education framework. The latter has been designed to strategically reduce the impact of sharing sensitive information among family members and friends.

The aim and objectives of this research are now considered. The aim of this research was to: *Develop a strategic framework to minimise information security risks in the UAE.*

A strategy has been developed using the result of the intervention study that has been conducted with school children. The framework has been designed to model the needs of UAE's organisational requirements in ensuring their information security. The framework was targeted to reduce the impact of culture in information security, starting with school children in the UAE. The strategic framework can be used to design an information security syllabus, security training and an information security culture programme that aims to reduce the threat of sharing sensitive information.

Due to the password sharing phenomena also existing in some advanced countries, the strategic framework could help to design an educational programme in order to minimise the risk of sharing sensitive information amongst family members, friends, co-workers etc. in such countries.

In order to achieve the aim of this research, several objectives were established namely:

Objective 1: Conduct a comprehensive literature review on Arab culture (UAE country) and its current ICT practices, sharing sensitive information, security standards and policies

This objective has been addressed in Chapters 2 and 3. The dissemination of information technology has rendered restriction and containment of information very difficult. The Arab world has not yet achieved the same level of maturity, with respect to information technology as the developed world. The potential and current impact of advanced information technology on information security in developed countries, and its relationship to Arab society whose culture is marked by sharing confidential information and it's a lack of understanding of the actual value of that information. Information

technology in the modern age can have a substantial effect in destabilising national security. Therefore, everyone should know the value of information and understand which information should not be shared with others. The technological expansion in the Arab world requires the development of security policies in information technology based on a specific infrastructure that inhibits the cultural factor from granting individuals the freedom to share confidential information.

Many cases of sharing sensitive information have led to a loss to both individuals and organisations. This has often been achieved through the social engineering attacks which manipulate human behaviour rather technology. The damage that can occur due to the sharing of sensitive information among individuals is extended to the law enforcement community. Law enforcement bodies can find it extremely difficult to identify perpetrators of identity theft because of information sharing.

The information security standards failed to sufficiently consider the role of culture which potentially forms a threat. This has been considered through analysing various information security standards and policies worldwide and existing initiatives to reduce the impact of culture on information security.

Objective 2: Investigate behaviours specific to Arab culture that could be pertinent to privacy sharing (surveys, literature review) in the UAE

This objective has been addressed in Chapter 4 through a pilot study conducted in major organisations in the UAE. Two approaches have been used to provide a proper foundation for the cultural issue on information privacy in order to proceed to the next stages. Based on the results obtained from the 90 participants, people from the UAE (Arabs) were willing to share their sensitive information (such as email content, credit card numbers etc) with family members and friends. The study has been compared with a similar study by Olson et al (2005) on 30 people who worked at mid-sized companies in the USA and used computers as part of their jobs; the difference can be seen in the comparison table in Chapter 4.

- Due to the need for local context investigations, interviews were conducted with two IT executives in Abu Dhabi. A summary of the key issues obtained from the interviews is as follows:
- Internal policies and compliance to international standards are not enough to prevent employees from sharing sensitive information;

- Policies are clear on the system but it is the implementation that usually generates problems as it involves people;
- There are procedures, rather than measures, that may be taken along with policies and standards, such as evaluation of employee awareness of information security;
- Courses by experts have been given to employees but little progress has been noticed;
- Technological development has revealed information sharing in a more obvious way than in the past (e.g. message broadcasts, etc);
- Awareness is the most important factor in information security and it has to be continuous and assessed to confirm that people are familiar with it;
- It has been noticed that employees from non-Arab cultures are more aware of the value of information and are more discreet in sharing it. This has been witnessed within organisations;
- There have been clear examples of cultural differences regarding information handling within organisations;
- Awareness in childhood would also mitigate the financial burdens of continuous yet inefficient training at a later age.

Objective 3: Investigate behaviours and attitude towards information security in GCC countries

This objective has been addressed in Chapter 4 where further countries of the GCC region are considered in this research. Based on information gathered in a typical social engineering attack, a questionnaire was devised and administered with municipality staff in 3 GCC countries, Oman, KSA and UAE, which represented the majority of the GCC population. According to the data obtained and the Kruskal–Wallis one-way ANOVA test, there were similarities among the 3 countries in most questions, showing similar behaviour towards information-sharing these countries. The behaviour of sharing sensitive information, including passwords, shown in Chapter 4 has a strong relation to the cultural attitude.

Objective 4: Investigate behaviours and attitude towards information security in a different culture than the Arab culture.

This objective was addressed in Chapter 4 where a comparison was made between the UK culture and the GCC countries. The results obtained from the questionnaire, which

targeted 90 private individuals (white English) who work in Council departments in the UK, was compared with 90 people of the GCC countries. According to the Mann-Whitney U test, there exists a statistically significant difference in information security preferences between the two groups. This result indicated there was a cultural difference between the two groups which demonstrated the impact of culture on information security through the sharing of sensitive information amongst family members and friends.

Objective 5: Critically investigate and analyse the information security strategy initiatives to minimise the risk of the sharing of sensitive information found in the UAE

This objective has been addressed in Chapters 5 and 6. Chapter 5 has presented different security mitigations to reduce the risk of sharing sensitive information. As a result, education and awareness was considered to be the best solution for adoption from the other security mitigation measures.

In Chapter 7, a method was designed to enable critical analysis of the existing national cybersecurity strategies for the United States, the United Kingdom and Australia in order to develop an education and awareness programme to reduce the occurrence of sharing sensitive information in the UAE. The analysis aimed to assess the possible adoption of certain elements, if any, of these strategies relating to education within the UAE.

The awareness strategies provided by the U.S., the UK and Australia provided some education initiatives for security threats in the password security domain. For example, the strategies maintain the importance of the selection of the password and the risk of choosing a weak password. However, sharing passwords with others is stated only as advice, without giving details of the risks associated with sharing passwords and the impact on both individuals and organisations. Therefore, the possibility of adopting awareness advice without educating users will not make any difference to cybersecurity risks in the UAE, since CERT.ae provides similar advice to awareness strategy for the advanced countries.

Finally, the information security risks found in the UAE should be dealt with strategically in order to significantly reduce the cultural impact.

Objective 6: Devise a strategy for privacy sharing in Arab culture (UAE), which comprises a solution or a set of solutions to the problem of sharing sensitive information to reduce overall information security risks

This objective has been addressed in Chapter 7. The proposed strategy was designed with

consideration of the social risk of sharing sensitive information with family members and friends. The strategy to be developed for private information sharing in Arab culture aims to reduce the overall information security risks.

The strategy targets school students in the UAE and assesses their information security awareness based on the course material designed to reduce information security risks.

In order to implement an effective information security education strategy, several aspects were taken into consideration before designing the taught materials:

- The education programme should be designed to cover the following aspects:
 - Differentiation between private and other information
 - The potential risk posed by sensitive information sharing
 - The impact of the risk as a result of the sharing phenomenon
- In order to design and implement an effective information security strategy that reduces the risk of sharing sensitive information amongst friends and family members, we must first acknowledge the reaction of school children to the information security education programme and how much this can contribute to building the required strategy for Abu Dhabi Emirate.

Objective 7: Implement the strategy (taught material) on samples of students in different schools, age groups (11-17) and gender

This objective has been addressed in Chapter 7. The teaching material used lessons and interactive software to teach about privacy as an aspect of information security. A sample of 1200 students, divided into groups by age and gender, was considered in the target schools. The respondents were equally divided between genders and with the following age groups:

- Less than 11 (20%) from each gender
- Between 11 and 13 (20%) from each gender
- Between 13 and 15 (20%) from each gender
- Between 15 and 17 (20%) from each gender
- Over 17 (20%) from each gender

The figure below shows the age and sex distributions according to the implemented strategy:

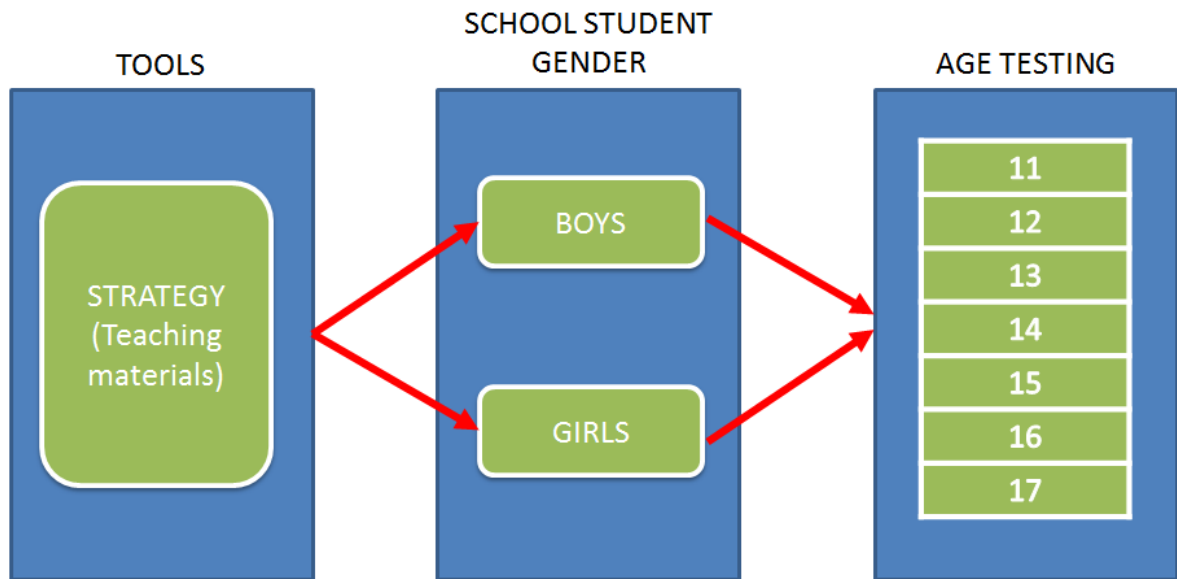


Figure 16: Teaching as a method of reducing information security risks

Due to the sensitivity of the study conducted in the school children, no direct interaction occurred with the school children. Although all the schools agreed to run the Likert scale assessment, not all of them agreed to run the Yes/No type assessment, hence a smaller number of respondents (500 students) has been considered.

Objective 8: Conduct a series of surveys to test applicability and assess the results of the implementation before and after the taught material

This objective has been addressed in Chapter 7. The study followed two approaches to measure the awareness of social engineering attacks and the potential to which information sharing can lead to compromise of the digital authentication. Accordingly, two types of surveys (quantitative and qualitative) were designed to gauge the students' sharing preferences before and after the training programme took place.

The first approach proposed for implementation used Likert scales as pre and post assessments of security awareness of the student groups whereas the second approach was qualitative and was conducted on two groups of 500 students each. The first group (the experiment group) was given taught material on information security threats and precautionary measures (part of 1200). The other group (the control group) was not given the material (not part of 1200).

The questionnaire used Likert-scale measures and 1071 responses were completed in December 2012. Shortly after the responses were collected, taught material was given to the students (1200) with the aim of raising the students' awareness of information

security risks.

In February 2013, the second stage of the assessment targeted a controlled group of 250 of each gender from the initial 1200 respondents, based on the same percentages as above for every age group. The approach used Yes/No questions with the reason for the choice, and with the aim of assessing their security awareness. There were 460 responses collected.

In April 2013, the questionnaire was distributed to a group of respondents who had not been given the taught material. This step was carried out in order to analyse the impact of teaching on students by comparing the results obtained from the taught group and those from the non-taught group. There were 450 responses collected.

In May 2013 the initial group of 1200 students were assessed using the Likert-scale measure in order to critically analyse the difference between the two assessments. There were 1053 responses collected.

8.2 Further Work

This thesis has provided a novel contribution to the field information security, particularly where cultural influences form a hurdle to information security compliance by sharing of sensitive information. However, further research is required to gain insight into several aspects of sensitive information sharing based on cultural and non-cultural influences.

The following limitations may be addressed by further research:

- The thesis covered a successful implementation of an information education programme for school children, which was designed based on the results of an associated intervention study. However, due to the sensitivity of the information collected and the anonymity that the survey followed, a comparison of individual students' performances in the pre- and post- tests was not conducted. Therefore, there was no way to match individual students' pre-test results to their results in post-test results. This may have resulted in loss of some information, for example individual awareness improvement. Further research may benefit from gauging individual improvements in information sharing awareness provided it can devise appropriate tools for matching pre- and post-test results.
- Due to time and curriculum-related constraints, the same material was designed and taught to all age groups of the targeted school students. Had the taught

material been appropriately adapted to different age groups, better performance in the intervention may have been achieved. Moreover, it is difficult for syllabus designers to know what specific content of the material suits a particular age group. Therefore, further research is needed in this respect, specifically to set the educational requirements for each age group (for example which age group should be educated about the risk of sharing credit card details).

Based on this study of sensitive information sharing by school children in the UAE, it is evident that social networks represent a significant threat to children, in particular in terms of cyberstalking and cyberbullying. The study has identified the aspects of minimising such threats by education; however, no in-depth coverage of how this is to be undertaken has been conducted. Therefore, further research is required to analyse and manage the threats represented by cyberstalking and cyberbullying. The following are some suggestions as to how this may be achieved:

- Design, implement and test for efficacy Internet safety programmes that address cyberbullying and cyberstalking attacks
- Run a series of assessments that aim to identify potential risky behaviour of the students in terms of information sharing over online social networks.
- Update the educational curricula according to the identified risk appropriately for all school levels (elementary, secondary etc.).
- Design an educational framework that addresses the risks, anticipates the impacts and offers mitigation advice to minimise the risks of cyberbullying and cyberstalking attacks.

Knowing that alternative security measures for mitigating social engineering attacks can be adopted in parallel with education, such as technical measures and legislation measures (mentioned in Chapter Five), further research is required in order to design a mitigation system that considers these measures. The following are some of the suggestions in this respect:

- For technological measures, an essential aspect of reducing social engineering is designing and implementing a log file system that contains the user access details and network computer details (IP address, MAC etc.) associated with the physical location of that computer in a network. Combining all these elements in one log file provides the network administrator with deeper knowledge about the activities on

the network. Moreover, password sharing among employees can be identified and discovered by the log file system. This step will enable the system administrator to monitor the entire network security access and identify anything unusual occurring in the network, which may flag social engineering threats. For example, if a finance manager accesses his/her computer from his/her office in an organisation, this normally indicates standard access. However, if the finance manager is accessing a network machine (especially several times) from the human resources department, there may be an indication that someone else is using the finance manager's credentials to log in to the system. In such cases, the technical measure mitigates the threat of the social engineering attack that uses others' password to illegitimately access their accounts.

The above-proposed technical measure can be part of the forensics readiness of the network such that the access details of the user can be used as digital evidence if required.

- Legislation can play a role in minimising the risk of social engineering attacks. Legislation measures require that the country's local laws be updated to consider sensitive information sharing. Further research is to investigate the suitable ways of enforcing such laws. For example, it can be set by the law that password sharing is an infraction and may result in legal consequences. Accordingly, the legal authorities will need to work closely with IT advisors in order to decide what counts as digital evidence and hence to be able to criminalise social engineers attackers.
- Moreover, social engineering attacks across borders are a serious issue, which has affected many online users across the globe. Further research is necessary to understand and propose how such attacks can be addressed from a legal perspective, and perhaps suggest laws and regulations to be followed by different countries in this regard in order to fight social engineering attacks more efficiently.

REFERENCES

7Safe UK (2010): *UK Security Breach Investigations Report*, available at http://www.7safe.com/breach_report/Breach_report_2010.pdf

Abawajy, J. (2012). User preference of cybersecurity awareness delivery methods. *Behaviour & Information Technology*, iFirstarticle

Aboul Hosn, D. (2012). Families warned to monitor children's use of computers. *Gulf News*. Available at <http://gulfnews.com/news/gulf/uae/crime/families-warned-to-monitor-children-s-use-of-computers-1.975025> [Accessed 18 October 2013].

Abu Bakr, F. A. (2001): *Open Management Systems - The Next Business Revolution of the Twenty First Century*. E-Track for Publication and Distribution, Cairo

Abu Dhabi Government (2013). Information Security Standards. Version 2.0

Abu-Musa, A. (2009). Exploring the importance and implementation of COBIT processes in Saudi organizations: An empirical study. *Information Management & Computer Security*, 17(2), 73-95.

Aburrous, M. R., Hossain, M. A., Dahal, K. P. & Thabatah, F. F. (2010). Experimental Case Studies for Investigating E-Banking Phishing Intelligent Techniques and Attack Strategies. *Journal of Cognitive Computation*, DOI: 10.1007/s12559-010-9042-7, Springer Verlag, 2 (3): 242-253.

ADSIC [1] (2010): *Information Security Programme*, available at <http://adsic.abudhabi.ae/Sites/ADSIC/Navigation/EN/Projects/information-security.html>, [Accessed on 25/11/2010]

ADSIC [2] (2010): *IT Security*, available at http://www.abudhabi.ae/egovPoolPortal_WAR/appmanager/ADeGP/Citizen?_nfpb=true&_pageLabel=p1938&lang=en&did=145050, [Accessed on 26/11/2010]

aeCERT. Computer Emergency Response Team (). [ONLINE] Available at: <http://www.aecert.ae/security.php>. [Accessed 23 May 2014].

Alarifi, A., Tootell, H., & Hyland, P. (2012, June). A study of information security awareness and practices in Saudi Arabia. In *Communications and Information Technology (ICCIT), 2012 International Conference on* (pp. 6-12). IEEE.

Alawneh, M. N. Q. (2012). Mitigating the Risk of Insider Threats When Sharing Credentials.

Al-Azazi, S. (2008): *A Multi-Layer Model for E-Government Information Security*

Assessment, a PhD thesis submitted to Cranfield University, School of Applied Sciences

Alder, P. (2006): *A Unified Approach to Information Security Compliance*. EDUCAUSE Review, 41(5), September–October, 46–61.

Al-Hamar, M., Dawson, R., & Guan, L. (2010, June). A Culture of Trust Threatens Security and Privacy in Qatar. In *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on* (pp. 991-995). IEEE.

Al-Kaabi, A. & Maple, C. (2012). Cultural Impact on Information Security: The Case of Arab Culture. In *IADIS International Conference e-Society*, 2011 (p. 391).

Alkaabi, A. & Maple, C. (2013). Cultural impact on user authentication systems. *Int. J. Business Continuity and Risk Management*, Vol. 4, No. 4.

Alkhaleej News (2010): *402 Cybercrimes in Abu Dhabi and Dubai in 2009*, an article dated 09/02/2010, available at <http://www.alkhaleej.ae/portal/f9cc2e32-6fe4-4949-bcd2-d35e88c51fd6.aspx>, [Accessed 15/11/2010]

Aloul, F. A. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, 3(3), 176-183.

Anderson, A. (2006): *Effective Management of Information Security and Privacy*, Number 1 Educause Quarterly

Andress, M. (2000): *Manage people to protect data*, InfoWorld, Vol. 22, Issue 46, 13 November 2000

Apple (2014). iPhone 5s - Features. [ONLINE] Available at: <https://www.apple.com/iphone-5s/features/> [Accessed 14 June 2014].

Armstrong, H., & Jayaratna, N. (2002). Internet security management: A joint postgraduate curriculum design. *Journal of Information Systems Education*, 13(3), 249-258.

Baker, J., Lee, B., & Goo, J. (2005). *The Impact of Social Engineering Attacks on Organizations: A Differentiated Study*. Florida Atlantic University, Boca Raton, FL.

Barakat, H. (1993). *The Arab World*. Berkeley: University of CA Press

Baruah, T. D. (2012). Effectiveness of Social Media as a tool of communication and its potential for technology enabled connections: A micro-level study. *International Journal of Scientific and Research Publications*, 2(5), 1.

Baskerville, R., & Pries-Heje, J. (1999). Grounded action research: a method for understanding IT in practice. *Accounting, Management and Information Technologies*,

9(1), 1-23.

BBC (2014). - History - Enigma (pictures, video, facts & news). [ONLINE] Available at: <http://www.bbc.co.uk/history/topics/enigma> [Accessed 14 June 2014].

BBC News (2013) No internet access in 17% of UK homes Available at: <http://www.bbc.com/news/technology-23620856> [Accessed 15 June 2014]

Bell, J. (2005): *Doing your Research Project*, A guide for first-time researchers in education, health and social science. 4th Ed, Open University Press

Benson, M. A., Compas, B. E., Layne, C. M., Vandergrift, N., Pašalić, H., Katalinksi, R., & Pynoos, R. S. (2011). Measurement of post-war coping and stress responses: A study of Bosnian adolescents. *Journal of Applied Developmental Psychology*, 32(6), 323-335.

Berti, J., & Rogers, M. (2004). Social engineering: the forgotten risk. *Information security management handbook*—.

Bishop, M. (2000). Education in information security. *Concurrency, IEEE*, 8(4), 4-8.

Bishop, M. (2005, September). Position: Insider is relative. In *Proceedings of the 2005 workshop on new security paradigms* (pp. 77-78). ACM.

Bjorhus, J (2014). Five outstate Minnesota banks sue Target over data breach [ONLINE] Available at: <http://www.startribune.com/business/246983121.html>. [Accessed 14 June 2014]

Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security is information risk management. In *Proceedings of the 2001 workshop on new security paradigms* (pp. 97-104). ACM.

Bogolea, B., & Wijekumar, K. (2004, October). Information security curriculum creation: a case study. In *Proceedings of the 1st annual conference on Information security curriculum development* (pp. 59-65). ACM.

Boneh, D., & Shaw, J. (1998). Collusion-secure fingerprinting for digital data. *Information Theory, IEEE Transactions on*, 44(5), 1897-1905.

Brave, D (1999). IT's New Labour Philosophy. *Australian Personal Computer* 20, 10

Britz, J.J. (1996). Technology as a threat to privacy: Ethical challenges to the information profession. <http://web.simmons.edu/~chen/nit/NIT%2796/96-025-Britz.html> [Accessed 24 April 2014]

Brocki, J. M., & Wearden, A. J. (2006). A critical evaluation of the use of interpretative phenomenological analysis (IPA) in health psychology. *Psychology and health*, 21(1), 87-

108.

Case Studies (2014). [ONLINE] Available at: <http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Studies.aspx> [Accessed 14 June 2014].

Cassell, C., & Symon, G. (Eds.). (2004). *Essential guide to qualitative methods in organizational research*. Sage.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2005): *The Value of Intrusion Detection Systems in Information Technology Security Architecture*, *Information Systems Research* Vol. 16, No. 1, March 2005, pp. 28–46

CERT (2009): *Towards E-Education*, available at <http://www.salim.ae/index-ar.php>, [Accessed on 09/11/2010]

CERT-SA [ONLINE] Available at: http://www.cert.gov.sa/index.php?option=com_content&task=view&id=69&Itemid=116. [Accessed 23 May 2014].

Chadwick, P. (2002): *Privacy in Diverse Victoria*, Office of the Victorian Privacy commissioner

Charmaz, K., & McMullen, L. M. (2011). *Five ways of doing qualitative analysis: Phenomenological psychology, grounded theory, discourse analysis, narrative research, and intuitive inquiry*. Guilford Press.

Chaula, J. A. et al. (2006): *Technology as a Tool for Fighting Poverty: How Culture in the Developing World Affect the Security of Information Systems*, Proceedings of the 4th IEEE International Workshop on Technology for Education in Developing Countries (TEDC'06)

Chawki, M., & Wahab, M. S. A. (2006). *Identity Theft in Cyberspace: Issues and Solutions*. *LexElectronica* [Spring 2006].

Checchi, R. M., Sevcik, G. R., Loch, K. D. and Straub, D. W. (2002): *An Instrumentation Process for Measuring ICT Policies and Culture*. Paper presented at the Information and Communications Technologies and Development

Chen, C.C., D. B. Medlin, & R.S. Shaw (2008). A cross-cultural investigation of situational information security awareness programs. *Applied Cognitive Psychology*, 18(6), 360-376

Chen, Y., & Xu, H. (2013, February). Privacy management in dynamic groups: understanding information privacy in medical practices. In Proceedings of the 2013 conference on Computer supported cooperative work (pp. 541-552). ACM.

Cheremushkin, D. V. and Lyubimov, A. V. (2010): *An Application of Integral Engineering Technique to Information Security Standards, Analysis and Refinement*, Proceedings of the 3rd International conference on Security of information and networks, ACM

Chinchani, R., Iyer, A., Ngo, H. Q., & Upadhyaya, S. (2005, June). Towards a theory of insider threat assessment. In *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on* (pp. 108-117). IEEE.

Chryssanthou, A., Apostolakis, I., and Varlamis, I. (2011). *Certification and Security in Health-Related Web Applications: Concepts and Solutions*. Medical Information Science Reference.

CIS (2011). Password Security: A Survey of Australian Attitudes toward Password Use and Management. Centre for Internet Safety.

Colwill, C. (2009). Human factors in information security: The insider threat—Who can you trust these days? *Information security technical report*, 14(4), 186-196.

Commonwealth of Australia (2014). Protecting personal information. *Cyber Smart*. <http://www.cybersmart.gov.au/Schools/Cyber%20issues/Protecting%20personal%20information.aspx> [Accessed 24 April 2014]

Computer Weekly. NHS trust uncovers password sharing risk to patient data. [ONLINE] Available at: <http://www.computerweekly.com/news/2240077810/NHS-trust-uncovers-password-sharing-risk-to-patient-data>. [Accessed 23 May 2014].

Conn, V. S., Hafdahl, A. R., Cooper, P. S., Brown, L. M., & Lusk, S. L. (2009). Meta-analysis of workplace physical activity interventions. *American journal of preventive medicine*, 37(4), 330-339.

Cox, A., Currall J. and Connolly, S. (2001): *The Human and Organisational Issues Associated With Network Security*, JISC Committee for Awareness, Liaison and Training (JCALT)

Creswell, J. W., & Clark, V. L. P. (2007). Designing and conducting mixed methods research.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *computers & security*, 32, 90-101.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2012). Future directions for behavioral information security research. *Computers & Security*.

CSFI (2010). Preliminary STUXNET Report V1.0, www.csfi.us

CSI (2006): Computer Crime and Security Survey, Computer Security Institute, FBI. Available at: www.gocsi.com, [accessed on 19/04/2011]

Čudanov, M., Jaško, O., & Jevtić, M. (2009). Influence of information and communication technologies on decentralization of organizational structure. *Computer Science and Information Systems*, 6(1), 93-109.

Cybercrime Law (2011): Latest News on Cybercrime Legislation from around the World, available at <http://www.cybercrimelaw.net/Cybercrimelaw.html>, accessed on 20/11/2011

Da Veiga, A., Martins, N. and Eloff, J. H. P. (2007): Information Security Culture: Validation of an Assessment Instrument, *Southern African Business Review*, 11(1), 147-166

Dating and romance scams (2014) [ONLINE] Available at: <http://www.scamwatch.gov.au/content/index.phtml/tag/datingromancescams>. [Accessed 14 June 2014].

Davis, A. (2014). Safeguard database connection strings and other sensitive settings in your code. *MSDN Magazine*, <http://msdn.microsoft.com/en-us/magazine/cc164054.aspx> [Accessed 25 April 2014]

Deloitte (2005): *Global Security Survey*, Deloitte Touche Tohmatsu: London

Denning, D. E. (2003): *Information Technology and Security*, appeared in *Grave New World: Global Dangers in the 21st Century* (Michael Brown ed.), Georgetown University Press

Denver Business Journal (2013). Banks and cybersecurity: What are the risk Available at: http://www.bizjournals.com/denver/blog/finance_etc/2013/11/banks-and-cybersecurity-what-are-the.html?page=all . [Accessed 14 June 2014].

Dhillon, G. (1995): *Interpreting the Management of Information Systems Security*, London: London School of Economics and Political Science

Dimensional Research (2011). *The Risk of Social Engineering on Information Security: A Survey of IT Professionals*.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal*, 19(4), 391-412.

Dourish, P., & Anderson, K. (2006). Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-computer interaction*, 21(3), 319-

342.

Dutta, S. and Coury, M.E. (2003): *ICT Challenges for the Arab World*, in Dutta, S., Lanvin, B. and Paua, F. (Eds.). *The Global Information Technology Report 2002-2003: Readiness for the Networked World* (World Economic Forum), New York: Oxford University Press, 116-131

Dutta, S., El-Hage, Ch., Sabbagh, K. and Tarazi, P. (2003): *Challenges for Information and Communication Technology Development in the Arab World, Part 1*

DW.DE (2013). Social media use evolving in Egypt | Middle East | DW.DE | 04.07.2013 . [ONLINE] Available at: <http://www.dw.de/social-media-use-evolving-in-egypt/a-16930251>. [Accessed 14 June 2014].

Emarat Alyoum (2013). Available at <http://www.emaratalyout.com/local-section/education/2013-04-13-1.565598>. [Accessed 12/06/2013].

Emarat Alyoum [1] (2010): *62 Cybercrimes in the State in two months*, an article dated 07/03/2010, available at <http://www.emaratalyout.com/business/local/62-2010-03-07-1.64590>, [Accessed on 13/11/2010]

Emarat Alyoum [2] (2010): *80% of the cyber-attacks are launched from within the organisations in UAE*, article by Abeer Abdulhalim, [Published on 10/11/2010]

Enzer, G. (2011): UAE faces high rates of cyber-crime, web article available at <http://www.itp.net/586180-uae-faces-high-rates-of-cyber-crime>, published September 18, accessed on 20/11/2011

Evans (2012). Report: London no safer for all its CCTV cameras - CSMonitor.com. [ONLINE] Available at: <http://www.csmonitor.com/World/Europe/2012/0222/Report-London-no-safer-for-all-its-CCTV-cameras> [Accessed 14 June 2014].

Everett, C. (2011). A risky business: ISO 31000 and 27005 unwrapped. *Computer Fraud & Security*, 2011(2), 5-7.

Fallan, L. (1999). Gender, exposure to tax knowledge, and attitudes towards taxation; An experimental approach. *Journal of Business Ethics*, 18(2), 173-184.

FAQ (2014). payment card issue FAQ . [ONLINE] Available at: <https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ>. [Accessed 14 June 2014].

Feng, J. X., & Hughes, J. (2009). Analyzing privacy and security issues in the information age-an ethical perspective. *WSEAS Transactions on Information Science and Applications*, 6(1), 126-135.

- Ferreira, A., Correia, R., Chadwick, D. W., Santos, H. M., Gomes, R., Reis, D., & Antunes, L. (2010). Password Sharing and How to Reduce It. *Certification and Security in Health-Related Web Applications: Concepts and Solutions: Medical Information Science Reference*, 243-263.
- File, T (2013). Computer and Internet Use in the United States. Current Population Survey Reports, P20-568. U.S. Census Bureau, Washington, DC.
<http://www.census.gov/prod/2013pubs/p20-569.pdf>
- Finkle, J (2014). "Target says it declined to act on early alert of security breach." *reuters.com* <http://www.reuters.com/article/2014/03/13/us-target-breach-idUSBREA2C14F20140313> [Accessed 15 April 2014]
- Furnell, S. M. et al. (2000): *Promoting Security Awareness and Training within Small Organisations*, Proceedings of the 1st Australian Information Security Management Workshop, Deakin University, Geelong, Australia
- GAISP (2003). http://www.issa.org/gaisp/_pdfs/v30.pdf V3.0,
- Georgia Tech Information Center (2008): *Emerging Cyber Threats Report for 2009*, October 15
- Giannoulis, Peter and Northcutt, Stephen. "Physical Security." *SANS*. January 25, 2007. Web. April 10, 2014. <<http://www.sans.edu/research/security-laboratory/article/281>>
- Glaser, T. D. (2009): *Culture and Information Security Outsourcing IT Services in China*, PhD thesis, Berlin, Technischen Universität Berlin
- Glynn, C (2013) Boston Marathon Bombing "Crowdsourcing: How citizens are using the Internet to help solve crimes - CBS News. [ONLINE] Available at: <http://www.cbsnews.com/news/boston-marathon-bombing-crowdsourcing-how-citizens-are-using-the-internet-to-help-solve-crimes> [Accessed 14 June 2014].
- Goodman, M (2011). From crowdsourcing to crime-sourcing: The rise of distributed criminality - O'Reilly Radar. [ONLINE] Available at: <http://radar.oreilly.com/2011/09/crime-sourcing.html> [Accessed 15 June 2014].
- Goulding, C. (2002). *Grounded theory: A practical guide for management, business and market researchers*. Sage.
- Granger, S. (2010). *Social engineering fundamentals, part II: Combat strategies*. <http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-ii-combat-strategies> [Accessed 24 April 2014]
- Gross, R., & Acquisti, A. (2005, November). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic

society (pp. 71-80). ACM.

Guido, M. D., & Brooks, M. W. (2013, January). Insider threat program best practices. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 1831-1839). IEEE.

Hadden, L.B. (2002), "An investigation of the audit committee and its role in monitoring information technology risks", DBA thesis, Nova Southeastern University, Fort Lauderdale-Davie, FL, AAT 3074875.

Halliday, J (2012). Phone hacking the tip of an iceberg of illegal snooping, Available at: <http://www.theguardian.com/media/2012/jul/06/phone-hacking-tip-iceberg> . [Accessed 15 June 2014]

Hamade, S.N. (2009): *Information and Communication Technology in Arab Countries: Problems and Solutions*, Sixth International Conference on Information Technology: New Generations, April

Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. Information Security technical report, 11(1), 55-61.

Harnesk, D., & Lindström, J. (2011). Shaping security behaviour through discipline and agility: Implications for information security management. *Information Management & Computer Security*, 19(4), 262-276.

Havenetidis, K (2013) Encryption and Biometrics: Context, methodologies and perspectives of biological data.

Haviland, W. A., Prins, H. E. L., McBride, B. and Walrath, D. (2010): *Cultural Anthropology: The Human Challenge*. Published by Cengage Learning, 13th edition

Hinson, G. (2008). Social Engineering Techniques, Risks, and Controls. *EDPAC: The EDP Audit, Control, and Security Newsletter*, 37(4-5), 32-46.

History.com (1905). Fingerprint evidence is used to solve a British murder case — History.com This Day in History — 3/27/1905. [ONLINE] Available at: <http://www.history.com/this-day-in-history/fingerprint-evidence-is-used-to-solve-a-british-murder-case> [Accessed 14 June 2014].

Hjelmås, E., & Wolthusen, S. D. (2006, September). Full-spectrum information security education: integrating B. Sc., M. Sc., and Ph. D. programs. In *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 5-12). ACM.

Hofstede, G. (2003). *Geert Hofstede Culture Dimensions*, available at <http://www.geert-hofstede.com>

Höne, K. and Eloff, J. H. P (2002): *Information security policy — what do international information security standards say?*, Elsevier Computers & Security, Volume 21, Issue 5, 1 October, Pages 402-409

Iimura, H. and Kimizuka, J. (2011): Discussion on Teaching Varieties of English to Students in Japan, whom desire to Study Abroad, Ibaraki Educational Research, 143-158

Inglesant, P. G., & Sasse, M. A. (2010, April). The true cost of unusable password policies: password use in the wild. In *Proceedings of the 28th international conference on Human factors in computing systems* (pp. 383-392). ACM.

Inness, J. (1992). *Privacy, intimacy and isolation*. New York: Oxford University Press.

Inthiran, A. and Seddon A. (2007): *Security Policies: Making it Work*, The 6th European Conference on Information Warfare and Security, Defence College of Management and Technology, Shrivenham, UK, 2-3 July

ISO 27005 Standard (2008): Information Technology – Security Techniques – Information Security Risk Management, BS ISO/IEC 27005:2008

ITP (2009): *UAE to Set Up Cybercrime Court*, an article dated 16/10/2009, available at <http://www.itp.net/578648-uae-to-set-up-cyber-crime-court>, accessed on 15/11/2010

ITU (2003): *Security in Telecommunication and Information Technology*, Telecommunication Standardization Sector of International Telecommunication Union, December

Jaafari, A. R. A. (1983): *Managerial Analysis as commencement of Development of the Arab City*, the Seventh Conference of the Arab Cities Organization: Governance and Regulation in the Service of Contemporary Arab Cities, Algeria

Jain, A. K., Hong, L., and Pankanti, S. (2000): *Biometrics: Promising Frontiers for Emerging Identification Market*, Comm. ACM, pp. 91 –98, Feb.

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: a tool for information security. *Information Forensics and Security, IEEE Transactions on*, 1(2), 125-143.

Janczewski, L. J., & Fu, L. (2010, October). Social engineering-based attacks: Model and New Zealand perspective. In *Computer Science and Information Technology (IMCSIT), Proceedings of the 2010 International Multiconference on* (pp. 847-853). IEEE.

Jones, A., & Martin, T. (2010). Digital forensics and the issues of identity. *Information security technical report*, 15(2), 67-71.

Jones, Le and Hill, E (February 7, 2010). Rom scam: How African fraudsters now make £80million a year ripping off women (and a few men) so desperate for love they'll believe

anything. Available at: <http://www.dailymail.co.uk/news/article-1354155/African-fraudsters-make-80m-year-ripping-women-desperate-love.html>

JPMorgan Chase Cyber-attack (2013). Almost Half A Million Corporate Customers' Data Breached, Bank Warns. [ONLINE] Available at: <http://www.ibtimes.com/jpmorgan-chase-cyberattack-almost-half-million-corporate-customers-data-breached-bank-warns-1496346> [Accessed 15 June 2014].

Kayarkar, H. & Sanyal, S. (2012). A survey on various data hiding techniques and their comparative analysis. 1-9.

Kelle, U. (2006). Combining qualitative and quantitative methods in research practice: purposes and advantages. *Qualitative research in psychology*, 3(4), 293-311.

Khalfan, A. M. (2004). Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. *International Journal of Information Management*, 24(1), 29-42.

Khalil, O. E. M. and Seleim, A. (2009): National Culture Practices and Societal Information Dissemination Capacity, *Journal of Information and Knowledge Management*, 9(2), 127-144

Khushmana, S., Todman, A. and Amin, S. (2009): *The Relationship between Culture and E-business Acceptance in Arab Countries*, Second International Conference on Developments in eSystems Engineering, IEEE

Klingman, C. (2005). The use of technology to combat identity theft. *The Department of the Treasury*. 1-117.

Kluge, D. & Sambasivam, S. (2008): Formal Information Security Standards in German Medium Enterprises, EDSIG

Ko, M. & Dorantes, C. (2006): The Impact Of Information Security Breaches On Financial Performance Of The Breached Firms: An Empirical Investigation, *Journal of Information Technology Management* Vol. 17, Number 2

Koch, R., Stelte, B., & Golling, M. (2012, June). Attack trends in present computer networks. In *Cyber Conflict (CYCON), 2012 4th International Conference on* (pp. 1-12). IEEE.

Koocher, G. P. (2009): *Ethics and the Invisible Psychologist*, *Psychological Services*, Vol. 6, No. 2, 97-107

Kotenko, I., Stepashkin, M. and Doynikova, E. (2011): *Security Analysis of Information Systems taking into account Social Engineering Attacks*, 19th International Euromicro Conference on Parallel, Distributed and Network-Based Processing, IEEE

- Kotter, J. and Schlesinger, L. A. (2008): Choosing Strategies for Change, Harvard Business Review, July–August
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2013, November). Social engineering attacks on the knowledge worker. In *Proceedings of the 6th International Conference on Security of Information and Networks* (pp. 28-35). ACM.
- Kruger, H. A., Flowerday, S., Drevin, L., & Steyn, T. (2011, August). An assessment of the role of cultural factors in information security awareness. In *Information Security South Africa (ISSA), 2011* (pp. 1-7). IEEE.
- Kubiatico, M., Haláková, Z., Nagyová, S., & Nagy, T. (2009). Slovak high school students' attitudes toward computers. *Interactive Learning Environments*, 19(5), 537-550.
- Lafferty, I. (2007). Medical identity theft: The future of healthcare is now – lack of federal law enforcement efforts means compliance professionals will have to lead the way. *Healthcare Compliance*, 9(1), 11-20.
- Lagner, R (2013) Stuxnet's Secret Twin. [ONLINE] Available at: http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack [Accessed 15 June 2014].
- Lagorio, C (2006). State Department Computers Hacked <http://www.cbsnews.com/news/state-department-computers-hacked/> [accessed 15 April, 2014]
- Lainhart, J.W. IV (2001), “An IT assurance framework for the future”, Ohio CPA Journal, Vol. 60No. 1, pp. 19-23
- Layton, T. P. (2006). Information Security: Design, Implementation, Measurement, and Compliance. CRC Press.
- Le Grand, C. and Ozier, W. (2000): Information Security Management Elements, Audit and Control, March
- Le, C. (2011) A Survey of Biometrics Security Systems. *A project report written under the guidance of Prof. Raj Jain*. Washington University in St. Louis.
- Leidner, D. E. and Kayworth T. (2006): A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict, MIS Quarterly, Vol. 30, no. 2, pp. 357-399
- Lewis, J. A. (2014). Cyber threat and response. *Centre for Strategic & International Studies*. 1-8.
- Li, N., & Kirkup, G. (2007). Gender and cultural differences in Internet use: A study of

China and the UK. *Computers & Education*, 48(2), 301-317.

Lichtenstein, S. and Swatman, P. M. C. (2001): *Effective Management and Policy in E-business Security*, Proceedings of Fourteenth Bled Electronic Commerce Conference, Bled, Slovenia

Light, D (1999) Surviving the Revolution.” *The Bulletin With Newsweek*.

Liu, S., & Cheng, B. (2009). Cyberattacks: Why, what, who, and how. *IT professional*, 11(3), 14-21.

Logan, P. Y., & Clarkson, A. (2005, February). Teaching students to hack: curriculum issues in information security. In *ACM SIGCSE Bulletin* (Vol. 37, No. 1, pp. 157-161). ACM.

Long, J. (2011). No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing. Syngress

Losavio, M. M. (2005, November). The law of possession of digital objects: Dominion and control issues for digital forensics investigations and prosecutions. In *Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on* (pp. 177-183). IEEE.

Luftman, J., and McLean, E. R. (2004): *Key issues for executives*. MIS Quarterly Executive, Vol. 3 (2), 14.

Luijff, E., Besseling, K., & Graaf, P. D. (2013). Nineteen national cybersecurity strategies. *International journal of critical infrastructures*, 9(1), 3-31.

Lytle, R (2011) Study: Online Education Continues Growth.”
<http://www.usnews.com/education/online-education/articles/2011/11/11/study-online-education-continues-growth> [Accessed April 17, 2014]

Madan, S. and Madan, S. (2010): *Security Standards Perspective to Fortify Web Database Applications from Code Injection Attacks*, International Conference on Intelligent Systems, Modelling and Simulation

Maftoon, P. and Soroush S. (2010): Utilizing the Analysis of Social Practices to Raise Critical Language Awareness in EFL Writing Courses, *Journal of Language Teaching and Research* 1.6 (2010): 815-824

Makaleh, S. (2011): Cyber Crime victims lost Dh735m in 12 Months, web article available at <http://gulfnews.com/business/technology/cyber-crime-victims-lost-dh735m-in-12-months-1.870533>, published September 21, accessed on 21/11/2011

Malagi, K., Angadi, A., & Gull, K (2013). A Survey on Security Issues and Concerns to

Social Networks. IJSR, Volume 2 Issue 5, (pp.256-265).

Mansourian, Y. (2006). Adoption of grounded theory in LIS research. *New Library World*, 107(9/10), 386-402.

Matavire, R., & Brown, I. (2008, October). Investigating the use of grounded theory in information systems research. In *Proceedings of the 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries: riding the wave of technology* (pp. 139-147). ACM.

McCombie, S., & Pieprzyk, J. (2010, July). Winning the phishing war: a strategy for Australia. In *Cybercrime and Trustworthy Computing Workshop (CTC), 2010 Second* (pp. 79-86). IEEE.

McCoy, C., & Fowler, R. T. (2004, October). You are the key to security: establishing a successful security awareness program. In *Proceedings of the 32nd annual ACM SIGUCCS fall conference* (pp. 346-349). ACM.

McCrum-Gardner, E. (2008). Which is the correct statistical test to use?. *British Journal of Oral and Maxillofacial Surgery*, 46(1), 38-41.

McFadzean, Ezingard and Birchall. "Perception of risk and the strategic impact of existing IT on information security strategy at board level." *Online Information Review*. Vol. 31 No. 5, 2007 pp. 622-660

Medlin, B. D., Cazier, J. A., & Foulk, D. P. (2008). Analyzing the vulnerability of US hospitals to social engineering attacks: how many of your employees would share their password? *International Journal of Information Security and Privacy (IJISP)*, 2(3), 71-83.

Miaoulis, W. (2009). Internet security breach found at UCSF-phishing. *HIPAA Security and Privacy Advisors*. <http://www.hipaasecurityandprivacy.com/2009/12/internet-security-breach-found-at-ucsf.html> [Accessed 23 April 2014]

Middle East Association. Bahrain urged to set up national plan to fight cyber crime. [ONLINE] Available at: <http://the-mea.co.uk/news/bahrain-urged-set-national-plan-fight-cyber-crime>. [Accessed 23 May 2014].

Mitneck, K.D., & Simon, W.L. (2002). *The art of deception: Controlling the human element of security*. London: Wiley.

Mohamed Ali, I. E. (2005): *The Impact of Information Systems on Government Bureaucracies in Arab Countries in Light of the Digital Revolution*, The Sixth Conference on Architecture, Department of Architecture - University of Asyut, Egypt

Mok, E., & Pang Woo, C. (2004). The effects of slow-stroke back massage on anxiety

and shoulder pain in elderly stroke patients. *Complementary Therapies in Nursing and Midwifery*, 10(4), 209-216.

Molok, N. N. A., Chang, S., & Ahmad, A. (2010). Information leakage through online social networking: Opening the doorway for advanced persistence threats.

Moore, A. (2008). Defining privacy. *Journal of Social Philosophy*, 39(3), 411-428.

Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2008). *The "big picture" of insider IT sabotage across US critical infrastructures* (pp. 17-52). Springer US.

Morrow, A (2013). In Post-Revolution Egypt, Social Media Shows Darkside
<http://www.ipsnews.net/2013/05/in-post-revolution-egypt-social-media-shows-dark-side>
[Accessed: April 17, 2014]

Munshi, A., Dell, P., & Armstrong, H. (2012, January). Insider threat behavior factors: A comparison of theory with reported incidents. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 2402-2411). IEEE.

Mwakalinga, J., & Kowalski, S. (2011). ICT Crime Cases Autopsy: Using the Adaptive Information Security Systems Model to Improve ICT Security. *International Journal of Computer Science and Network Security*, 11(3), 114-123.

National cybersecurity Strategies in the World — ENISA. [ONLINE] Available at: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world>. [Accessed 23 May 2014].

Naylor, L. L. (1996): *Culture and Change: An Introduction*, Greenwood Press, pp. 195-196

Newbould, M., & Furnell, S. (2009, December). Playing Safe: A prototype game for raising awareness of social engineering. In *Australian Information Security Management Conference* (p. 4).

Newman, R. C. (2006, September). Cybercrime, identity theft, and fraud: practicing safe internet-network security threats and vulnerabilities. In *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 68-78). ACM.

NISS (2011). Developing National Information Security Strategy for the Kingdom of Saudi Arabia Draft 7. National Information Security Strategy.

NIST (2002): *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*, In National Institute of Standards and Technology, Special Publication, Reports on Computer Systems Technology, Vol. SP 800-30

- Nohlberg, M. (2008). Securing information assets: Understanding, measuring and protecting against social engineering attacks. Thesis, Stockholm University, 1-225
- Notoatmodjo, G., & Thomborson, C. (2009, January). Passwords and perceptions. In *Proceedings of the Seventh Australasian Conference on Information Security-Volume 98* (pp. 71-78). Australian Computer Society, Inc.
- NPR (2014). Edward Snowden: From 'Geeky' Dropout To NSA Leaker : [ONLINE] Available at: <http://www.npr.org/2014/04/16/303733011/edward-snowden-from-geeky-drop-out-to-nsa-leaker>. [Accessed 14 June 2014].
- Obeidat, B. Y., Shannak, R. O., & Al-Jarrah, I. M. (2012). Toward Better Understanding for Arabian Culture: Implications Based on Hofstede's Cultural Model. *European Journal of Social Sciences*, 28(4), 512-522.
- OCERT About OCERT. [ONLINE] Available at: <http://www.cert.gov.om/about.aspx#.UzxOCahdXng> [Accessed 23 May 2014].
- Olanrewaju, R.F., Ali, N., Khalifa, O & Manaf, A.A. (2013). ICT in telemedicine: Conquering privacy and security issues in health care services. *Electronic Journal of Computer Science and Information Technology*, 4(1), 19-24.
- Olson, J. S. et al. (2005): *A Study of Preferences for Sharing and Privacy*, Proceedings of CHI. ACM, April 2005
- Organisation for Economic Cooperation and Development (OECD). (2008). OECD policy guidance on online identity theft. *OECD Ministerial Meeting on the Future of the Internet Economy*, Seoul, Korea, 17-18 June. 1-20.
- Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004, October). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In *Proceedings of the 5th conference on Information technology education* (pp. 177-181). ACM.
- OUCH (2013) The Monthly Security Awareness Newsletter for Computer Users. SANS May 2013
- Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environment.
- Pepitone, J (2012). Boston's Legacy: Can Crowdsourcing Really Fight Crime? <http://www.nbcnews.com/tech/internet/bostons-legacy-can-crowdsourcing-really-fight-crime-n74831> [Accessed: 17 April 2014]
- Pfleeger, S. L., & Stolfo, S. J. (2009). Addressing the insider threat. *Security & Privacy, IEEE*, 7(6), 10-13.

Ponemon Institute. (2005). National survey on data security breach notification. The Ponemon Institute.

Pornari, C. D., & Wood, J. (2010). Peer and cyber aggression in secondary school students: The role of moral disengagement, hostile attribution bias, and outcome expectancies. *Aggressive Behavior*, 36(2), 81-94.

Potts, M. (2012). The state of information security. *Network Security*, 2012(7), 9-11.

Poulter, S (2013). The online shopping frenzy: Web retailers see fastest sales growth for 13 years. <http://www.dailymail.co.uk/news/article-2463951/The-online-shopping-frenzy-Web-retailers-fastest-sales-growth-13-years.html> [Accessed 16 April 2014]

Q-CERT. [ONLINE] Available at: <http://www.qcert.org/about-q-cert> [Accessed 23 May 2014].

Rai, B. S. (2011): UAE Ups its Battle against Cybercrime, article in Emirates 24/7 dated Tuesday, October 04, 2011, available at <http://www.emirates247.com/business/technology/uae-ups-its-battle-against-cybercrime-2011-10-04-1.421776>, accessed On 20/11/2011

Ramachandran, S., Srinivasan, V. R. and Goles, T. (2008): Information Security Cultures of Four Professions: A Comparative Study, Proceedings of the 41st Hawaii International Conference on System Sciences

Ramos, J & Ballel, P (2008). Globalisation, New Technologies (ICTs) and Development: a Global Perspective. http://www.edemocracycentre.ch/files/ICTs_development_EdC_1.pdf [Accessed 15 April 2014]

Ranger, S. (2007). Data breach laws make companies serious about security.

Razavi, M. N., & Iverson, L. (2006, November). A grounded theory of information sharing behavior in a personal learning space. In Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work (pp. 459-468). ACM.

Record online sales over Christmas (2014) <http://www.bbc.com/news/business25671561>
<http://www.bbc.com/news/business-25671561> [Accessed 17 April 2014]

ReedSmith (2010): Data Security Preventing and Controlling Employee-Caused Breaches, by Jaworski, R. M. May 5

Report Details (2013). National bureau of statistics (UAE) [ONLINE] Available at: <http://www.uaestatistics.gov.ae/EnglishHome/ReportDetailsEnglish/tabid/121/Default.aspx?ItemId=2226&PTID=104&MenuId=1>. [Accessed 16 June 2014]

Research Method Knowledge Base (2013). Two-Group Experimental Designs. Available at <http://www.socialresearchmethods.net/kb/expsimp.php> [Accessed 12/05/2013]

Reuters (2014). Target missed many warning signs leading to breach: U.S. Senate report [ONLINE] Available at: <http://www.reuters.com/article/2014/03/25/us-target-breach-senate-idUSBREA201VA20140325>. [Accessed 14 June 2014].

Reuters. Exclusive: Snowden persuaded other NSA workers to give up passwords - sources. [ONLINE] Available at: <http://mobile.reuters.com/article/idUSBRE9A703020131108?irpc=932>. [Accessed 23 May 2014].

Reymond, L., Charles, M., Israel, F., Read, T., & Treston, P. (2005). A strategy to increase the palliative care capacity of rural primary health care providers. *Australian Journal of Rural Health, 13*(3), 156-161.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7), 241-253.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826.

Right to rub out embarrassing pictures and data posted online floated by The Australian Law Reform Commission (2013). <http://www.news.com.au/technology/online/right-to-rub-out-embarrassing-pictures-and-data-posted-online-floated-by-the-australian-law-reform-commission/story-fnjwnhzhf-1226766338419> [Accessed 20 April 2014]

Ritter, T. (2008). Password-sharing hinders probe into serious blunder. Article dated May 30. Available at <http://www.computerweekly.com/blogs/public-sector/2008/05/passwordsharing-hinders-probe.html>, [Accessed on 21/06/2012]

Robila, S. A., & Ragucci, J. W. (2006, June). Don't be a phish: steps in user education. In *ACM SIGCSE Bulletin* (Vol. 38, No. 3, pp. 237-241). ACM.

Robinson, N., Graux, H., Parrilli, D., Klautzer, L., & Valeri, L. (2011). Non legislative measures to combat identity theft and identity related crime: Final Report. *DG Home Affairs*, Rand, Europe.

Romanosky, S., Telang, R., & Acquisti, A. (2010). Do data breach disclosure laws reduce identity theft? 1-42.

Rosbrow, L (2014). How the Middle East is Solving the Gender Gap that Silicon Valley is Ignoring. *Policymic.com* <http://www.policymic.com/articles/86521/how-the-middle-east-is-solving-the-gender-gap-that-silicon-valley-is-ignoring> [Accessed 17 April 2014]

Rosen, J (2011). Universal Service Fund Reform: Expanding Broadband Internet Access in the United States <http://www.brookings.edu/research/papers/2011/04/universal-service-fund-rosen> [Accessed 16 April 2014]<http://www.brookings.edu/research/papers/2011/04/universal-service-fund-rosen>

Rouse, M (2005). *What is a security token*. 2005. <http://searchsecurity.techtarget.com/definition/security-token> [Accessed 7 April 2014]

Ryder, N. (2011). *Financial crime in the 21st century: Law and policy*. Northampton, MA: Edward Elgar Publishing.

SANS (2001). *History of Encryption*. <https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730> [Accessed 7 April 2014]

SANS (2012). Privileged Password Sharing: “root” of All Evil. A SANS Whitepaper written by J. Michael Butler, February.

Scheb, J., & Scheb II, J. (2011). *Criminal law*. NY: Cengage Learning.

Schlienger, T. and Teufel S. (2003): *Information Security Culture - The Socio-Cultural Dimension in Information Security Management*, Proceedings of the 14th International Workshop on Database and Expert Systems Applications, IEEE

Schroeder, N. J. (2005): Using Prospect Theory to Investigate Decision-Making Bias Within An Information Security Context, Air Force Institute Of Technology Wright-Patterson Air Force Base, Ohio

Science and Technology Committee (2007). Personal internet security. *House of Lords Science and Technology Committee*. 5th report of session 2006-07, HL paper 165-I.

Search Security (2010): *Forrester's Advice for Data Governance Maturity Model Success*, an interview with Forrester Research Senior Analyst Andrew Jaquith, available at http://searchsecurity.techtarget.com/video/0,297151,sid14_gci1522125,00.html?track=N L-431&ad=799181&asrc=EM_NLT_12908098&uid=10365888, accessed on [Accessed 11/11/2010]

Shaikh, S. A. (2004, October). Information security education in the UK: a proposed course in secure e-commerce systems. In *Proceedings of the 1st annual conference on Information security curriculum development* (pp. 53-58). ACM.

Sharma, S. K., & Sefchek, J. (2007). Teaching information systems security courses: A hands-on approach. *Computers & Security*, 26(4), 290-299.

Shubinsky, G. D., & Sobel, A. (2013). U.S. Patent Application 13/786,696.

Siddiqui, A., & Muntijir, M. (2013). A study of possible biometric solution to curb frauds in ATM transaction. *IJASCSE*, 2(2), 1-6.

Singh, S., Cabraal, A., & Hermansson, G. (2006, November). What is your husband's name?: sociological dimensions of internet banking authentication. In *Proceedings of the 18th Australia conference on Computer-Human Interaction: Design: Activities, Artefacts and Environments* (pp. 237-244). ACM.

Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., & Furlong, M. (2007, April). Password sharing: implications for security design based on social practice. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 895-904). ACM.

Siponen, M. and Willison, R. (2009): *Information security management standards: Problems and solutions*, Elsevier Information & Management, Volume 46, Issue 5, June, Pages 267-270

Six charged in connection with alleged internet dating scam (2014). *Theguardian.com*. <http://www.theguardian.com/uk-news/2014/feb/21/six-charged-connection-alleged-match-com-dating-site-fraud> [Accessed 20 April 2014]

Smart Card Alliance (2003). Privacy and secure identification systems: the role of smart cards as a privacy-enabling technology. *A Smart Card Alliance White Paper*, 1-34.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, 24(2), 124-133.

State Department Suffers Computer Break-in (2006) *usatoday.com*
http://usatoday30.usatoday.com/news/washington/2006-07-11-state-department_x.htm
[Accessed 15 April 2014]http://usatoday30.usatoday.com/news/washington/2006-07-11-state-department_x.htm

Stay Smart Online. [ONLINE] Available at: <http://www.staysmartonline.gov.au/>.
[Accessed 23 May 2014].

Stoneburner, G., Goguen, A. and Feringa, A. (2002): *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology Special Publication 800-30, 54 pages, July 2002

Stop.Think.Connect. Resource Guide. [ONLINE] Available at: <http://www.stcguide.com>.
[Accessed 23 May 2014].

Strauss, A., & Corbin, J. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (Second ed.). Sage Publications, Inc.

Taylor, J (2012). Aust govt dumps broad mandatory filter for Interpol block. *Zdnet.com*.

<http://www.zdnet.com/au/aust-govt-dumps-broad-mandatory-filter-for-interpol-block-7000007080/> [accessed 20 April 2014]

Taylor, J (2013).UK to automatically filter ‘adult’ internet content.” *Zdnet.com*.
<http://www.zdnet.com/uk/uk-to-automatically-filter-adult-internet-content-7000018403/>
[Accessed 20 April 2014]

Technology use in Australia (2013). *aifs.gov.au*
<http://www.aifs.gov.au/cfca/pubs/papers/a145634/04.html> [Accessed 16 April 2014]

Teddlie, C., & Tashakkori, A. (Eds.). (2009). *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences*. Sage Publications Inc.

Tejay, G. (2005): Making Sense of Information Systems Security Standards, AMCIS 2005 Proceedings

The White House (2011). International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.

The White House. The Comprehensive National Cybersecurity Initiative. [ONLINE] Available at: <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>. [Accessed 23 May 2014].

Thoburn, J. (2009): *The Impact of World Recession on the Textile and Garment Industries of Asia*, Working Paper, Research and Statistics Branch, United Nations Industrial Development Organization

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information management & computer security*,6(4), 167-173.

Tohmatsu, D. T. (2003). Global security survey. *New York, NY: Deloitte Touche Tohmatsu*.

Tornikoski, A. (2014). *The threat landscape*.http://www.f-secure.com/en/web/business_global/software-updater/threat-landscape. [Accessed 25 April 2014]

Tracy, R (2014). In a Cyber Breach, Who Pays, Banks or Retailers? *wsj.com*,
<http://online.wsj.com/news/articles/SB10001424052702303819704579316861842957106>

Tuna, F. Incekara, S. and Tunc, S. (2011): *Measuring High School Students’ Knowledge about Climate Change: A Case Study from Istanbul*, World Applied Sciences Journal 15 (2): 297-303, ISSN 1818-4952

Tung, L (2009).Mandatory ISP Filter due mid-2011. *Zdnet.com*.

<http://www.zdnet.com/mandatory-isp-filter-due-mid-2011-1339300060/> [Accessed 20 April 2014]

Twitchell, D. P. (2006, September). Social engineering in information assurance curricula. In *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 191-193). ACM.

UAE (2006). The Federal Law No. (2) of 2006 on The Prevention of Information Technology Crimes. Official Gazette of the United Arab Emirates, Volume 442, 36th year, Muharam 1427 H/ January 2006.

UAE E-Council (2010): *Strategy*, available at <http://ecouncil.ae/Sites/GSEC/Navigation/EN/EGovProgram/strategy,did=95774.html>, accessed on 25/11/2010

UAE Interact (2009): *New Department to Fight Cybercrimes*, an article dated 16/12/2009, available at http://www.uaeinteract.com/docs/New_department_to_fight_cyber_crimes/38792.htm, accessed on 09/11/2010

UNIDIR (2013). The Cyber Index: International Security Trends and Realities. United Nations Institute for Disarmament Research.

University of California (UC) Santa Cruz (2014). Security breach examples and practices to avoid them. *Information Technology Services*. Retrieved April 23, 2014, from <http://its.ucsc.edu/security/breaches.html>

UT Dallas News (2013). Corporate Executives Discuss Technology and its Effects on Corporate Culture . [ONLINE] Available at: http://www.utdallas.edu/news/2013/4/18-23221_Executives-Discuss-Technology-and-its-Effects-on-C_article-wide.html?WT.mc_id=NewsRSS [Accessed 14 June 2014]

Van Doom, P (2014). Barclays Data Breach Makes Target Look Tame. *Thestreet.com*, <http://www.thestreet.com/story/12325789/1/barclays-data-breach-makes-target-look-tame.html><http://www.thestreet.com/story/12325789/1/barclays-data-breach-makes-target-look-tame.html>

Verdasys (2011, January). Protecting Against WikiLeaks Events and the Insider Threat, *White Paper*.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, 24(2), 99-104.

Warren, M. J., & Leitch, S. (2006, December). Social Engineering and its Impact via the Internet. In *Australian Information Security Management Conference* (p. 85).

Web Users in the Middle East Emphasize Social Networking (2013). *emarketer.com*.
<http://www.emarketer.com/Article/Web-Users-Middle-East-Emphasize-Social-Networking/1010437> [Accessed 17 April 2014]

Werner, L. (2004): *Teaching Principled and Practical Information Security*, Consortium for Computing Sciences in Colleges, JCSC 20, 1 October

Wheeler, D. L. (2004): *The Internet in the Arab World: Digital Divides and Cultural Connections*. Lecture presented to the Royal Institute for Inter-Faith Studies, June 16

Wingens, M.; Windzio, M., De Valk; H. and Aybek, C. (2011): *A Life-Course Perspective on Migration and Integration*, Springer; 1st Edition

Wonnacott, T. H. & Wonnacott, R. J. (1990). *Introductory Statistics for Business and Economics*. John Wiley & Sons; 4th Edition.

Woodhouse, S. (2007): *Information Security: End User Behavior and Corporate Culture*, Seventh International Conference on Computer and Information Technology, IEEE

Woodward, J. D. (2001): *What Concerns Do Biometrics Raise and How Do they Differ from Concerns about other Identification Methods?* United States. Army, Arroyo Center, Army biometric applications: identifying and addressing sociocultural concerns, 2001

Wright, R (2006). State Dept. Probes Computer Attacks.*washingtonpost.com*.
<http://www.washingtonpost.com/wp-dyn/content/article/2006/07/11/AR2006071101032.html> [Accessed 15 April 2014]

WSJ (2014). Closed-Circuit TV Footage Shows London Bombers on Practice Run [ONLINE] Available at: <http://online.wsj.com/news/articles/SB112722720447846137>. [Accessed 14 June 2014].

Wu, H., Chou, C., Ke, H., and Wang, M. (2010): *College Students' Misunderstanding about Copyright Laws for Digital Library Resources*. *The electronic library*, 28(2), 197-209.

Wyatt, E (2014). 2 Regulators Issue Guidelines on Sharing cybersecurity Information.*nytimes.com*.
http://bits.blogs.nytimes.com/2014/04/10/2-regulators-issue-guidelines-on-sharing-cyber-security-information/?_php=true&_type=blogs&hpw&rref=technology&r=0 [Accessed 11 April 2014]

Yang, Y., Lutes, J., Li, F., Luo, B., & Liu, P. (2012, February). Stalking online: on user privacy in social networks. In *Proceedings of the second ACM conference on Data and Application Security and Privacy* (pp. 37-48). ACM.

Yusuf, H. (2003): *The Arab Region and the Digital Divide*, PC Magazine, 1 May

Zawaya (2010): *Computer Emergency Response Team Obtains ISO Certificate*, a web article dated 21/10/2010, available at <http://www.zawya.com/arabic/story.cfm/sidZAWYA20101021120533/lok120500101021>, [accessed on 27/11/2010]

Zhao, J. et al (2010): *Cognition and Culture in ICT Experience*, 11th International Conference on Parallel and Distributed Computing, Applications and Technologies, IEEE

APPENDIX 1

هل من الممكن ان يتشارك ما يلي		نعم
الزوج		
أفضل صديق خارج العمل		
الوالد / الجد		
الأبناء البالغون		
مدير الأصل		
الأخوة		
زميل موثوق / عضو فريق		
اولائك الصغار		
اقرباؤك		
أعضاء في نفس فريق العمل		
الاجراء عندك		
لشخص في مشروع اخبارهم قد يكون ضروريا		
محامي المؤسسة		
اشخاص ترغب بإثارة اعجابهم		
زملاء لاجتماع معين		
مجلة المؤسسة		
منافس محتمل		
موقعك الشخصي / بلوق		
موظف المبيعات (شخصيا أو على شبكة الانترنت)		
مختلفة عمل او مكتبها ولم يعلم احد بها		
كل محتوى بويك الإلكتروني		
رقم بطاقة الائتمان		
رقم الضمان الاجتماعي		
محاولة عمل محملة (على سبيل المثال استخدام الكمبيوتر للعمل الخيري)		
الاجل المتبقي لك من خارج العمل		
الراتب		
فصل شخصي كبير (إبرد من وظيفة أو طلاق)		
سلك سائق تعينه خطا		
قائمة الأصحاء في الموقع الاجتماعية		
مواقع الانترنت الغير متعلقة بالعمل والتي تستخدمها خلال الترام		
الحالة الاجتماعية		
تقويمات الأباء أو طفلي		
إرثك حول أشخاص آخرين		
طلبات تقدمت بها إلى وظيفة أخرى / جامعة		
لوجين إلى جهاز الكمبيوتر الشخصي مع ضامن عدم النظر إلى أي شيء		
فصل شخصي صغير (على سبيل المثال مشروع تعلم الخبز)		
مجموعات البريد الإلكتروني التي تنتمي إليها (خارج الشركة)		
سجل / ملخص لمعلوماتك في قاعدة البيانات		
التسجيلات (السيرة الذاتية وغيرها)		
وثائق ذات الصلة بالعمل تستخدمها		
الحالة الصحية		
مدخلاتك في دفتر التقويم (أموال، تحفيزات، الخ...)		
إذا كنت حاملا		
عمل تحت التفتيش		
موتير قمت به عبر الفيديو		
مواقع ذات الصلة بالعمل قمت بتصفحها		
الموقع الحالي (عبر التويتر على سبيل المثال)		
الوضع الراهن ("مستقل"، "مستقل") على اليرضة		
أوراق قيمة أو صيحات الجزية		
مجموعات البريد الإلكتروني التي تنتمي إليها (داخل الشركة)		
تجارتك شخصية صغيرة (على سبيل المثال متجر وطق للتراصة)		
عندما تكون متوقفا		
رقم هاتف المنزل		
تجارتك شخصية كبيرة (أزقة عالية)		
العمر		
رقم العوال		
رقم هاتف مكتبك في العمل		
عنوان بريد العمل الإلكتروني		

	Salesperson (live or web-based)	My personal website/blog	Potential or confirmed competitor	Company newsletter	People in an upcoming meeting	People I want to impress (e.g. hire, date)	Corporate lawyer	People in a project for whom it is relevant	People who work for me	Other team members	People in extended family	Young child of mine	Trusted colleague/team member	Sibling	My manager	Adult child of mine	Parent/grandparent	Best friend outside of work	Spouse
Transgression that is well understood to be wrong (e.g. accessing pornographic images on a work computer)																			
All of my email content																			
Credit card number																			
Social Security Number																			
A potential transgression -- action not universally understood as wrong, more in a grey area (e.g. using your work computer for charitable activities)																			
Outside income																			
Salary																			
Large personal failure (e.g. fired from previous job)																			
Personal behaviour I feel bad about (e.g. spoke sharply to a colleague)																			
Buddy list (who's on my list)																			
Non-work related websites I've looked at at work																			
Recent history of status (looking for trends)																			
History of my job performance scores																			
Opinions I have about other people (assume in digital form)																			
My application to another job/school																			
Access to my computer with personal assurance that they won't look at anything																			
Small personal failure (e.g. project missteps that led to failure)																			
What email groups I belong to (external to the company)																			
Record/summary of database interactions																			
Preferences (politics, religion, associates, etc.) (assume in digital form)																			
Work-related documents I've accessed																			
My health status																			
Specific calendar entries																			
Pregnancy status																			
Work in progress																			
Desktop video conference																			
Work-related websites I've looked at																			
Current location																			
Current status (on line, "busy") from IM																			
Past finished papers, products, etc.																			
What email groups I belong to (internal to the company)																			
Small personal success (e.g. project chosen to demo)																			
When available (on a shared calendar)																			
Home phone number																			
Large personal success (e.g. big promotion)																			
Age																			
Mobile number																			
Work desk phone number																			
Work email address																			

Qualitative Analysis: Interview Questions

1. Is the extent of protection provided by the security policies of the organisation as well as by following international standards in your opinion enough to prevent employees from sharing sensitive information with each other or to the outside of the organisation?
2. Are there any measures that can be taken along with policies and standards to further boost the role of information security?
3. Do you do awareness courses on the importance of information and its security in the organisation? If yes, who and what are these courses usually aimed at?
4. In your opinion, and by virtue of your experience in the organisation, do customs and traditions provide grounds for greater potential for sharing sensitive information? Have you encountered any case of the spread of sensitive information based on certain cultural traditions? How did you deal with such situations or how can you deal with it in case it happens?
5. By virtue of being involved with staff from diverse backgrounds and cultures, have you noticed obvious differences characterising Arab culture in terms of sharing sensitive information? Have there been any certain situations encountered?

APPENDIX 2

Questionnaire

Hypothesis: Arabs are prone to sharing information that is typically withheld

Are you willing to share the following information with close people (i.e. relative or close friends)?

1. Access to personal PC
 - a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
2. Work Email content
 - a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
3. Credit card details
 - a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
4. Work Email password
 - a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
5. Personal email password
 - a. Strongly agree

- b. Agree
- c. Neither agree nor disagree
- d. Disagree
- e. Strongly disagree

6. Confidential work information

- a. Strongly agree
- b. Agree
- c. Neither agree nor disagree
- d. Disagree
- e. Strongly disagree

7. Current location

- a. Strongly agree
- b. Agree
- c. Neither agree nor disagree
- d. Disagree
- e. Strongly disagree

8. Work-related documents

- a. Strongly agree
- b. Agree
- c. Neither agree nor disagree
- d. Disagree
- e. Strongly disagree

9. Personal mobile password

- a. Strongly agree
- b. Agree
- c. Neither agree nor disagree
- d. Disagree
- e. Strongly disagree

10. Access to work PC

- a. Strongly agree
- b. Agree
- c. Neither agree nor disagree
- d. Disagree
- e. Strongly disagree

11. Past finished work-related papers, products

- a. Strongly agree
- b. Agree
- c. Neither agree nor disagree
- d. Disagree
- e. Strongly disagree

12. Social media password (Facebook, Twitter)

- a. Strongly agree
- b. Agree
- c. Neither agree nor disagree
- d. Disagree
- e. Strongly disagree

13. Personal email content

- a. Strongly agree
- b. Agree
- c. Neither agree nor disagree
- d. Disagree
- e. Strongly disagree


14. Online banking details

- a. Strongly agree
- b. Agree
- c. Neither agree nor disagree
- d. Disagree
- e. Strongly disagree

Ethics form:

FACULTY OF CREATIVE ARTS, TECHNOLOGIES AND SCIENCE

Form for Research Ethics Projects (Ethics Form)

Student Name	Ahmed Alkaabi
Student Number	0813839
Degree Pathway	PhD
Supervisor name	Prof Carsten Maple
Supervisor Signature	
Title of project	Developing a Culture-based Information Security Strategy for Abu Dhabi

SECTION A Proposal

Please summarise in the research proposal (Screening Form) the ethical issues involved and how they will be addressed.

In any proposal involving human participants please provide information on how:

- **informed consent will be obtained**
- **confidentiality will be observed**
- **the nature of the research and the means of dissemination of the outcomes will be communicated to participants.**

SECTION B Check List

Please answer the following questions by circling **YES** or **NO** as appropriate.

Does the study involve vulnerable participants or those unable to give informed consent (e.g. children, people with learning disabilities, your own students)?	YES
	NO
Will the study require permission of a gatekeeper for access to participants (e.g. schools, self-help groups, residential homes)?	YES
	NO
Will it be necessary for participants to be involved without consent (e.g. covert observation in non-public places)?	YES
	NO
Will the study involve sensitive topics (e.g. obtaining information about sexual activity, substance abuse)?	YES
	NO
Will blood, tissue samples or any other substances be taken from participants?	YES
	NO
Will the research involve intrusive interventions (e.g. the administration of drugs, hypnosis, physical exercise)?	YES
	NO
Will financial or other inducements be offered to participants (except reasonable expenses or small tokens of appreciation)?	YES
	NO
Will the research investigate any aspect of illegal activity (e.g. drugs, crime, underage alcohol consumption or sexual activity)?	YES
	NO
Will participants be stressed beyond what is considered normal for them?	YES
	NO
Will the study involve participants from the NHS (patients or staff) or will data be obtained from NHS premises?	YES
	NO

If the answer to any of the questions above is “Yes”, or if there are any other significant ethical issues, then further ethical consideration is required. Please document carefully how these issues will be addressed.

Signed (student): Ahmed

Date: 2/7/2012

Countersigned (Supervisor): Professor Carsten Maple



Date: 4.7.12

APPENDIX 3

Questionnaire (English Version)

Information Security Awareness*

Please read the following carefully: يرجى قراءة ما يلي بعناية:

The aim of the study is to increase the awareness level of information security to prevent you from being a victim of computer crimes. The questionnaire in the second page requires you to identify the potential risks that result from certain actions.

Pressing Agree in the box below means you accept to participate in this questionnaire.

Please note the following points before you press Agree:

- No personal information will be obtained from you (your personal information, your school name, etc.)all data are anonymised
- Neither your teachers nor your parents or your classmates will have access to your answers
- Your participation in this research study is voluntary. You may choose not to participate or withdraw at any point by closing the page
- Your answers are very valuable to the researcher for further studies
- Your answer is protected and secured*

1. If you do not wish to participate in the research study, please decline participation by clicking on the "disagree" button.

The "disagree" button.

agree

I am you willing to share the following information with or allow access to close people (i.e. relative, close friends or friends of friends):

1. Access to a personal PC
 - a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
2. School email content
 - a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
3. School email password
 - a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
4. Personal email password
 - a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
5. Confidential school information, such as registration details, performance, etc.
 - a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
6. Current location, such as updates on social media websites
 - a. Strongly agree

- b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
7. School-related documents, such as transcripts, marks, performance, etc.
- a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
8. Personal mobile password
- a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
9. Access to school PC
- a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
10. Past school-related information, such as previous school marks, performance, etc.
- a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
11. Social media password (Facebook, Twitter)
- a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree

12. Personal email content
 - a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
13. Access to personal mobile phone
 - a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
14. Access to personal USB memory drive
 - a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree
15. Access to other personal mobile devices (laptop, tablet, PDA, etc.)
 - a. Strongly agree
 - b. Agree
 - c. Neither agree nor disagree
 - d. Disagree
 - e. Strongly disagree

Questionnaire (Arabic Version)

f. الهدف من هذه الدراسة هو زيادة مستوى الوعي بأمن المعلومات لحمايةك من أن تكون ضحية للجرائم الإلكترونية. الاستبيان في الصفحة الثانية يتطلب منك تحديد المخاطر المحتملة التي تنجم عن إجراءات معينة. الضغط اختياريك "أوفق" في المربع أدناه يعني أنك موافق على المشاركة في هذا الاستبيان

يرجى ملاحظة النقاط التالية قبل الضغط على أوفق

■ إن يتم الحصول على أية معلومات شخصية عنك مثل المعلومات الشخصية الخاصة بك، اسم مدرستك، الخ جميع المعلومات سوف تكون مجهولة الهوية
■ لا معلمك ولا والديك ولا زملائك في المدرسه سيعلمون ما هي إجاباتك
■ مشاركتك في هذه الدراسة البحثية طوعية. يمكنك اختيار عدم المشاركة أو الانسحاب في أي لحظة عن طريق إغلاق الصفحة
■ إجاباتك هي قيمة جدا لهذا البحث ولمزيد من الدراسات في المستقبل
■ سوف يتم المحافظة على إجاباتك من أي وصول لغير أغراض البحث

g. إذا كنت لا ترغب في المشاركة في هذه الدراسة البحثية، يرجى إختيار لا أوافق

● لا اوافق .

وافق

الاسئلة:

1. الدخول إلى جهاز الكمبيوتر الشخصي

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض

2. محتوى البريد الإلكتروني المدرسي :

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض

3. كلمة السر للبريد الإلكتروني المدرسي :

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض

4. كلمة السر للبريد الإلكتروني الشخصي :

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض

5. سرية المعلومات المدرسية مثل : تفاصيل التسجيل , الأداء , ..الخ.

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض

6. الموقع الحالي، مثل التحديثات على مواقع وسائل التواصل الاجتماعية (فيس بوك، تويتر، بلاك بيري مسنجر)

:

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض

7. الوثائق التي لها صلة بمدرستك ، مثل : النصوص ، العلامات ، الأداء ، ...الخ.

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض

8. كلمة السر للهاتف المحمول الشخصي :

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض

9. الدخول إلى كمبيوتر المدرسة الخاص بك :

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض

10. معلومات سابقه ذات صلة بمدرسك، مثل : علامات المدرسة السابقة ، الأداء ، .. الخ.

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض

11. كلمة السر لوسائل التواصل الاجتماعي، مثل : الفيسبوك وتويتر .

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض

12. محتوى البريد الإلكتروني الشخصي :

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض

.h

13. الدخول إلى الهاتف المحمول الشخصي :

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض

14. الدخول إلى ذاكرة التخزين الشخصية (USB) :

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض


i. 15. الدخول إلى غيرها من الأجهزة الشخصية، مثل : الكمبيوتر المحمول ، الأقراص ، ..الخ.

- أ- أوافق بشدة
- ب- أوافق
- ت- محايد
- ث- أعارض بشدة
- ج- أعارض

Ethics form

FACULTY OF CREATIVE ARTS, TECHNOLOGIES AND SCIENCE

Form for Research Ethics Projects (Ethics Form)

Student Name	Ahmed Alkaabi
Student Number	0813839
Degree Pathway	PhD
Supervisor name	Prof Carsten Maple
Supervisor Signature	
Title of project	Developing a Culture-based Information Security Strategy for Abu Dhabi

SECTION A Proposal

Please summarise in the research proposal (Screening Form) the ethical issues involved and how they will be addressed.

In any proposal involving human participants please provide information on how:

- **informed consent will be obtained**
- **confidentiality will be observed**
- **the nature of the research and the means of dissemination of the outcomes will be communicated to participants.**

SECTION B Check List

Please answer the following questions by circling **YES** or **NO** as appropriate.

Does the study involve vulnerable participants or those unable to give informed consent (e.g. children, people with learning disabilities, your own students)?	YES
	NO
Will the study require permission of a gatekeeper for access to participants (e.g. schools, self-help groups, residential homes)?	YES
	NO
Will it be necessary for participants to be involved without consent (e.g. covert observation in non-public places)?	YES
	NO
Will the study involve sensitive topics (e.g. obtaining information about sexual activity, substance abuse)?	YES
	NO
Will blood, tissue samples or any other substances be taken from participants?	YES
	NO
Will the research involve intrusive interventions (e.g. the administration of drugs, hypnosis, physical exercise)?	YES
	NO
Will financial or other inducements be offered to participants (except reasonable expenses or small tokens of appreciation)?	YES
	NO
Will the research investigate any aspect of illegal activity (e.g. drugs, crime, underage alcohol consumption or sexual activity)?	YES
	NO
Will participants be stressed beyond what is considered normal for them?	YES
	NO

Will the study involve participants from the NHS (patients or staff) or will data be obtained from NHS premises?	YES
	NO


If the answer to any of the questions above is “Yes”, or if there are any other significant ethical issues, then further ethical consideration is required. Please document carefully how these issues will be addressed.

The research involves surveying school students on sharing information and IT related material will be given to them. The researcher has obtained the permission of the relevant authority, Abu Dhabi Educational Council, to do the survey (Available upon request)

Signed (student): Ahmed

Date: 26/11/2012

Countersigned (Supervisor): Professor Carsten Maple

Date: 

Permission to do the study (Abu Dhabi Emirate)



التاريخ: 2012/7/29

السادة/ مدراء المدارس الحكومية في إمارة أبو ظبي

الموضوع: تسهيل مهمة باحثين

يطيب لنا أن نهدىكم أطيب التحيات.

ونود إعلامكم بموافقة مجلس أبو ظبي للتعليم على موضوع الدراسة التي سيجريها الباحث النقيب/ أحمد محمد راشد الكعبي، من القيادة العامة لشرطة أبو ظبي، بعنوان:

"استراتيجية أمن المعلومات لإمارة أبو ظبي"

لذا، يرجى التكرم بتسهيل مهمة الباحث ومساعدته على إجراء الدراسة المشار إليه.

شاكرين لكم حسن تعاونكم

محمد سالم محمد الظاهري

المدير التنفيذي لقطاع العمليات المدرسية



APPENDIX 4

Opened Ended Questionnaire (English Version)

Information Security Awareness*

Please read the following carefully: يرجى قراءة ما يلي بعناية:

The aim of the study is to increase the awareness level of information security to prevent you from being a victim of computer crimes. The questionnaire in the second page requires you to identify the potential risks that result from certain actions. Pressing Agree in the box below means you accept to participate in this questionnaire. Please note the following points before you press Agree:

- No personal information will be obtained from you (your personal information, your school name, etc.)all data are anonymised
- Neither your teachers nor your parents or your classmates will have access to your answers
- Your participation in this research study is voluntary. You may choose not to participate or withdraw at any point by closing the page
- Your answers are very valuable to the researcher for further studies
- Your answer is protected and secured

*

1. If you do not wish to participate in the research study, please decline participation by clicking on the "disagree" button.

The "disagree" button.

agree

Questions

1. May all information be shared with friends and relatives?

a. Yes, because

- b. No, because
 - c. Not sure because.....
- 2. **Would you share your email password with a friend?**
 - a. Yes, because
 - b. No, because
 - c. Not sure because.....
- 3. **Would you share your email content with a friend if requested?**
 - a. Yes, because
 - b. No, because
 - c. Not sure because.....
- 4. **Would you share your sensitive information with a friend that you met in social media website (i.e. Facebook, twitter, chatting website) but not in person?**
 - a. Yes, because
 - b. No, because
 - c. Not sure because.....
- 5. **Would you allow access to your personal computer that contains sensitive information to a friend or relative if requested?**
 - a. Yes, because
 - b. No, because
 - c. Not sure because.....
- 6. **Would you allow access to your phone to a friend or relative if requested?**
 - a. Yes, because
 - b. No, because
 - c. Not sure because.....
- 7. **Can it be serious consequences sharing sensitive information with others?**
 - a. Yes, because
 - b. No, because
 - c. Not sure because.....
- 8. **Generally, is it safe to share your email content with close people you believe that they will not divulge it?**
 - a. Yes, because
 - b. No, because
 - c. Not sure because.....

9. If there is an urgent matter, would you give your password to a trusted person to access your computer?
- a. Yes, because
 - b. No, because
 - c. Not sure because.....
10. Would you regularly tell where you are in your social media accounts?
- a. Yes, because
 - b. No, because
 - c. Not sure because.....
11. Would you give access to your Facebook to a person you trust?
- a. Yes, because
 - b. No, because
 - c. Not sure because.....
12. Would you give your email password to a person you trust?
- a. Yes, because
 - b. No, because
 - c. Not sure because.....
13. In case you shared your account password with someone, will you change it later on?
- a. Yes, because
 - b. No, because
 - c. Not sure because.....
14. Do you have different passwords for different accounts?
- a. Yes, because
 - b. No, because
 - c. Not sure because.....
15. Do you lend your USB flash memory to a friend if requested without checking whether it has sensitive information stored?
- a. Yes, because
 - b. No, because
 - c. Not sure because.....
16. Do you have your password(s) written somewhere?
- a. Yes, because
 - b. No, because

c. Not sure because.....

17. Have you ever given your password of any account to someone?

a. Yes, with.....

b. No, because

c. Not sure because.....

18. Are you careful when you open email attachments about who the sender is?

a. Yes, because

b. No, because

c. Not sure because.....

19. Do you have any email or other Internet accounts you share with others (i.e. sibling, friend, parent)?

a. Yes, I sharewith.....

b. No, because

c. Not sure because.....

20. Do you share any instant messenger's passwords with others?

a. Yes, because

b. No, because

c. Not sure because.....

Open Ended Questionnaire (Arabic Version)

الهدف من هذه الدراسة هو زيادة مستوى الوعي بأمن المعلومات لحمايتك من أن تكون ضحية للجرائم الإلكترونية. الاستبيان في الصفحة الثانية يتطلب منك تحديد المخاطر المحتملة التي تنجم عن إجراءات معينة. الضغط اختيارك اختيارك "أوافق" في المربع أدناه يعني أنك موافق على المشاركة في هذا الاستبيان

يرجى ملاحظة النقاط التالية قبل الضغط على أوافق

■ لن يتم الحصول على أية معلومات شخصية عنك مثل المعلومات الشخصية الخاصة بك، اسم مدرستك، الخ جميع المعلومات سوف تكون مجهولة الهوية
■ لا معلمك ولا والديك ولا زملائك في المدرسه سيعلمون ما هي إجاباتك
■ مشاركتك في هذه الدراسة البحثية طوعية. يمكنك اختيار عدم المشاركة أو الانسحاب في أي لحظة عن طريق إغلاق الصفحة
■ إجاباتك هي قيمة جدا لهذا البحث ولمزيد من الدراسات في المستقبل
■ سوف يتم المحافظة على إجاباتك من أي وصول لغير أغراض البحث

إذا كنت لا ترغب في المشاركة في هذه الدراسة البحثية، يرجى إختيار لا أوافق

لا اوافق .

اوافق

الاسئلة:

1. هل جميع المعلومات يمكن تبادلها مع الأصدقاء والأقارب ؟

أ. نعم ، بسبب

ب. لا ، بسبب

ج. غير متأكد ، بسبب

2. هل تشارك وتبادل كلمة السر لبريدك الإلكتروني مع صديق ؟

أ. نعم ، بسبب

ب. لا ، بسبب

ج. غير متأكد ، بسبب

3. هل تشارك محتوى البريد الإلكتروني الخاص بك مع صديق إذا طلب منك ؟

أ. نعم ، بسبب

- ب. لا ، بسبب
- ج. غير متأكد ، بسبب
4. هل تتبادل المعلومات الحساسة الخاصة بك مع صديق اجتمعت وتعرفت عليه من خلال مواقع الاتصال الاجتماعي (الفيسبوك وتويتر ، ومواقع الدردشة) ؟
- أ. نعم ، بسبب
- ب. لا ، بسبب
- ج. غير متأكد ، بسبب
5. هل تسمح لصديق أو قريب إذا طلب منك للدخول إلى جهاز الكمبيوتر الشخصي الخاص بك الذي يحتوي على معلومات حساسة ؟
- أ. نعم ، بسبب
- ب. لا ، بسبب
- ج. غير متأكد ، بسبب
6. هل تسمح لصديق أو قريب إذا طلب منك للدخول إلى الهاتف الخاص بك ؟
- أ. نعم ، بسبب
- ب. لا ، بسبب
- ج. غير متأكد ، بسبب
7. بشكل عام، هل يعتبر خطراً إذا قمت بتبادل المعلومات الحساسة مع الآخرين ؟
- أ. نعم ، بسبب
- ب. لا ، بسبب
- ج. غير متأكد ، بسبب
8. بشكل عام، هل هو آمن لمشاركة محتوى البريد الإلكتروني الخاص بك مع أناس تثق بهم ؟
- أ. نعم ، بسبب
- ب. لا ، بسبب
- ج. غير متأكد ، بسبب

9. إذا كان هناك مسألة ملحه وأمرأ عاجل ، هل تعطي كلمة السر لشخص موثوق به للوصول إلى جهاز الكمبيوتر الخاص بك ؟

- أ. نعم ، بسبب
- ب. لا ، بسبب
- ج. غير متأكد ، بسبب

10. هل تقول دائماً أنه لديك حساب في مواقع الاتصال الاجتماعي ؟

- أ. نعم ، بسبب
- ب. لا ، بسبب
- ج. غير متأكد ، بسبب

11. هل تسمح لشخص تثق به للدخول إلى حساب الفيسبوك الخاص بك ؟

- أ. نعم ، بسبب
- ب. لا ، بسبب
- ج. غير متأكد ، بسبب

12. هل تعطي كلمة السر للبريد الإلكتروني الخاص بك إلى شخص تثق به ؟

- أ. نعم ، بسبب
- ب. لا ، بسبب
- ج. غير متأكد ، بسبب

13. في حال كنت تتشارك كلمة السر لحسابك مع شخص آخر ، هل سوف تقوم بتغيير كلمة السر في وقت لاحق ؟

- أ. نعم ، بسبب
- ب. لا ، بسبب
- ج. غير متأكد ، بسبب

14. هل لديك كلمات مرور مختلفة لحسابات مختلفة ؟

- أ. نعم ، بسبب
- ب. لا ، بسبب
- ج. غير متأكد ، بسبب

15. هل تعطي ذاكرتك(الفلاش USB) إلى أحد الأصدقاء إذا طلب منك دون التحقق إذا كان بها معلومات حساسة وخاصة مخزنة ؟

أ. نعم ، بسبب

ب. لا ، بسبب

ج. غير متأكد ، بسبب

16. هل لديك كلمة السر الخاصة بك مكتوبة في مكان ما ؟

أ. نعم ، بسبب

ب. لا ، بسبب

ج. غير متأكد ، بسبب

17. هل قمت بإعطاء كلمة السر الخاص بك لأي حساب في أي وقت كان لأي شخص ؟

أ. نعم ، بسبب

ب. لا ، بسبب

ج. غير متأكد ، بسبب

18. هل أنت حذر عندما تقوم بفتح مرفقات البريد الإلكتروني ؟

أ. نعم ، بسبب

ب. لا ، بسبب

ج. غير متأكد ، بسبب

19. هل لديك أي بريد إلكتروني أو حسابات انترنت أخرى مشتركة ؟

أ. نعم ، بسبب

ب. لا ، بسبب

ج. غير متأكد ، بسبب

20. هل تبادلت كلمات السر لأي مراسلات فورية مع الآخرين ؟

أ. نعم ، بسبب

ب. لا ، بسبب

ج. غير متأكد ، بسبب

APPENDIX 5

Course Material:

CONTENT

- * What is information.
- * Types of information
- * Information Sharing.
- * Sensitive Information.
- * Private information.
- * Sensitive Private Information.
- * What happens if sensitive information is shared?
- * Further Consequences

Information Security

أمن المعلومات

Types of Information and Information Sharing

أنواع المعلومات ومشاركة المعلومات

What is Information?

- * Information: is a valuable asset for individuals as well as organisations.
- * Information is used in everyday life without even knowing. For example: you use information when you call a phone number, when you tell the taxi driver an address.

* المعلومات هي أحد الأصول القيمة للأفراد وكذلك المنظمات.

* تستخدم المعلومات في الحياة اليومية حتى من دون معرفة ذلك. مثال: عند الاتصال برقم هاتف فانت تستخدم المعلومات ، كذلك عندما تقول لسائق سيارة أجرة عنوانك.

Types of Information

- * Some information is for daily use, Such as phone numbers, email addresses, and web addresses.
- * Certain information is called sensitive because it should be only known by certain people.
- * Information should be kept protected from being accessed by unauthorised people.

* بعض المعلومات للاستخدام اليومي. مثل أرقام الهواتف وعناوين البريد الإلكتروني وعناوين المواقع الإلكترونية.

* المعلومات الحساسة لأنه يفترض أن تُعرف فقط من قبل بعض الناس.

* ولذلك ينبغي أن تبقى مثل هذه المعلومات محمية من الوصول إليها من قبل الأشخاص غير المصرح له.

Information Sharing

- * Some information can be shared because it is necessary to share it.
- * Necessity depends on the situation, for example:
 - * Given your email address to your friend so he/she can send you emails.
 - * Given your home address to the taxi driver so he can drive you there.
 - * Given your home address to the school so they can send you letters.

- * احيانا يتم تبادل ومشاركة بعض المعلومات بين الناس لانه أمر ضروري.
- * وهذه الضرورة تعتمد على الموقف، على سبيل المثال :
 - * أن تعطي عنوان بريدك الإلكتروني لصديقك حتى يتمكن أن يرسل لك رسائل عن طريقه.
 - * أن تعطي عنوان منزلك إلى سائق سيارة أجرة حتى يتمكن من إيصالك إلى المنزل.
 - * أن تعطي المدرسة عنوان منزلك حتى يتمكنوا من إرسال رسائل لك.

So certain information may be shared with certain people in certain situations

إذا يمكن تبادل بعض المعلومات مع بعض الناس في حالات معينة.

Sensitive Information

- * What about sensitive information?
- * Should you share sensitive information with certain people in certain situations?
- * What is considered sensitive information?
- * Information is called sensitive when it might cause harm to the original owner in case it is disclosed.

- * ماذا عن المعلومات الحساسة ؟
- * هل يجب عليك تبادل ومشاركة المعلومات الحساسة مع بعض الناس في حالات معينة ؟
- * ما هي المعلومات التي تعتبر معلومات حساسة ؟
- * تسمى المعلومات حساسة اذا كانت ستسبب ضرراً للمالك الأصلي في حالة الكشف عنها.

Private Information

- * Information about you is called private information. This includes your age, your home address, etc.
- * You may need to share private information with some people in some situations.

- * المعلومات التي تكون عنك تسمى المعلومات الخاصة ، وتشمل عمرك ، عنوان منزلك ، ... الخ
- * قد تحتاج لتبادل ومشاركة المعلومات الخاصة بك مع بعض الناس في بعض الحالات.

Sensitive Private Information

- * Some private information can be sensitive
 - * For example, your password to your email, your pin code for your credit card and your login details to your computer
- * Sensitive private information should be kept to yourself.

* بعض المعلومات الخاصة يمكن أن تكون حساسة.

* على سبيل المثال : كلمة السر لبريدك الإلكتروني ، الرقم السري لبطاقة الائتمان الخاصة بك ، وتفاصيل تسجيل الدخول إلى جهاز الكمبيوتر الخاص بك.

* ينبغي أن تُبقي المعلومات الخاصة الحساسة لنفسك.

What happens if sensitive private information is shared?

- * There are different risks associated with sharing sensitive private information. For example:
 - * Sharing your computer password laptop/ mobile or iPad can cause:
 1. Accessing sensitive information stored on your system.
 2. Disclosing sensitive information stored on your system.
 3. Modifying or delete information stored on your system.
 4. Changing your password to stop you from accessing your device.
 - * Sharing you account passwords in Hotmail/Yahoo/Gmail/Facebook or Twitter may cause:
 - * Identity theft (someone pretends to be you)

* هناك مخاطر مختلفة مرتبطة بتبادل المعلومات الخاصة الحساسة. على سبيل المثال:

* تبادل كلمة السر للكمبيوتر الخاص بك، لأي باد أو الهاتف ، وهذا قد يسبب :

1. الوصول إلى المعلومات الحساسة المخزنة على النظام الخاص بك.

2. الكشف عن المعلومات الحساسة المخزنة على النظام الخاص بك.

3. تعديل أو حذف المعلومات المخزنة على النظام الخاص بك.

4. تغيير كلمة المرور الخاصة بك لإيقافك من الوصول إلى جهازك.

* تتبادل كلمة السر للحسابات الهوتميل أو ياهو أو جوجل أو الفيسبوك أو تويتر ، وهذا يسبب :

* سرقة الهوية (شخص يدعي أنه أنت)

Further Consequences

- * Sharing a password can be even more dangerous than you think.
- * For example:
 1. If you use the same password for your computer and email account.
 2. Knowing your password's selection style can help in guessing your other passwords. For example: phone number, date of birth, etc.

* تبادل ومشاركة كلمة السر يمكن أن يكون أكثر خطورة مما كنت تعتقد.

* على سبيل المثال:

1. ربما أنك تستخدم نفس كلمة السر لكمبيوترك الشخصي و حساب البريد الإلكتروني.
2. نمط كلمة السر يمكن أن يساعد في تخمين كلمات السر الأخرى الخاصة بك، على سبيل المثال: رقم هاتفك، تاريخ ميلادك،... الخ.

Conclusion

- * Information is important and is everywhere.
- * We use and share information all the time.
- * Some information has to be shared in order to allow people do tasks for us.
- * Some information may be shared sometime for necessity.
- * Some information is private, but may be shared in certain situations.
- * Some information are private and sensitive and should not be shared with anyone.

- * المعلومات مهمة وموجودة في كل مكان.
- * نحن نستخدم ونتبادل المعلومات في كل وقت.
- * بعض المعلومات يمكن أن تتبادل وتتشارك مع بعض الناس للقيام بمهام من أجلنا.
- * بعض المعلومات يمكن أن تتبادل في بعض الأوقات وذلك عند الضرورة.
- * بعض المعلومات خاصة، ولكن قد نتبادلها في حالات معينة.
- * بعض المعلومات خاصة وحساسة ، لذلك ينبغي أن لا نتبادلها مع أي شخص.

Answers (English Version)

3. May all information be shared with friends and relatives?

No, only certain information can be shared. This depends on the type of information and necessity of sharing it.

4. Would you share your email password with a friend?

No, as above, in any normal case, my friend does need my email password.

5. Would you share your email content with a friend if requested?

No, my email content is intended to me. If any content is for sharing, I may forward the email.

6. Would you share your sensitive information with a friend that you met in social media website (i.e. Facebook, twitter, chatting website)?

No, sensitive information should not be shared with those who unauthorised to have it.

7. Would you allow access to your personal computer that contains sensitive information to a friend or relative if requested?

No, sensitive information should not be shared with those who unauthorised to have it.

8. Would you allow access to your phone to a friend or relative if requested?

Yes, for making a call but not leave the phone with them.

9. Can there be serious consequences of sharing sensitive information with others?

Yes, (Slides 9, 10, 11)

10. Generally, is it safe to share your email content with people you trust?

No, because if you trust some people with some information, any threat happens to their information will happen to yours as well. (More details Slides 9, 10, 11)

11. If there is an urgent matter, would you give your password to a trusted person to access your computer?

Usually no, but discretion is used to assess urgency. If this happens, the password needs to be changed at the earliest opportunity

12. Would you regularly tell where you are in your social media accounts?

No. This may lead to stalking, robbing, privacy compromise, etc.

13. Would you give access to your Facebook to a person you trust?

No, accessing Facebook is of no interest other than the profile owner. Even though Facebook profile may contain no sensitive information, giving access may lead to many issues.

14. Would you give your email password to a person you trust?

No, the password should not be given to anyone other than the account holder (More details Slides 9, 10, 11).

15. In case you shared your account password with someone, will you change it later on?

Yes, but I wouldn't initially share it.

16. Do you have different passwords for different accounts?

Yes, it is important to have different passwords for different accounts. If one account is compromised, the other can still be protected.

17. Would you lend your USB flash memory to a friend if requested without checking whether it has sensitive information stored?

No, because I would not know what would happen to it. Even if I trust the friend, the flash memory might be lost or stolen.

18. Do you have your password(s) written somewhere?

No, I memorise passwords because writing them might lead to that someone finds them

19. Have you ever given your password of any account to someone?

No, passwords should never be given to anyone.

20. Are you careful when you open email attachments?

Yes, because these attachments may have hacking scripts or malicious software which would compromise the stored information.

21. Do you have any shared email or other Internet accounts?

No, all accounts I have are mine.

22. Do you share any instant messenger's passwords with others?

No, any password should never be given to anyone.

Answers (Arabic Version)

3. هل يمكن تبادل المعلومات الحساسة مع الأصدقاء والأقارب ؟
لا ، يمكن تبادل معلومات معينة فقط ، وهذا يعتمد على نوع المعلومات وضرورة تبادلها .
4. هل تتشارك كلمة السر للبريد الإلكتروني مع صديق ؟
لا ، على النحو الوارد أعلاه ، وفي أي حالة صديقي لا حاجة له لمعرفة كلمة السر للبريد الإلكتروني الخاص بي .
5. هل تتشارك محتوى البريد الإلكتروني الخاص بك مع صديق إذا طلب منك ؟
لا ، فمحتوى البريد الإلكتروني خاص بي وأنا المقصود به ، إذا فأني محتوي كان للتبادل سوف أقوم بإعادة توجيه البريد الإلكتروني.
6. هل تتبادل المعلومات الحساسة الخاصة بك مع صديق اجتمعت وتعرفت عليه من خلال مواقع الاتصال الاجتماعي (الفيسبوك وتويتر ، ومواقع الدردشة) ؟
لا ، لا ينبغي أن نتبادل معلومات حساسة مع أولئك الأشخاص الذين غير مصرح لهم بمعرفتها .
7. هل تسمح لصديق أو قريب إذا طلب منك للدخول إلى جهاز الكمبيوتر الشخصي الخاص بك الذي يحتوي على معلومات حساسة ؟
لا ، لا ينبغي أن نتبادل معلومات حساسة مع أولئك الأشخاص الذين غير مصرح لهم بمعرفتها .
8. هل تسمح لصديق أو قريب إذا طلب منك للدخول إلى الهاتف الخاص بك ؟
نعم ، لإجراء مكالمة ولكن لا أترك الهاتف معهم .
9. يمكن أن تكون هناك عواقب وخيمة من تبادل المعلومات الحساسة مع الآخرين ؟
نعم ، (شرائح 9 ، 10 ، 11)
10. هل هو آمن لمشاركة محتوى البريد الإلكتروني الخاص بك مع أناس تثق بهم ؟
لا ، لأنه إذا كنت تثق في بعض الناس لبعض المعلومات ، فأني تهديد يحدث لمعلوماتهم سوف يحدث لك كذلك . (لمزيد من التفاصيل الشرائح 9 ، 10 ، 11).
11. إذا كان هناك مسألة ملحة وأمرأ عاجل ، هل تعطي كلمة السر لشخص موثوق به للوصول إلى جهاز الكمبيوتر الخاص بك ؟
عادة لا ، ولكن يتم تقدير الوضع لتقييم الاستعجال. إذا حدث هذا ، نحتاج إلى تغيير كلمة المرور في أقرب فرصة ممكنة .
12. هل تقول دائماً أنه لديك حساب في مواقع الاتصال الاجتماعي ؟

لا ، فهذا قد يؤدي إلى المطاردة، والسرقه ، وسطو الخصوصية أي تعرضها للخطر ، الخ

13. هل تسمح لشخص تثق به للدخول إلى حساب الفيسبوك الخاص بك ؟

لا ، فالأكثر خطراً لسماح الآخرين لدخول الفيسبوك هو الدخول على المعلومات الشخصية ، على الرغم من ملف التعريف للفيسبوك قد لا يحتوي على معلومات حساسة ، ولكن الدخول والوصول إليه قد يؤدي إلى العديد من القضايا.

14. هل تعطي كلمة السر للبريد الإلكتروني الخاص بك إلى شخص تثق به ؟

لا ، لا ينبغي أن تعطى كلمة المرور إلى أي شخص غير صاحب الحساب (مزيد من التفاصيل الشرائح 9 ، 10 ، 11).

15. في حال كنت تتشارك كلمة السر لحسابك مع شخص آخر ، هل سوف تقوم بتغيير كلمة السر في وقت لاحق ؟

نعم ، لكنني لن أتبادلته منذ بداية الأمر .

16. هل لديك كلمات مرور مختلفة لحسابات مختلفة ؟

نعم ، فمن المهم أن تكون كلمات المرور مختلفة لحسابات مختلفة ، فإذا تم اختراق حساب واحد ، فالأخرى لا تزال محمية.

17. هل تعطي ذاكرتك (الفاش USB) إلى أحد الأصدقاء إذا طلب منك دون التحقق إذا كان بها معلومات حساسة وخاصة مخزنة؟

لا ، لأنني لا أعرف ما الذي سيحدث لها ، حتى لو كنت أثق في الصديق ، فقد يتم فقدان الفلاش أو سرقة.

18. هل لديك كلمة السر الخاصة بك مكتوبة في مكان ما ؟

لا ، أنا أحفظ كلمات السر لأنه كتابتها قد يؤدي إلى أن شخصاً ما قد يجدها .

19. هل قمت بإعطاء كلمة السر الخاص بك لأي حساب في أي وقت كان لأي شخص ؟

لا ، لا ينبغي أبداً أن تعطى كلمات السر إلى أي شخص .

20. هل أنت حذر عندما تقوم بفتح مرفقات البريد الإلكتروني ؟

نعم ، لأن هذه المرفقات قد يكون بها نصوص القرصنة أو برامج ضارة التي من شأنها أن تؤثر سلباً على المعلومات المخزنة.

21. هل لديك أي بريد إلكتروني أو حسابات انترنت أخرى مشتركة ؟

لا ، جميع الحسابات التي لدي هي لي .

22. هل تبادلت كلمات السر لأي مراسلات فورية مع الآخرين ؟

لا ، لا ينبغي أبداً أن تعطى أي كلمة السر لأحد.

APPENDIX 6

Categories for Individual Questions

3. May all information be shared with friends and relatives?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	15	7
Differentiation between different accounts	12	4
Necessity of keeping good relationships with friends and relatives	4	16
Necessity of helping others	6	14
Depending on the situation and at the discretion of the respondent	12	5
Awareness of risks and outcomes of cybercrimes	11	8
Importance for relatives and friends to check on the respondent	7	17
Belief that friends and relatives will not harm the respondent	7	14
Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	14	9
Carefulness with online activities	12	6

4. Would you share your email password with a friend?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	12	7
Differentiation between different accounts	13	10
Necessity of keeping good relationships with friends and relatives	9	23
Necessity of helping others	2	12
Depending on the situation and at the discretion of the respondent	16	14
Awareness of risks and outcomes of cybercrimes	15	4
Importance for relatives and friends to check on the respondent	2	4
Belief that friends and relatives will not harm the respondent	6	8
Passwords are protected (i.e. passwords not shared, different passwords for	12	10

different accounts)		
Carefulness with online activities	13	8

5. Would you share your email content with a friend if requested?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	14	8
Differentiation between different accounts	15	6
Necessity of keeping good relationships with friends and relatives	4	15
Necessity of helping others	3	20
Depending on the situation and at the discretion of the respondent	12	10
Awareness of risks and outcomes of cybercrimes	11	9
Importance for relatives and friends to check on the respondent	5	9
Belief that friends and relatives will not harm the respondent	7	12
Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	12	6
Carefulness with online activities	17	5

6. Would you share your sensitive information with a friend that you met in social media website (i.e. Facebook, twitter, chatting website)?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	11	4
Differentiation between different accounts	23	6
Necessity of keeping good relationships with friends and relatives	2	16
Necessity of helping others	2	14
Depending on the situation and at the discretion of the respondent	12	10
Awareness of risks and outcomes of cybercrimes	11	8
Importance for relatives and friends to check on the respondent	8	11
Belief that friends and relatives will not harm the respondent	10	12
Passwords are protected (i.e. passwords	10	9

not shared, different passwords for different accounts)		
Carefulness with online activities	11	10

7. Would you allow access to your personal computer that contains sensitive information to a friend or relative if requested?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	10	6
Differentiation between different accounts	11	5
Necessity of keeping good relationships with friends and relatives	7	13
Necessity of helping others	2	15
Depending on the situation and at the discretion of the respondent	14	7
Awareness of risks and outcomes of cybercrimes	14	5
Importance for relatives and friends to check on the respondent	7	23
Belief that friends and relatives will not harm the respondent	9	17
Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	12	4
Carefulness with online activities	14	5

8. Would you allow access to your phone to a friend or relative if requested?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	12	5
Differentiation between different accounts	15	12
Necessity of keeping good relationships with friends and relatives	9	15
Necessity of helping others	3	14
Depending on the situation and at the discretion of the respondent	14	8
Awareness of risks and outcomes of cybercrimes	14	6
Importance for relatives and friends to check on the respondent	1	15
Belief that friends and relatives will not harm the respondent	6	14
Passwords are protected (i.e. passwords	12	5

not shared, different passwords for different accounts)		
Carefulness with online activities	14	6

9. Can there be serious consequences of sharing sensitive information with others?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	12	8
Differentiation between different accounts	11	9
Necessity of keeping good relationships with friends and relatives	3	12
Necessity of helping others	8	19
Depending on the situation and at the discretion of the respondent	17	2
Awareness of risks and outcomes of cybercrimes	14	9
Importance for relatives and friends to check on the respondent	7	15
Belief that friends and relatives will not harm the respondent	5	17
Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	11	4
Carefulness with online activities	12	5

10. Generally, is it safe to share your email content with people you trust?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	11	5
Differentiation between different accounts	11	8
Necessity of keeping good relationships with friends and relatives	8	16
Necessity of helping others	8	9
Depending on the situation and at the discretion of the respondent	12	9
Awareness of risks and outcomes of cybercrimes	14	10
Importance for relatives and friends to check on the respondent	7	20
Belief that friends and relatives will not harm the respondent	8	11
Passwords are protected (i.e. passwords	10	6

not shared, different passwords for different accounts)		
Carefulness with online activities	11	6

11. If there is an urgent matter, would you give your password to a trusted person to access your computer?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	13	3
Differentiation between different accounts	18	8
Necessity of keeping good relationships with friends and relatives	8	15
Necessity of helping others	4	19
Depending on the situation and at the discretion of the respondent	12	8
Awareness of risks and outcomes of cybercrimes	14	10
Importance for relatives and friends to check on the respondent	2	10
Belief that friends and relatives will not harm the respondent	2	12
Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	12	8
Carefulness with online activities	15	7

12. Would you regularly tell where you are in your social media accounts?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	15	9
Differentiation between different accounts	14	6
Necessity of keeping good relationships with friends and relatives	4	16
Necessity of helping others	4	12
Depending on the situation and at the discretion of the respondent	13	4
Awareness of risks and outcomes of cybercrimes	15	9
Importance for relatives and friends to check on the respondent	1	19
Belief that friends and relatives will not harm the respondent	5	12
Passwords are protected (i.e. passwords	15	5

not shared, different passwords for different accounts)		
Carefulness with online activities	14	8

13. Would you give access to your Facebook to a person you trust?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	12	12
Differentiation between different accounts	13	5
Necessity of keeping good relationships with friends and relatives	4	13
Necessity of helping others	9	14
Depending on the situation and at the discretion of the respondent	13	5
Awareness of risks and outcomes of cybercrimes	11	7
Importance for relatives and friends to check on the respondent	7	14
Belief that friends and relatives will not harm the respondent	8	16
Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	12	5
Carefulness with online activities	11	9

14. Would you give your email password to a person you trust?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	12	7
Differentiation between different accounts	11	5
Necessity of keeping good relationships with friends and relatives	6	12
Necessity of helping others	7	14
Depending on the situation and at the discretion of the respondent	12	12
Awareness of risks and outcomes of cybercrimes	13	6
Importance for relatives and friends to check on the respondent	8	13
Belief that friends and relatives will not harm the respondent	6	16

Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	12	7
Carefulness with online activities	13	8

15. In case you shared your account password with someone, will you change it later on?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	17	12
Differentiation between different accounts	15	9
Necessity of keeping good relationships with friends and relatives	4	17
Necessity of helping others	3	12
Depending on the situation and at the discretion of the respondent	12	3
Awareness of risks and outcomes of cybercrimes	12	9
Importance for relatives and friends to check on the respondent	6	12
Belief that friends and relatives will not harm the respondent	6	14
Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	12	8
Carefulness with online activities	13	4

16. Do you have different passwords for different accounts?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	12	5
Differentiation between different accounts	14	6
Necessity of keeping good relationships with friends and relatives	9	12
Necessity of helping others	5	16
Depending on the situation and at the discretion of the respondent	16	7
Awareness of risks and outcomes of cybercrimes	11	6
Importance for relatives and friends to check on the respondent	5	25

Belief that friends and relatives will not harm the respondent	2	13
Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	12	6
Carefulness with online activities	14	4

17. Would you lend your USB flash memory to a friend if requested without checking whether it has sensitive information stored?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	13	9
Differentiation between different accounts	11	10
Necessity of keeping good relationships with friends and relatives	8	15
Necessity of helping others	9	12
Depending on the situation and at the discretion of the respondent	15	9
Awareness of risks and outcomes of cybercrimes	13	4
Importance for relatives and friends to check on the respondent	6	9
Belief that friends and relatives will not harm the respondent	2	17
Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	11	8
Carefulness with online activities	12	7

18. Do you have your password(s) written somewhere?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	9	10
Differentiation between different accounts	12	3
Necessity of keeping good relationships with friends and relatives	2	9
Necessity of helping others	3	15
Depending on the situation and at the discretion of the respondent	17	6
Awareness of risks and outcomes of cybercrimes	16	5

Importance for relatives and friends to check on the respondent	6	18
Belief that friends and relatives will not harm the respondent	6	25
Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	13	4
Carefulness with online activities	16	5

19. Have you ever given your password of any account to someone?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	11	9
Differentiation between different accounts	13	8
Necessity of keeping good relationships with friends and relatives	3	16
Necessity of helping others	7	12
Depending on the situation and at the discretion of the respondent	15	4
Awareness of risks and outcomes of cybercrimes	14	10
Importance for relatives and friends to check on the respondent	10	17
Belief that friends and relatives will not harm the respondent	3	11
Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	11	6
Carefulness with online activities	13	7

20. Are you careful when you open email attachments?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	14	12
Differentiation between different accounts	15	7
Necessity of keeping good relationships with friends and relatives	4	11

Necessity of helping others	6	14
Depending on the situation and at the discretion of the respondent	14	6
Awareness of risks and outcomes of cybercrimes	11	7
Importance for relatives and friends to check on the respondent	1	10
Belief that friends and relatives will not harm the respondent	5	16
Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	14	8
Carefulness with online activities	16	9

21. Do you have any shared email or other Internet accounts?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	11	7
Differentiation between different accounts	13	11
Necessity of keeping good relationships with friends and relatives	1	17
Necessity of helping others	7	13
Depending on the situation and at the discretion of the respondent	15	2
Awareness of risks and outcomes of cybercrimes	14	4
Importance for relatives and friends to check on the respondent	9	16
Belief that friends and relatives will not harm the respondent	6	15
Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	13	7
Carefulness with online activities	11	8

22. Do you share any instant messenger's passwords with others?		
Category	Taught (%)	Untaught (%)
Differentiation between private and other information	18	9
Differentiation between different accounts	10	7
Necessity of keeping good relationships with friends and relatives	8	15
Necessity of helping others	1	11

Depending on the situation and at the discretion of the respondent	11	10
Awareness of risks and outcomes of cybercrimes	15	5
Importance for relatives and friends to check on the respondent	8	14
Belief that friends and relatives will not harm the respondent	7	15
Passwords are protected (i.e. passwords not shared, different passwords for different accounts)	11	8
Carefulness with online activities	11	6